

# SafeNet eToken FIDO

---

## STARTING AND USER GUIDE



Document Information

<b>Product Name/Version</b>	SafeNet eToken Fusion
<b>Release Date</b>	21 March 2025

Revision History

<b>Revision</b>	<b>Date</b>	<b>Reason</b>
Rev. A	21 March 2025	Initial Release

# CONTENTS

CHAPTER 1: Overview .....	4
What is SafeNet eToken FIDO? .....	4
CHAPTER 2: Using FIDO 2.0 with SafeNet eToken FIDO .....	5
Initialization .....	5
Add a PIN .....	5
CHAPTER 3: Registration .....	8
To register a device: .....	8
CHAPTER 4: Authentication .....	11
To authenticate with a device: .....	11
CHAPTER 5: Reinitialization .....	13
To reinitialize a device: .....	13
CHAPTER 6: FIDO on a Microsoft 365 Account .....	16
Initialization .....	16
To initialize a device: .....	16
To register a device on Microsoft: .....	16
Authentication with a device .....	23
CHAPTER 7: FIDO on Android .....	26
Initialization .....	26
To register a device: .....	26
Authentication with a device .....	29
CHAPTER 8: Technical Specifications .....	31
Product Characteristics .....	31
Touch Sense Functionality .....	32
Device LED Behavior .....	33
Support Contact .....	34
CHAPTER 9: Activate your Fido keys in SafeNet Trusted Access .....	35
What is SafeNet Trusted Access and how to use it? .....	35

# CHAPTER 1: Overview

## What is SafeNet eToken FIDO?

---

SafeNet eToken FIDO is designed for FIDO based applications and offers perfect integration with native support from the Microsoft environments and mobile with USB-C connector.

The devices embed a FIDO applet compliant with Fast IDentity Online 2.0 (FIDO2) standard and offers passwordless access for cloud apps, network domains and all Azure AD-connected apps and services.

Passwordless authentication replaces passwords with other methods of identity improving the levels of assurance and convenience. This type of authentication has gained traction because of its considerable benefits in easing the login experience for users and surmounting the inherent vulnerabilities of text-based passwords. These advantages include less friction, a higher level of security that's offered for each app and the elimination of the legacy password.

# CHAPTER 2: Using FIDO 2.0 with SafeNet eToken FIDO

This section describes how to initialize, register, authenticate, and perform more operations on SafeNet eToken FIDO.

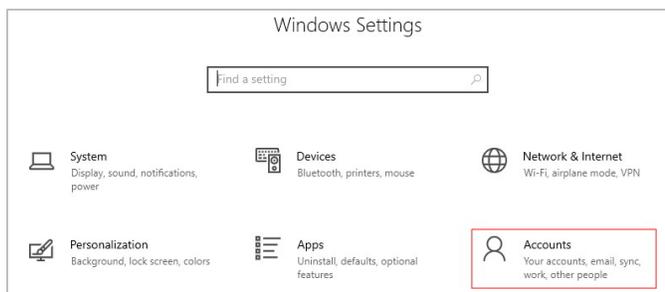
## Initialization

Perform the following steps to initialize a device:

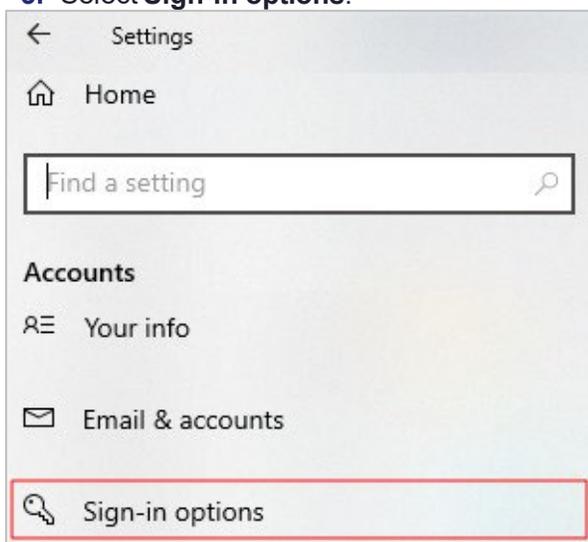
### Add a PIN

To add a PIN to a security key:

1. On your Windows computer, select **Start > Settings**.
2. Select **Accounts**.



3. Select **Sign-in options**.



4. Select **Security Key**.

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  
This option is currently unavailable—click to learn more
-  **Security Key**  
Sign in with a physical security key

5. Select **Manage**.

 Security Key  
Sign in with a physical security key

Manage a physical security key that can log you into applications.

[Learn more](#)

**Manage**

6. Insert your token into the USB port.

Windows Hello setup ×



Tap your security key on the reader or insert it into the USB port.

**Close**



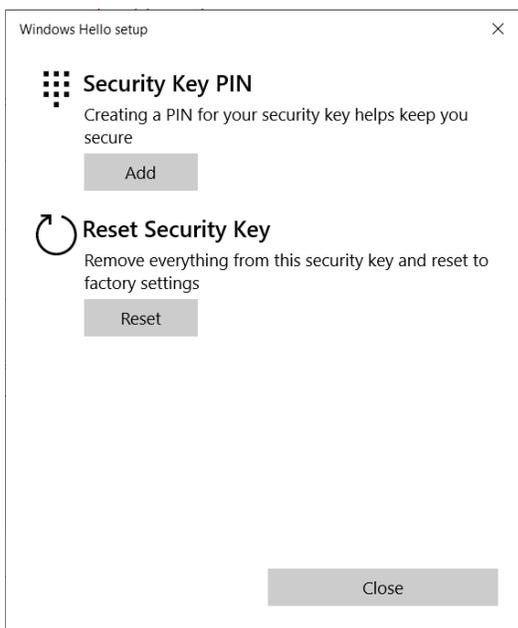
1. Insert the security key in the USB port.



2. Tap the key when the LED light is on

7. Select **Add**, located under the Security Key PIN option.

8.



