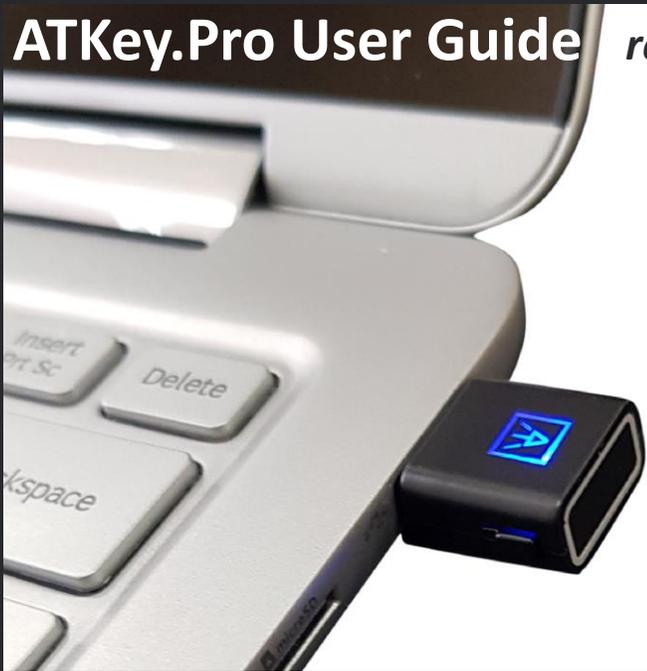


AUTHTREND

-The trend of Authentication-

ATKey.Pro User Guide *rev: 1.0*



Fingerprint Enabled Security Key

slim • compact • best fingerprint experience



- About ATKey.Pro Page 3
- Outlook Page 4
- [Functionalities](#) Page 5
- [Fingerprint enrollment](#) Page 6
- [APP – ATKey for Windows](#) Page 9
- [Windows Hello](#) Page 11
- [FIDO2: Azure AD](#) Page 13
- [FIDO2: Microsoft account](#) Page 15
- [FIDO U2F](#) Page 17
- [LED](#) Page 19

Fingerprint enabled USB security key

- HID device, no driver needs
- Portable key for any Windows, Mac or Chromebook
- Up to 10x fingerprints, matching < 1 sec., FAR < 1/50,000, FRR < 2 %
- FIDO2 certificate



 **KEY**.Pro

Tri-color LED/Logo

Click-able button

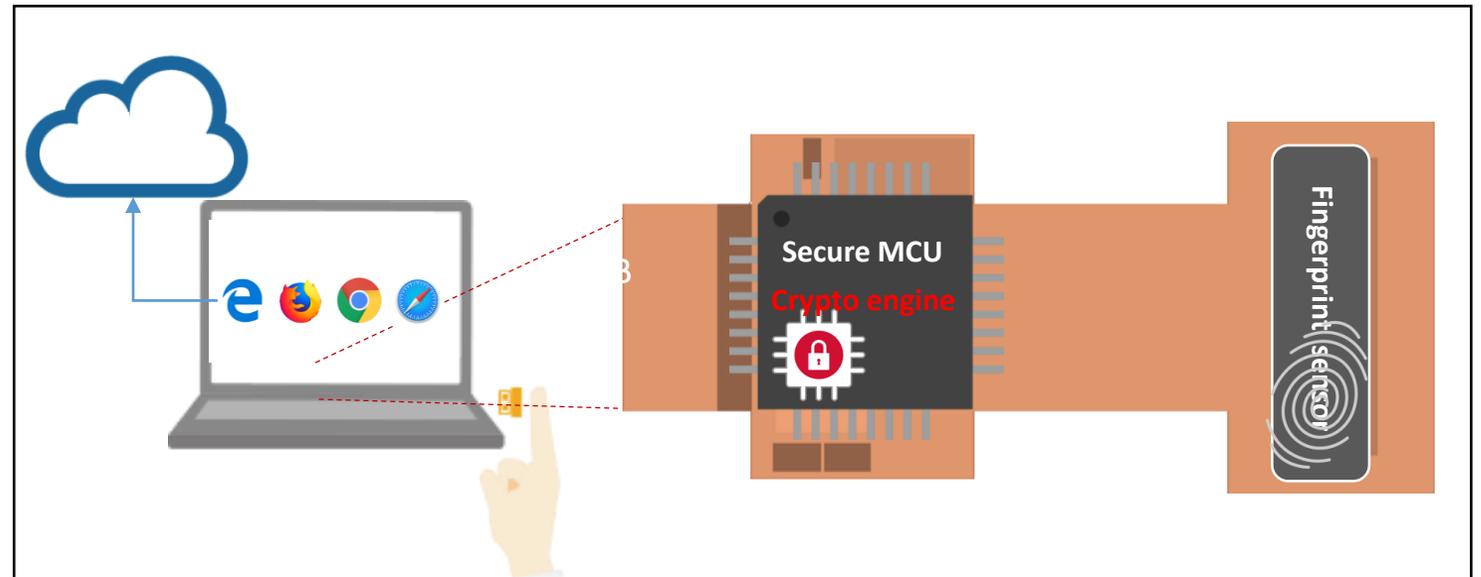
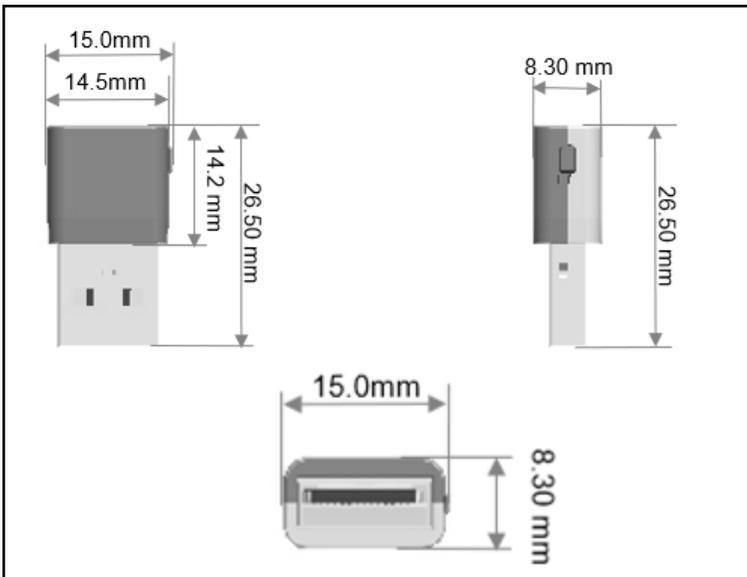
Keycode