9. Enter a security key PIN and then re-enter it in the fields provided.

10. Select **OK**.



**Before you can use the token, you must register it on the protected website you want to access.**

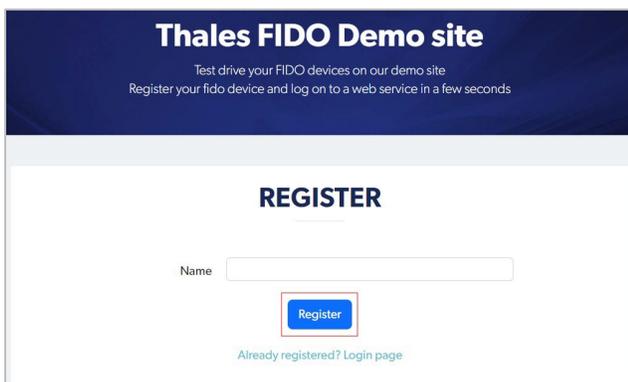
## CHAPTER 3: Registration

### To register a device:

1. Go to: <https://fido.demo.gemalto.com/>.

**NOTE** This site is used as an example, only. To authenticate using a FIDO-compatible method on a supported website, refer to the website's help section for detailed instructions.

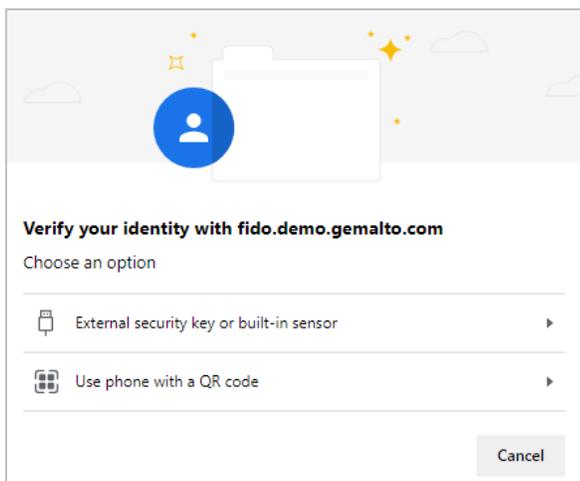
2. Select **Register Now**.
3. Enter your name in the field provided and then select **Register**.



The screenshot shows the 'Thales FIDO Demo site' header with the text 'Test drive your FIDO devices on our demo site' and 'Register your fido device and log on to a web service in a few seconds'. Below this is a 'REGISTER' section with a 'Name' input field and a blue 'Register' button. A link for 'Already registered? Login page' is visible at the bottom.

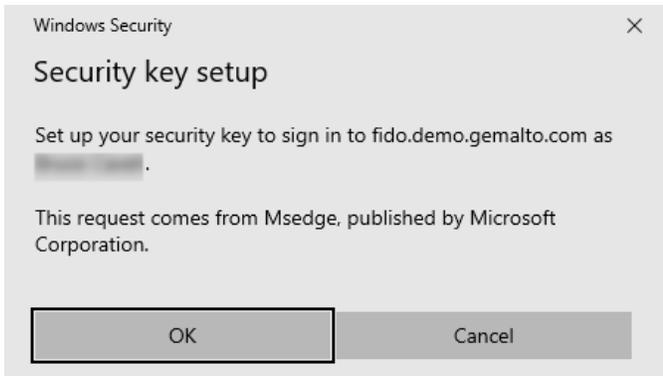
- Select **External security key or built-in sensor**.

**NOTE** The **Use phone with a QR code** option is not supported by this product.

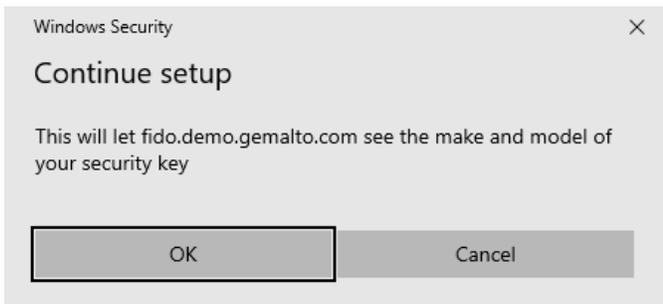


The screenshot shows a screen titled 'Verify your identity with fido.demo.gemalto.com'. It asks the user to 'Choose an option' and provides two choices: 'External security key or built-in sensor' and 'Use phone with a QR code'. A 'Cancel' button is located at the bottom right.

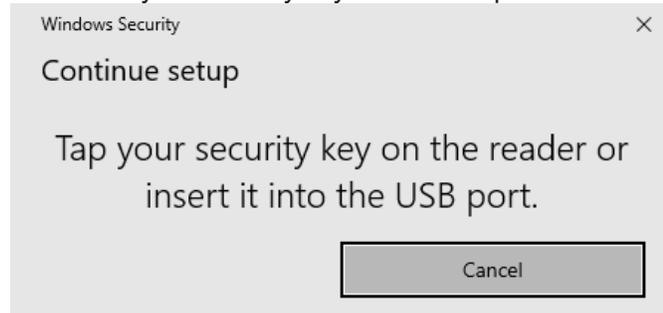
4. Select **OK**.



**5. Select OK.**



**6. Insert your security key to the USB port.**



**7. Insert the PIN**

**8. Touch the security key once requested.**



The welcome screen displays, and your token is now accessible.

**Thales FIDO Demo site**  
Test drive your FIDO devices on our demo site  
Register your fido device and log on to a web service in a few seconds

**WELCOME !**

 **eToken FIDO**  
Type: packed  
AAGUID: efb96b10-a9ee-4b6c-a4a9-d32125ccd4a4  
Counter: 2 

Logout

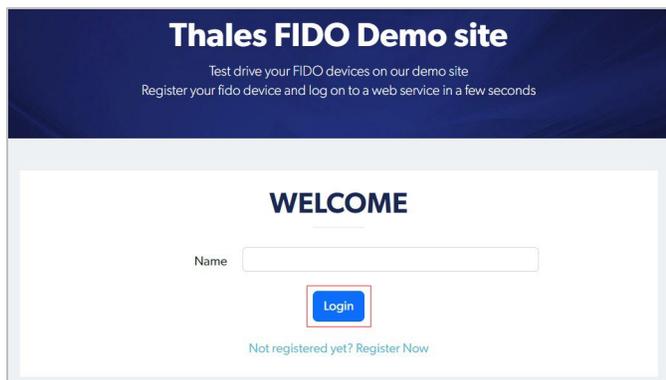
## CHAPTER 4: Authentication

### To authenticate with a device:

1. Go to: <https://fido.demo.gemalto.com/>.

**NOTE** This site is used as an example, only. To authenticate using a FIDO-compatible method on a supported website, refer to the website's help section for detailed instructions.

2. Enter the name that you used during “[Initialization](#)” and then select **Login**.



The screenshot shows the Thales FIDO Demo site. At the top, it says "Thales FIDO Demo site" and "Test drive your FIDO devices on our demo site Register your fido device and log on to a web service in a few seconds". Below this is a "WELCOME" section with a "Name" input field and a "Login" button. A link "Not registered yet? Register Now" is also visible.

A Windows Security pop-up displays to authenticate the user.

3. Insert your device into the USB port.



The screenshot shows a Windows Security pop-up dialog titled "Making sure it's you". It contains the text: "Please sign in to fido.demo.gemalto.com. This request comes from Msedge, published by Microsoft Corporation. Tap your security key on the reader or insert it into the USB port." There is a "Cancel" button at the bottom.

4. Insert the PIN.
5. Touch the security key once requested.

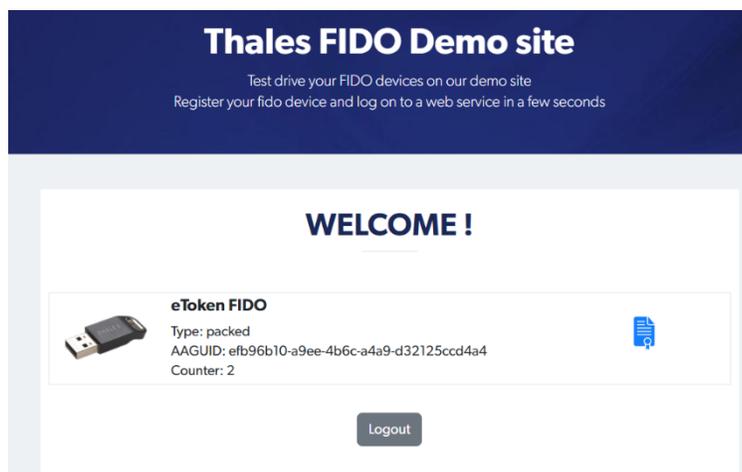


On a PC, tap the security key while it is inserted to complete authentication.



On a mobile device, tap the security key while it is connected to complete authentication.

You now have access to the site.

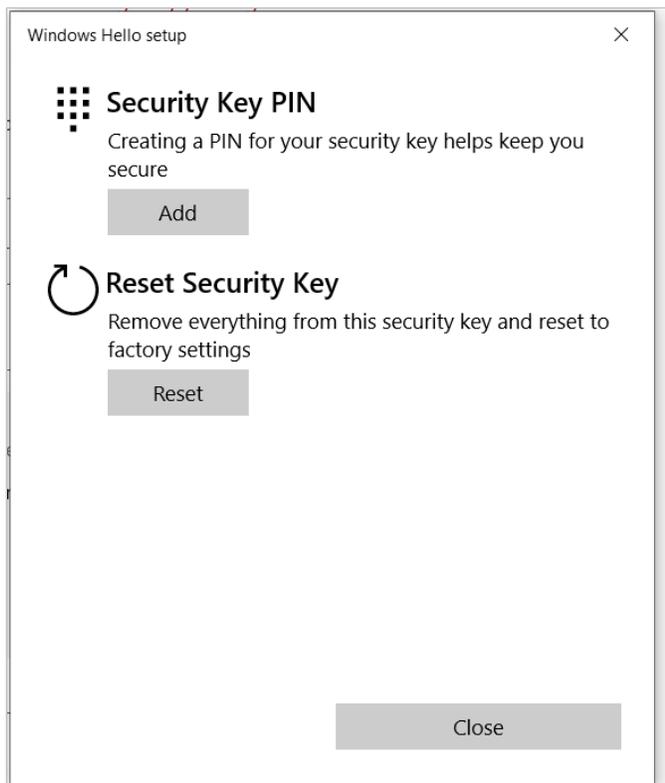


# CHAPTER 5: Reinitialization

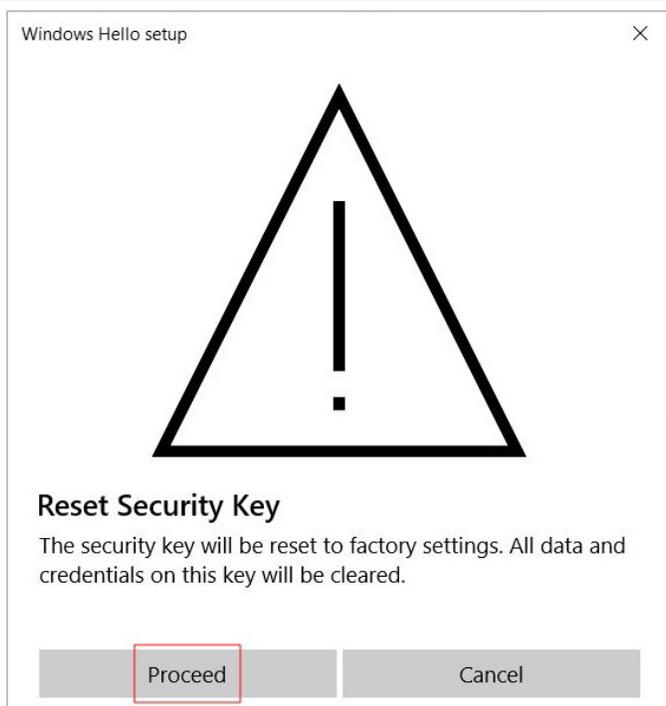
**\*\*WARNING\*\*** This is a destructive procedure. All data and credentials previously created with the security key will be lost.