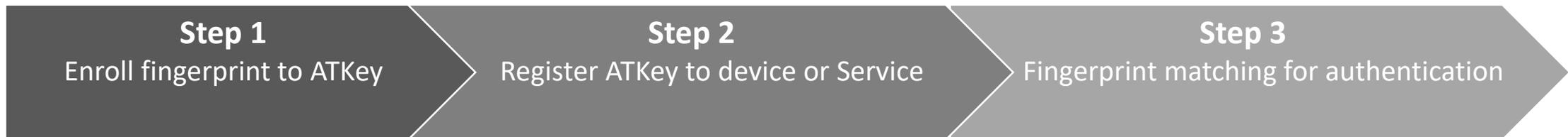
- Each key has his own unique keycode
- It's equal to serial number
- Check keycode for production records, customer service and warranty



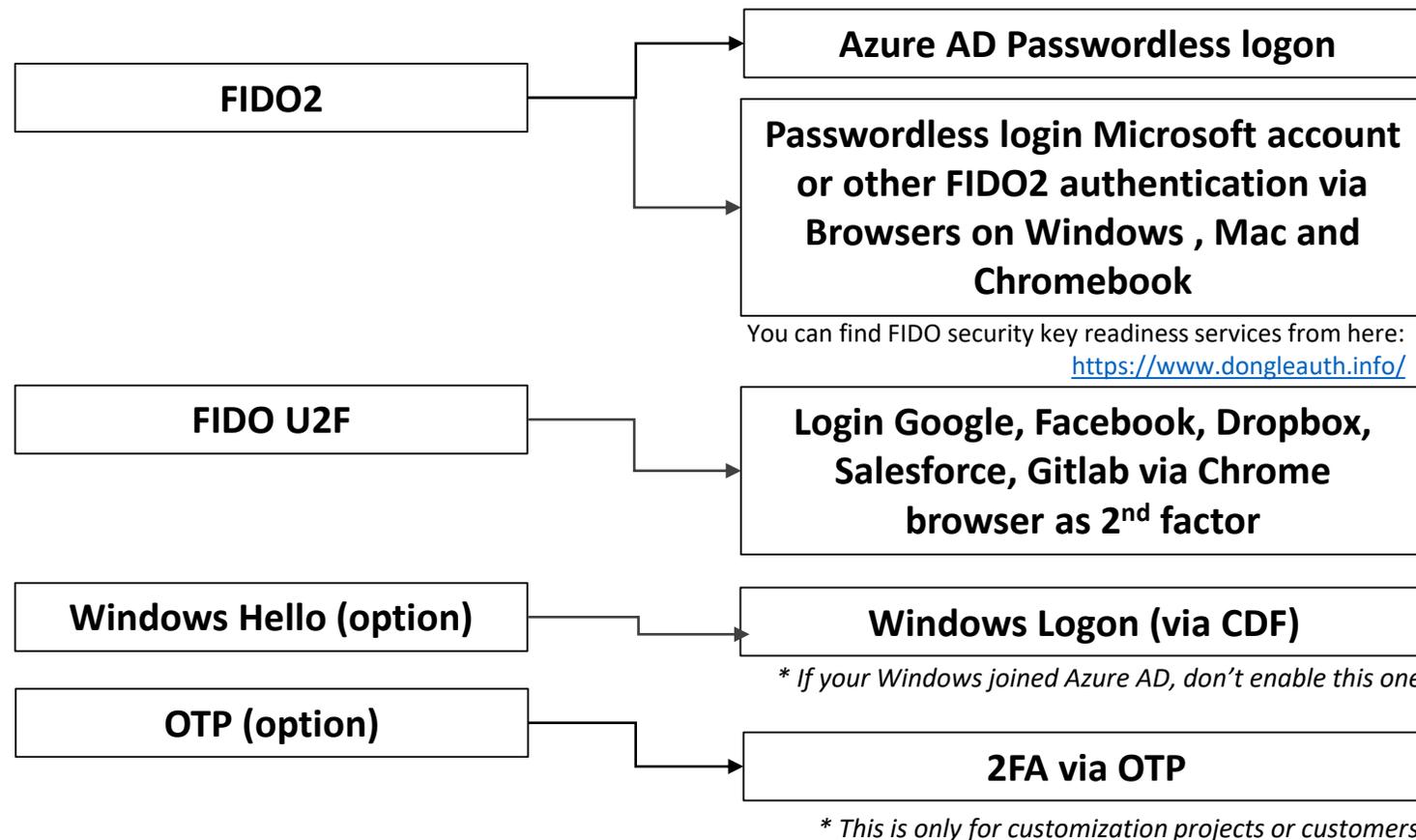
Fingerprint sensor

Silicon keychain





Standalone enrollment (patent filing)
<https://youtu.be/IDrcZxWXAL4>
or through Windows Settings (build 1903)
or through "ATKey for Windows" app



Standalone enrollment

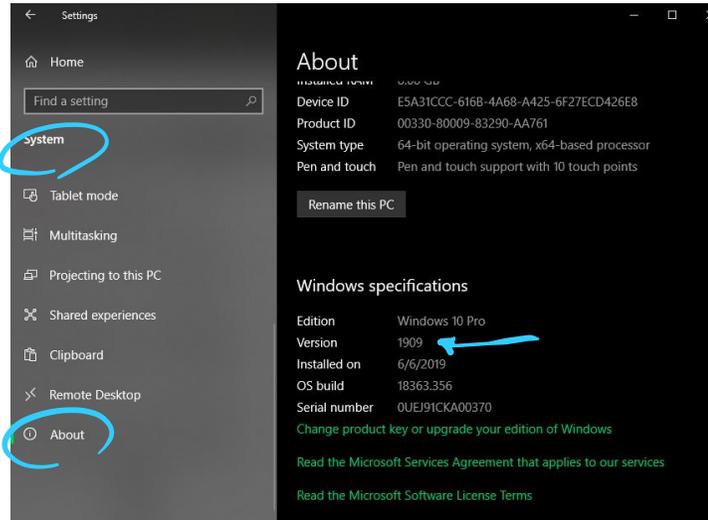
- Insert ATKey.Pro into USB port
- Check Youtube video here for the detail: <https://youtu.be/IDrcZxWXAL4>
- LED is BLUE ON, quick click side-button 3x times (by nail) to go into enrollment mode:
 - If there is no any fingerprint enrolled, LED turns to WHITE
 - If there are any enrolled fingerprints, LED is GREEN flashing, please verify enrolled fingerprint to start enrolling new finger
- Put your specific finger on sensor, touch and lift your finger (LED is WHITE flashing, from slow to faster), repeat it more than 12 times till LED shows GREEN (13th time), then your fingerprint is enrolled



- If you want to quit from standalone enrollment, click button once, LED will turn to Blue, back to normal state.

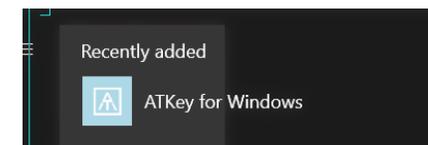
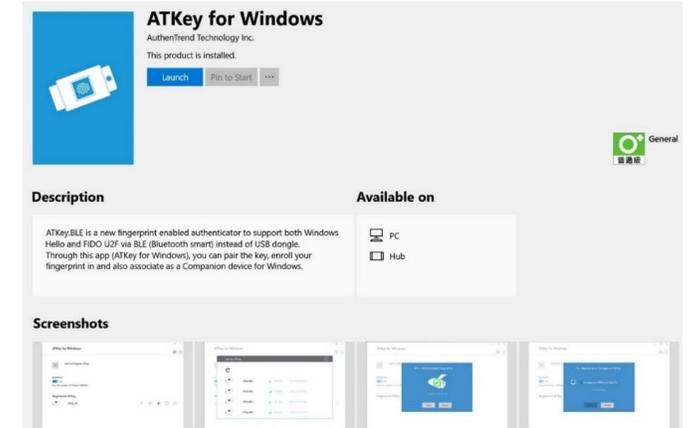
Enroll from Windows Settings