## To reinitialize a device:

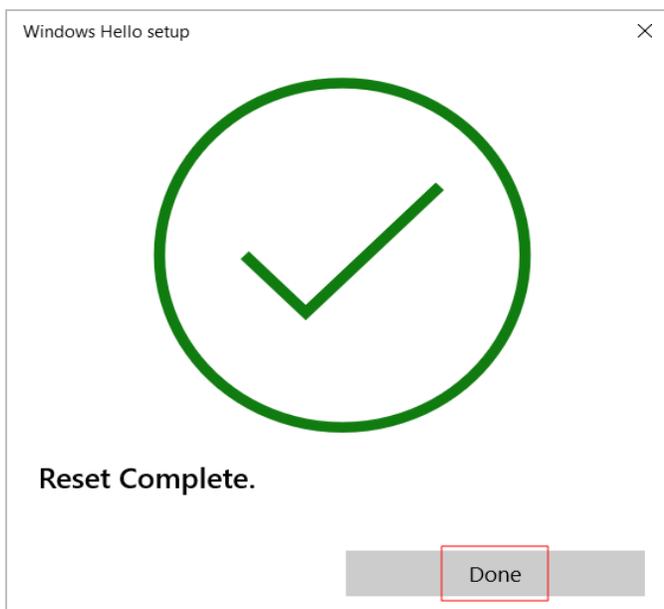
1. Perform steps 1 to 4 of [“Initialization of the device”](#).
2. Select **Reset**.



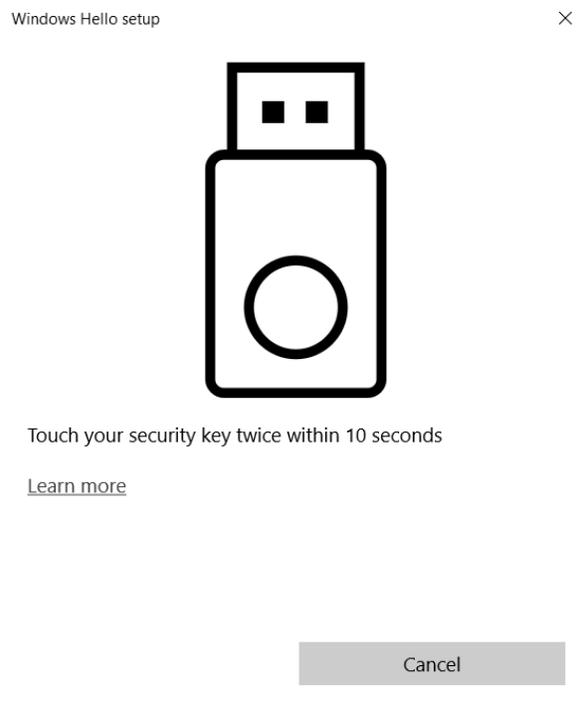
A message warns about resetting to factory settings.



### 3. Select Proceed



4. Remove and insert your security key into the port.
5. to complete the reset operation, touch the token twice once requested.



6. Select **Done**.
7. To re-initialize the security key, go to "[Initialization](#)".

# CHAPTER 6: FIDO on a Microsoft 365 Account

This section describes how to initialize, register, and authenticate eToken FIDO on a Microsoft 365 Account.

## Initialization

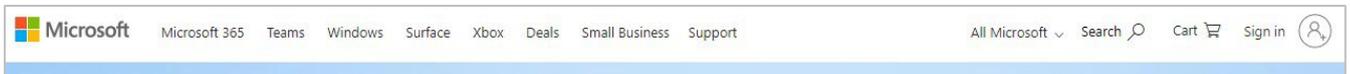
To initialize a device:

1. Add a PIN to a device, see [“Add a pin”](#).

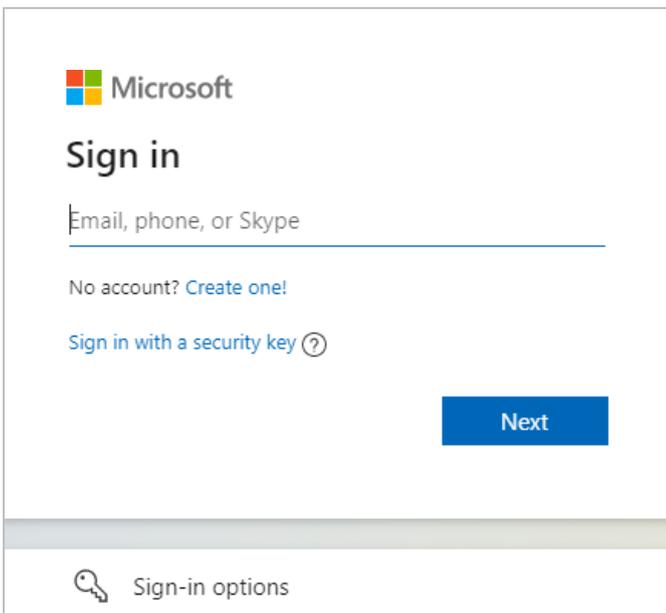
To register a device on Microsoft:

### Scenario 1

1. Go to <https://www.microsoft.com> and then select **Sign in**  at the top-right of the page.



2. Select your preferred Sign-in option.





## Sign-in options

 Face, fingerprint, PIN or security key   
Use your device to sign in with a passkey.

 Sign in with GitHub 

 Forgot my username

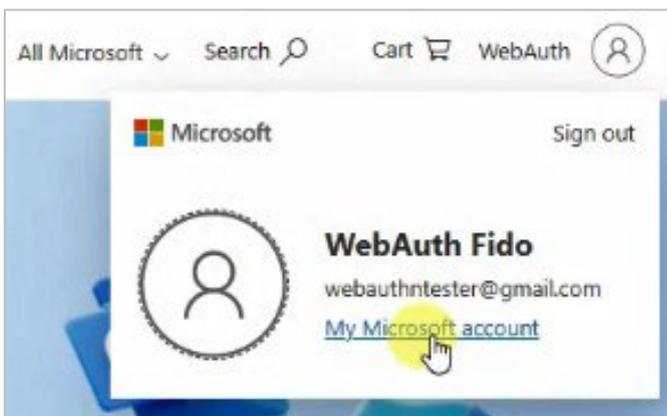
Back

### Scenario 2

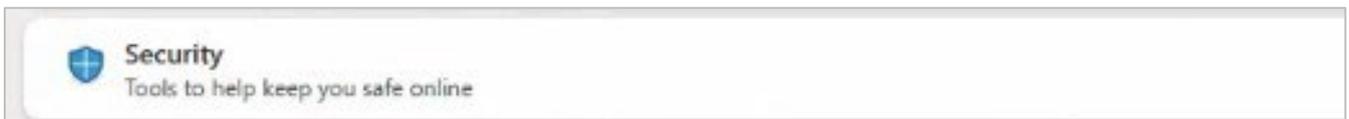
1. Go to <https://www.microsoft.com> and select **WebAuth**  at the top-right of the page.



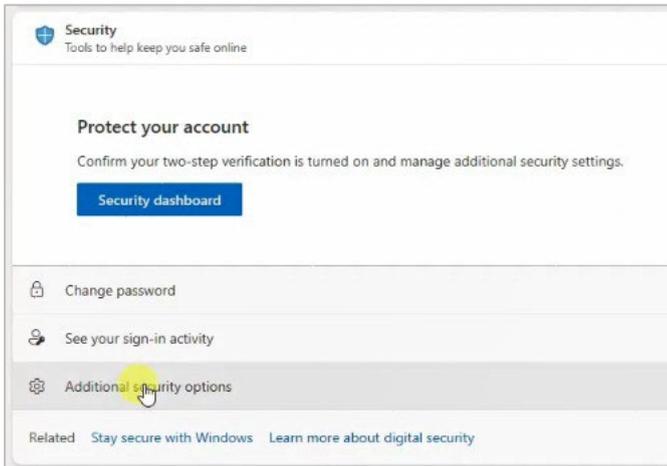
2. Select **My Microsoft account**.



3. Select **Security**.



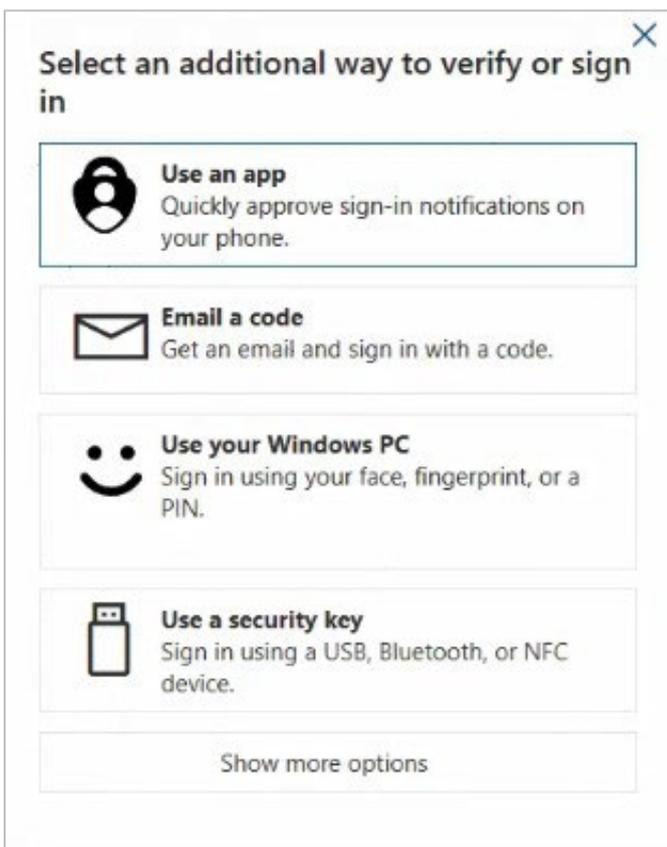
4. Select **Additional security options**.



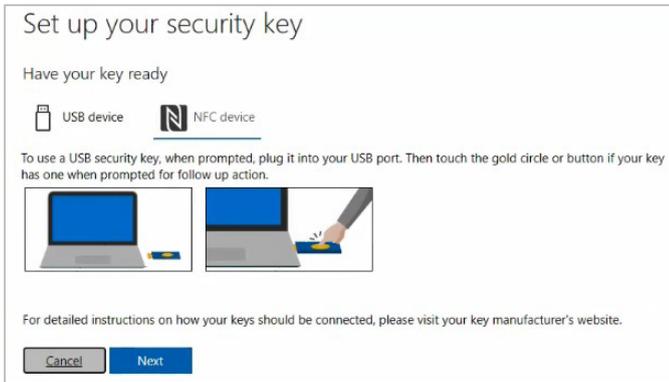
5. Select **Add a new way to sign in or verify**.



6. Select **Use a security key**.



7. Select **USB device** and then select **Next**.

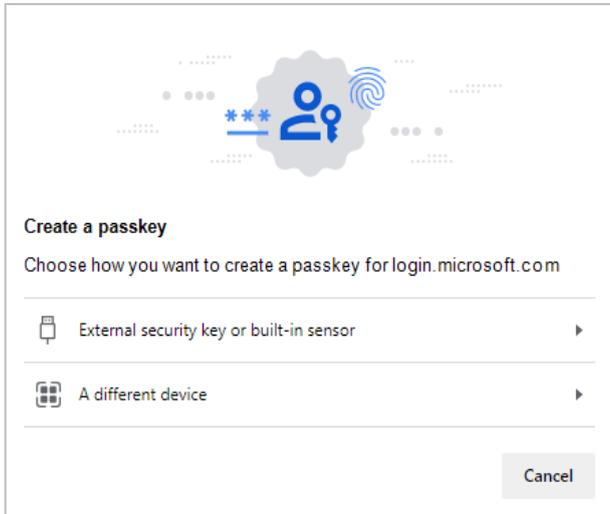


The following screen displays in the background during the set-up procedure.



**8. Select External security key or built-in sensor.**

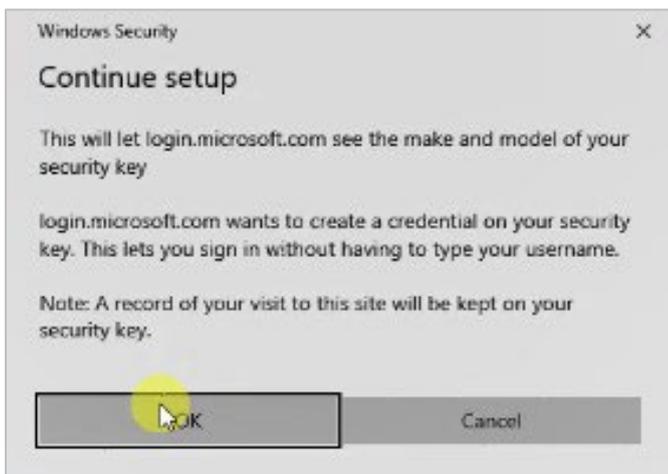
**NOTE** This option displays only if you do not provide the security key within the allotted time. This could occur if, for example, you do not have a smart card reader.