- If your OS is Windows 10 build 1903 or later versions, you can manage ATKey as security key
 - PIN code, add/delete fingerprints, reset
 - jump to [“Windows Settings” page](#) for the detail
- Windows Settings => System => About



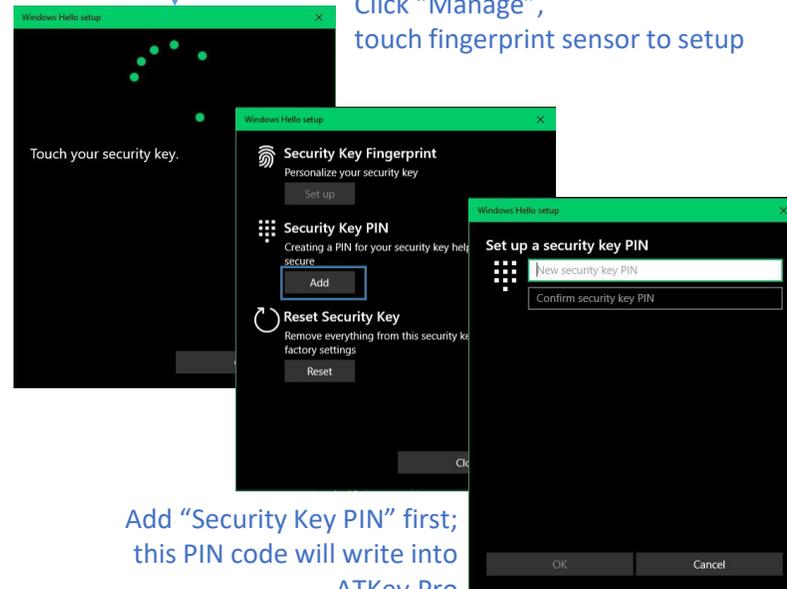
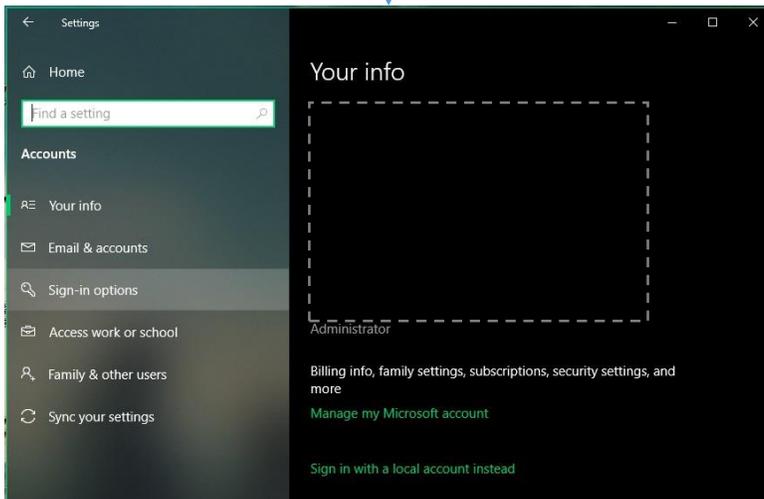
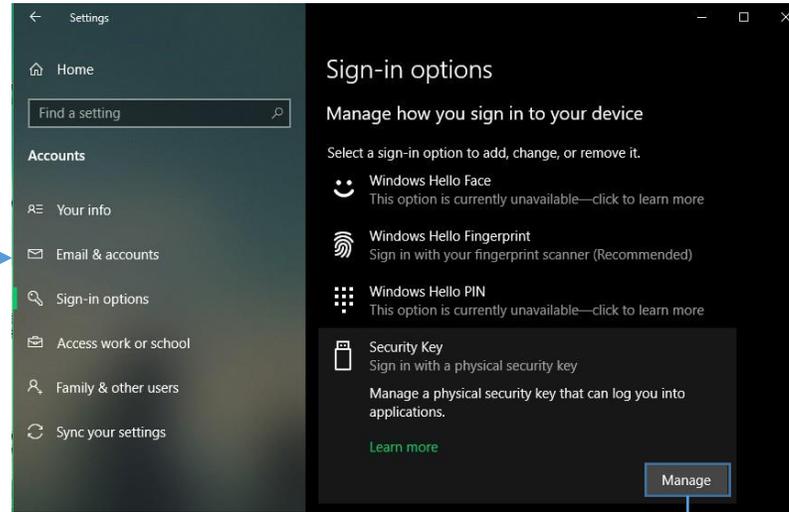
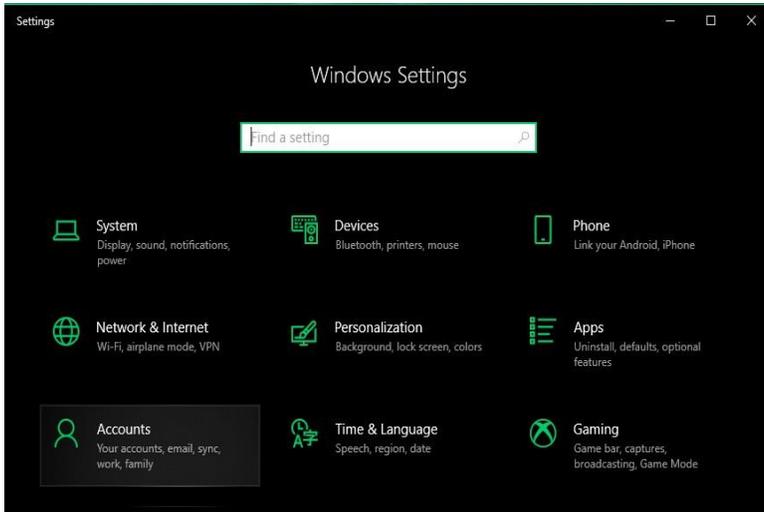
Enroll from ATKey for Windows app