9. Select **OK**.



10. Select **OK**.



11. Insert your security key into the USB port.





12. Enter a name for your security key and then select **Next**.

## Set up your security key

Name your new security key

Hint: Name it so you'll know later which key this one is.

13. Select **Got it**.

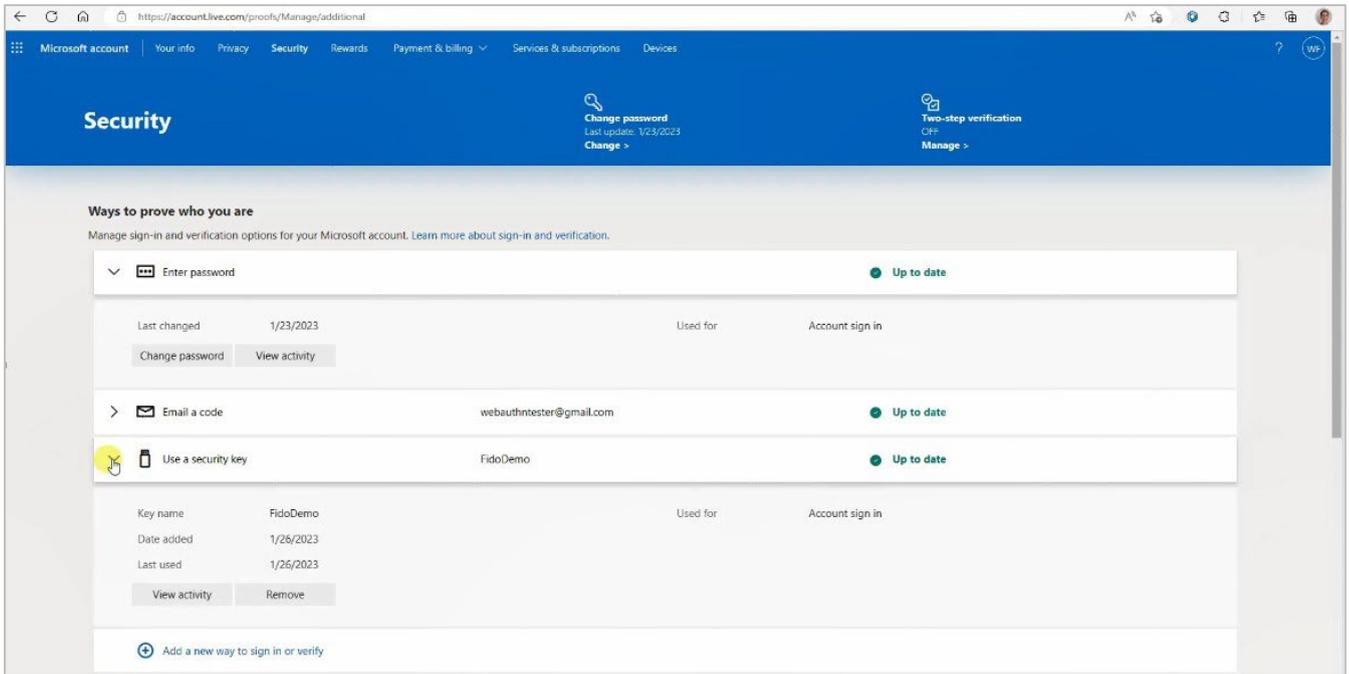
You're all set!

Next time you sign in, you can use your security key instead of a password to sign in.

  
[Add another security key](#)

You can now use your security key to sign in.

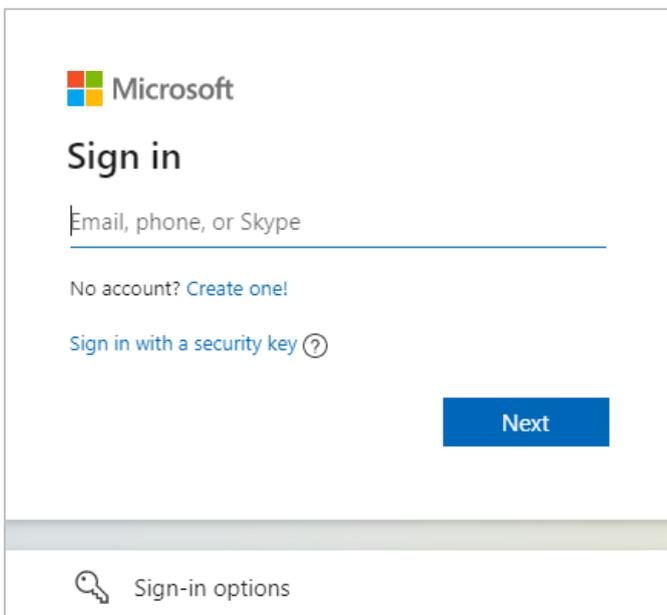
Your security key is listed, as shown in the following screenshot.



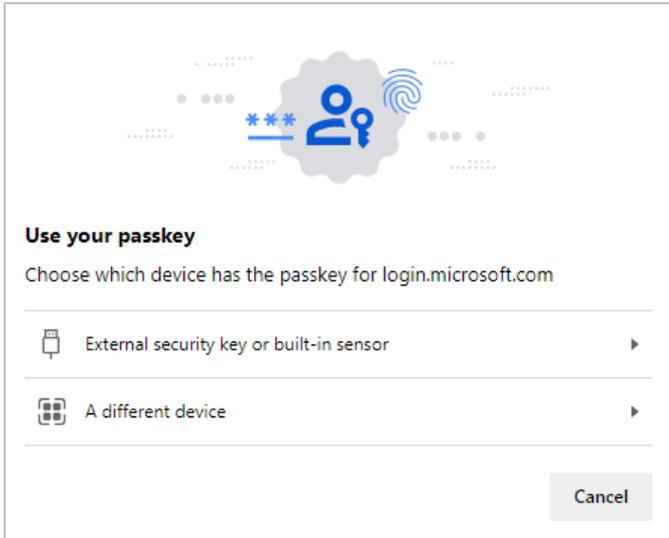
## Authentication with a device

To authenticate with a device on a Microsoft site:

1. Go to the Microsoft site and then select **Sign in with a security key**.



2. Select **External security key or built-in sensor**.



3. Insert your device into the USB port.



#### 4. Select your sign-in preference.



The image shows a Microsoft sign-in preference dialog box. At the top left is the Microsoft logo. Below it is the email address 'webauthntester@gmail.com'. The main heading is 'Stay signed in?'. Below this is the text 'Stay signed in so you don't have to sign in again next time.' There is a checkbox labeled 'Don't show this again' which is currently unchecked. At the bottom, there are two buttons: a grey 'No' button and a blue 'Yes' button.