- Download “ATKey for Windows” app from Windows Store to manage ATKey:
 - Enroll fingerprint
 - Add/delete fingerprint
 - ATKey information
 - Companion ATKey to Windows (Windows Hello login)
 - Firmware upgrade
- Search “ATKey” or “AuthenTrend” from Windows Store to find the app, download and install



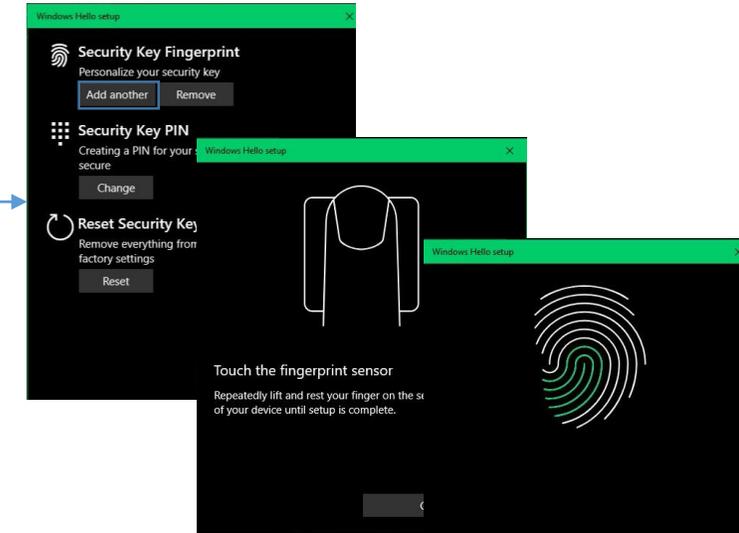
- Jump to [“ATKey for Windows”](#) for the detail

- Windows Settings => Account => Sign-in options => Security Key => add **“PIN code”** and enroll **“Fingerprints”**

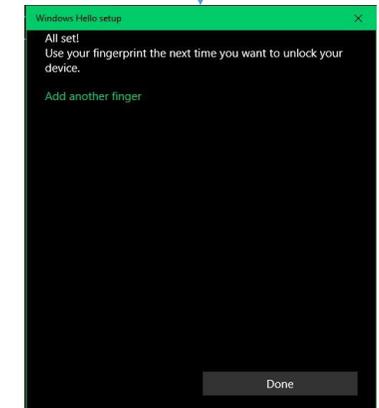


Click “Manage”,
touch fingerprint sensor to setup

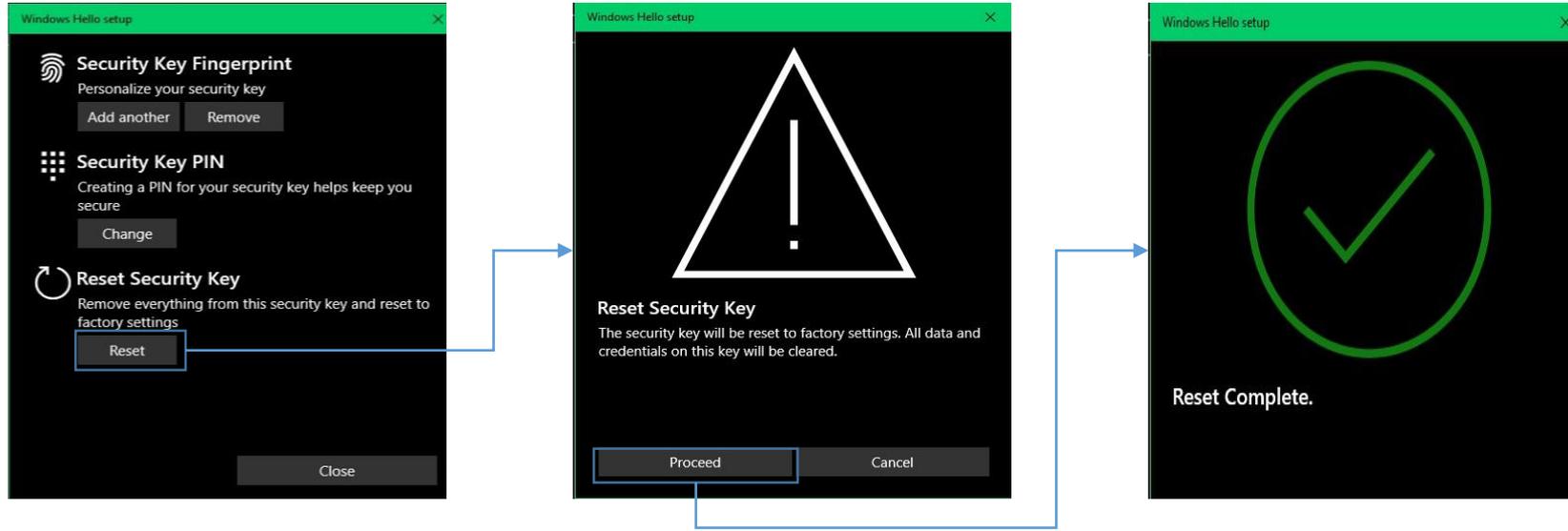
Add “Security Key PIN” first;
this PIN code will write into
ATKey.Pro



- Setup “Security Key Fingerprint”
- Type-in PIN code, following screen hint to enroll fingerprint, until “All Set!”



- Windows Settings => Account => Sign-in options => Security Key => **Reset Security key (Delete PIN code and erase all fingerprints)**

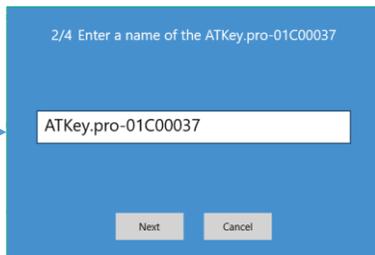
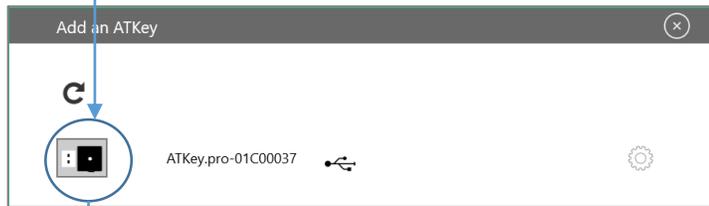
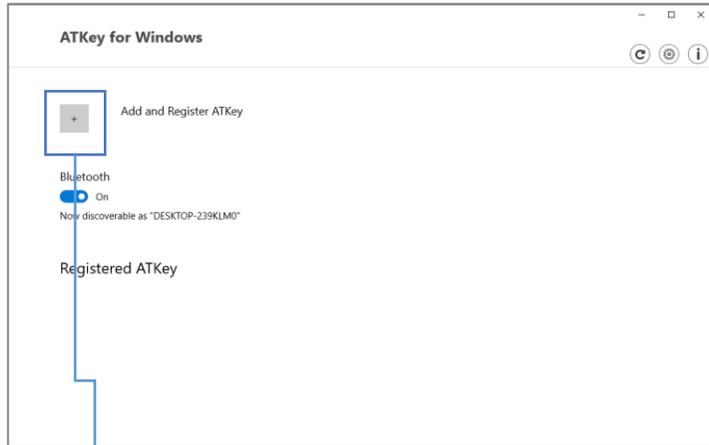


Following UI message, remove and re-insert USB port, all actions need to be done within 10 seconds.

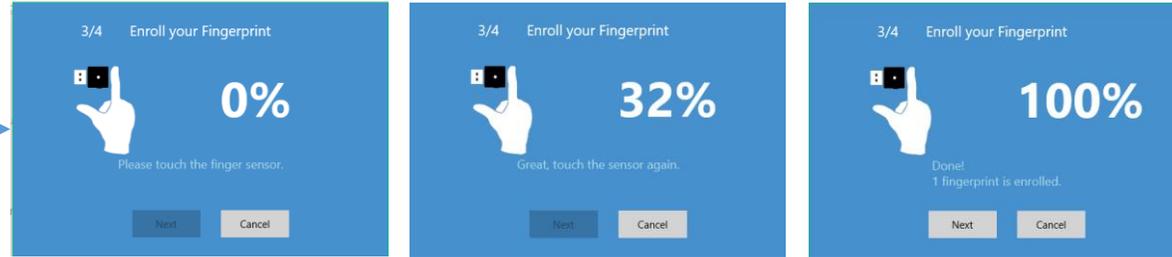
Touch fingerprint to confirm reset;
Not verified enrolled fingerprint to rest, this designed for IT Administrator