You now have access to the Microsoft website.

# CHAPTER 7: FIDO on Android

This section describes how to initialize, register, authenticate, and perform more operations on the SafeNet eToken FIDO on Android.

Before, please make sure '[FIDO Key Manager](#)' (FKM) application is installed on your Android device.

## Initialization

Perform the following steps to initialize an eToken FIDO:

### Add a PIN

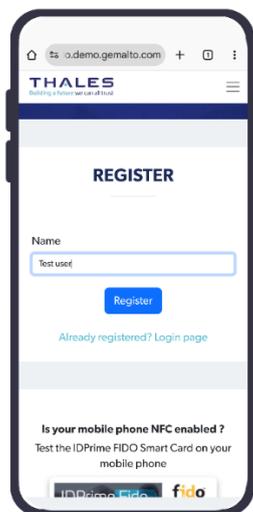
To add a PIN please follow the detailed steps in [PIN Management](#)

## To register a device:

1. Go to: <https://fido.demo.gemalto.com/>.

**NOTE** This site is used as an example, only.

2. Select **Register Now**.
3. Enter your name in the field provided and then select **Register**.

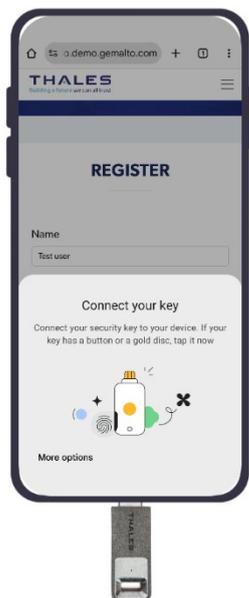


- Select **External security key or built-in sensor**.

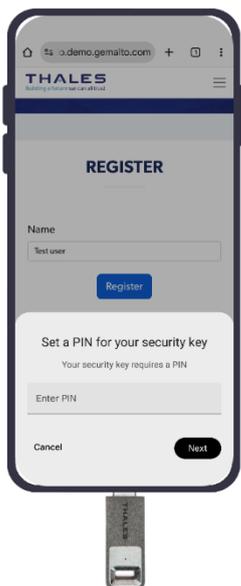
**NOTE** This option displays only if you do not provide the security key within the allotted time. This could occur if, for example, you do not have a smart card reader.

**NOTE** The **Use phone with a QR code** option is not supported by this product.

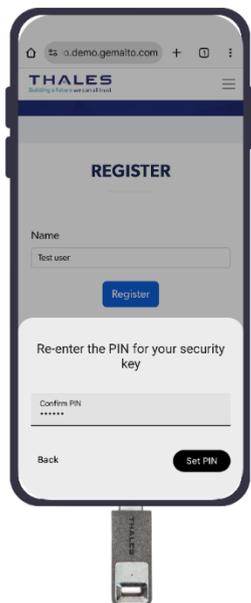
#### 4. Insert your key.



#### 5. Set up the PIN.



6. Re-enter the PIN



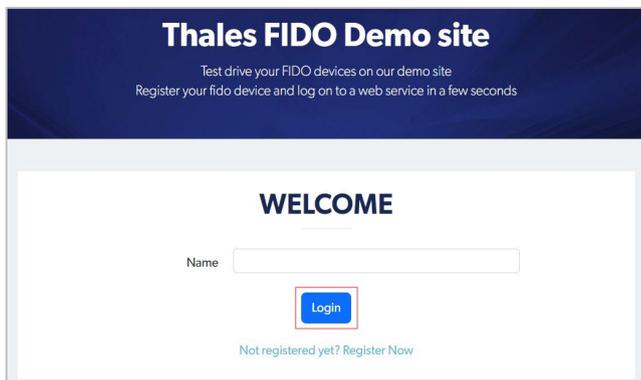
7. The welcome screen displays, and your token is now accessible.



## Authentication with a device

**NOTE** This site is used as an example, only. To authenticate using a FIDO-compatible method on a supported website, refer to the website's help section for detailed instructions.

1. Go to: <https://fido.demo.gemalto.com/>.
2. Enter the name that you used during “[Registration](#)” and then select **Login**.



The screenshot shows the 'Thales FIDO Demo site' interface. At the top, it says 'Test drive your FIDO devices on our demo site' and 'Register your fido device and log on to a web service in a few seconds'. Below this is a 'WELCOME' section with a 'Name' input field and a 'Login' button. A link for 'Not registered yet? Register Now' is also visible.

A Windows Security pop-up displays to authenticate the user.



3. Insert your device to the USB-C port on your mobile.

## Thales FIDO Demo site

Test drive your FIDO devices on our demo site  
Register your fido device and log on to a web service in a few seconds

### WELCOME !



#### eToken FIDO

Type: packed  
AAGUID: efb96b10-a9ee-4b6c-a4a9-d32125ccd4a4  
Counter: 2



Logout

You now have access to the site.