KEY.Pro | App "ATKey for Windows" – Enroll fingerprint

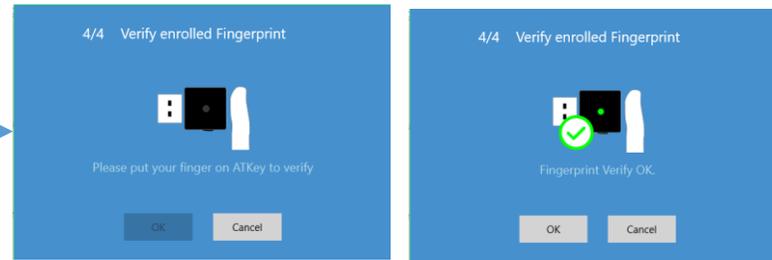
- Launch "ATKey for Windows" app (version 2.0.57.0 or later version)
- Click "Add and Register ATKey" – please make sure ATKey.Pro inserts to USB port and LED shows blue ON



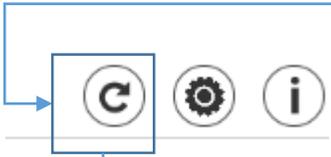
Default name is -: ATKey.Pro + Keycode



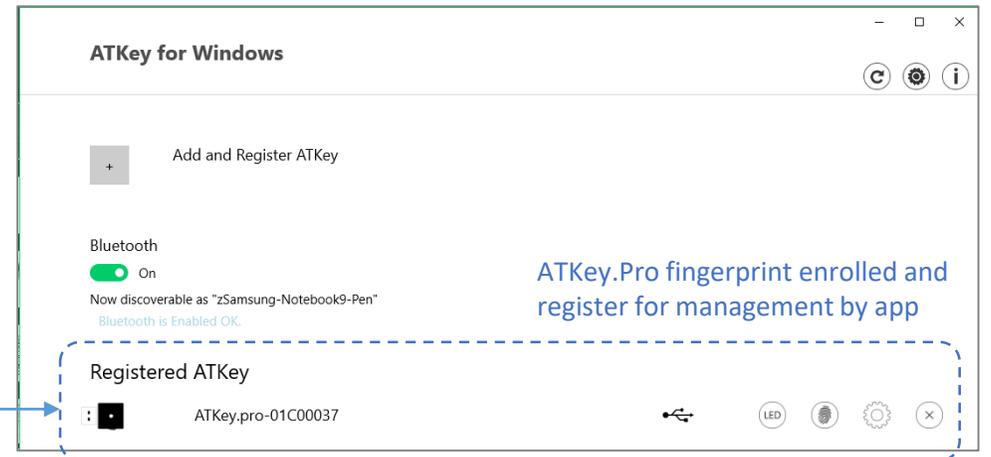
around 12 times touch/enroll to finish ONE fingerprint enrollment



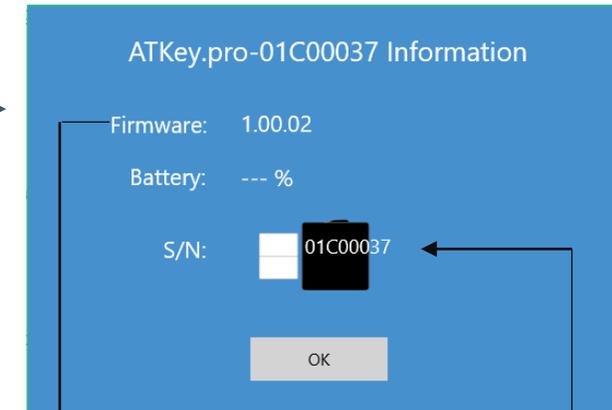
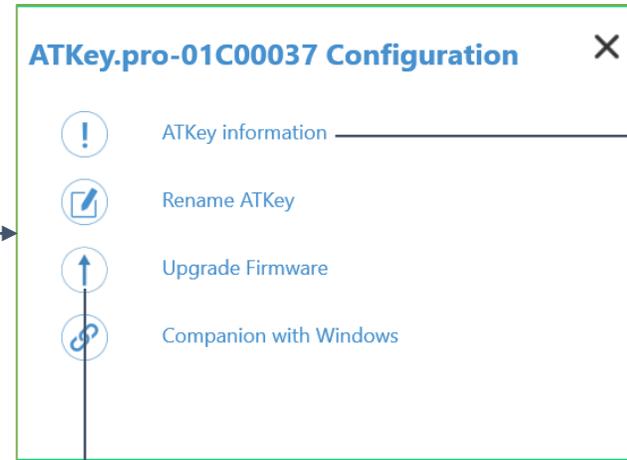
Verify enrolled fingerprint to confirm