# CHAPTER 8: Technical Specifications

## Product Characteristics

CHARACTERISTICS	DESCRIPTION
<b>MEMORY</b>	52K
<b>STANDARDS</b>	API and Standards Support: > FIDO 2.0 and U2F
<b>OPERATING SYSTEMS</b>	> FIDO: Supported in Windows 10 and other FIDO compliant operating systems. > PKI: Windows Server 2008/R2, Windows Server 2012 and 2012 R2, Windows 7, Windows 8 > Windows 10, Windows 11, Mac OS, Linux
<b>DIMENSIONS</b>	> USB-A: 16mm*8mm*40.5mm > USB-C: 12mm*6.5mm*38mm
<b>OPERATING TEMPERATURE</b>	0° C to 70° C (32° F to 158° F)
<b>STORAGE TEMPERATURE</b>	-40° C to 85° C (-40° F to 185° F)
<b>HUMIDITY RATING</b>	0-100% without condensation
<b>WATER RESISTANCE CERTIFICATION</b>	IP X7 – IEC 529
<b>USB CONNECTOR</b>	> USB type A and USB type C supports USB 1.1 and 2.0 (full speed)
<b>CASING</b>	Hard molded plastic, tamper evident
<b>MEMORY DATA RETENTION</b>	At least 10 years
<b>MEMORY CELL REWRITES</b>	At least 500,000
<b>COMPATIBILITY</b>	Microsoft Azure Active Directory accounts
<b>CERTIFICATIONS</b>	> U2F (USB) certification, Version 1.1 > FIDO2 Level 1, Version 2.0 > CC EAL5+ certified according to EN 419211 part 2 to part 6 (corresponding to the PP QSCD)

	> Conformity to: • French ANSSI • eIDAS compliant for e-signature
<b>ATR</b>	• 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 85 59 56 FB 12 01 78 82 90 00 88
<b>PRODUCT NAME</b>	SafeNet eToken FIDO
<b>MASK VERSION</b>	G286
<b>APPLET VERSION</b>	> FIDO 2.0.2.B > IDPrime Java Applet 4.4.2.a
<b>PIN</b>	Default PIN: "0000"

## Touch Sense Functionality

To use the touch sense functionality, consider the following:

- > Presence detection is required as part of FIDO authentication.
- > The presence detection surface is present at the backside of the token.
- > The presence detection surface should only be touched and NOT pressed.
- > The LED on the SafeNet eToken FIDO fades in and out while waiting to detect a human.

presence. When the presence detection surface is touched:

- the LED remains lit on SafeNet eToken FIDO
- the LED turns off on SafeNet eToken FIDO

Example of touch sense usage:

Below image represents the SafeNet eToken Fusion



Below image represents the SafeNet eToken FIDO:



## Device LED Behavior

The below table describes the different LED modes of the device:

LED MODE	DESCRIPTION
<b>TURN OFF</b>	Device is not connected to computer or USB port is suspended
<b>TURN ON</b>	Device is connected to computer and ready for operation.
<b>FADE IN / FADE OUT</b>	Device waits for human presence detection. This feature is triggered by firmware while parsing the CTAP2 payloads to detect if user presence is required for specific commands. User should touch the device within predefined time-out period (30 sec) otherwise CTAP2 request is rejected.
<b>BLINK</b>	Device failure. Device led blinks in a predefined pattern. Contact your Thales sales representative.

---

## Support Contact

---

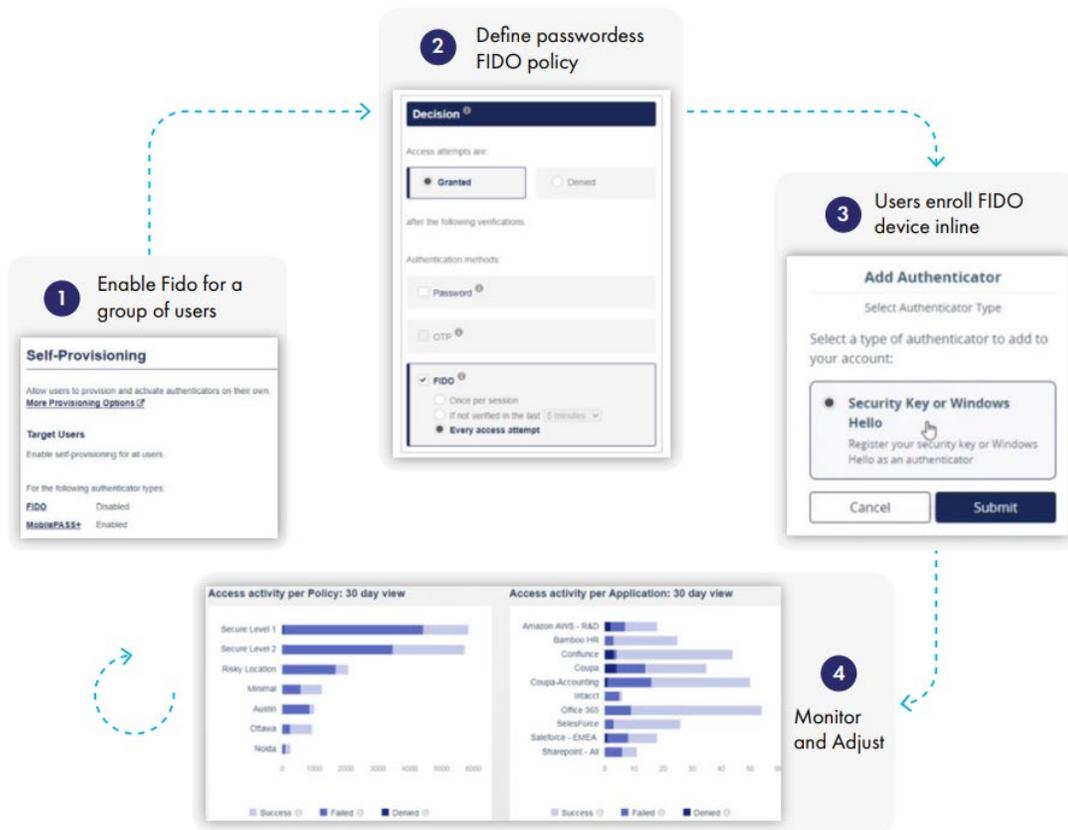
If you encounter a problem while installing, registering, or operating this product, please refer to the documentation above before contacting support.

If you cannot resolve the issue, contact SAS Support Escalation Team at this dedicated email address:  
[dl\\_sassupportescalationteam@thalesgroup.com](mailto:dl_sassupportescalationteam@thalesgroup.com).

# CHAPTER 9: Activate your Fido keys in SafeNet Trusted Access

## What is SafeNet Trusted Access and how to use it?

[SafeNet Trusted Access](#) offers secure, simple access to all your enterprise-managed applications with seamless passwordless authentication.



[Discover how to enable FIDO authentication with your security key in SafeNet Trusted Access.](#)

Discover how the [end users can self-provision SafeNet eToken Fusion or eToken FIDO in SafeNet trusted Access.](#)

**SIGN UP FOR A FREE TRIAL FOR STA**