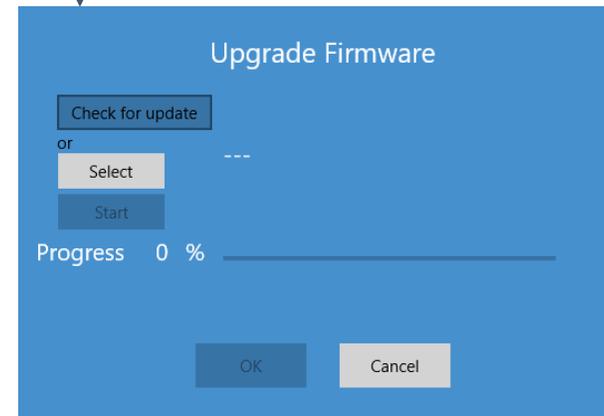
Click to refresh the page



- ATKey management – information, rename, firmware upgrade

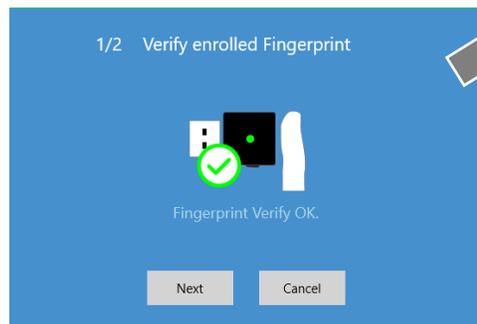
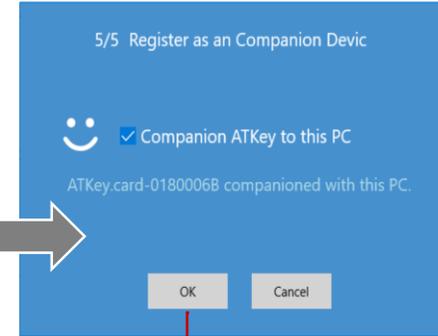
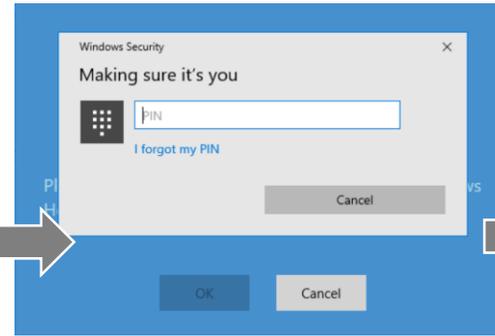
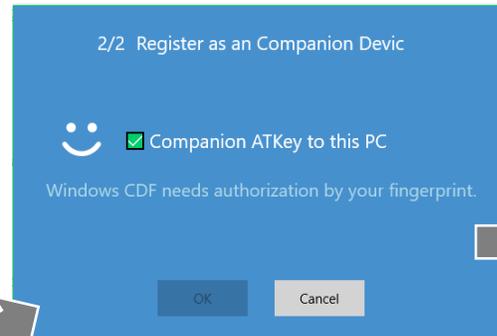
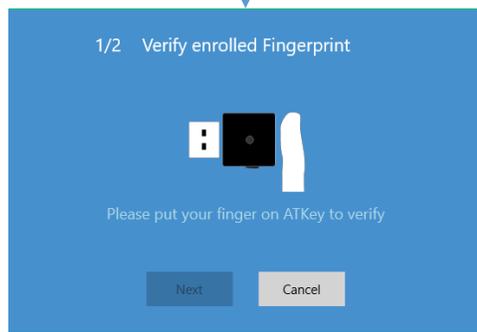
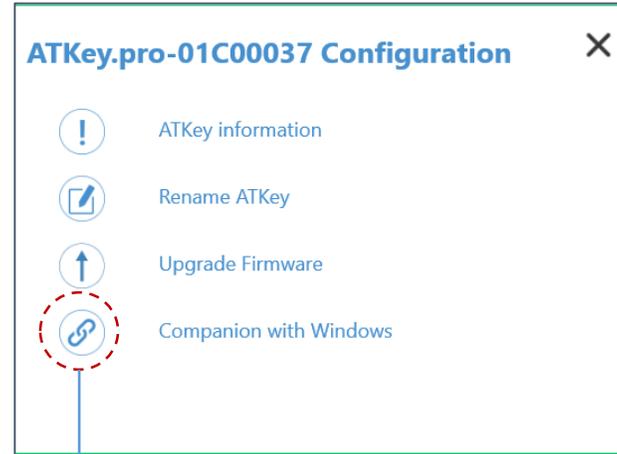


- read firmware version here
- Read "keycode" here

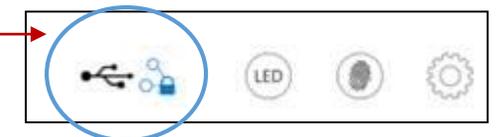


- "Check for Update"
- Select encrypted firmware image to upgrade manually
- Please wait till 100% done, then plug ATKey.Pro off USB port; re-insert to USB port, waiting ~15 sec to boot to new firmware (LED from White to Blue ON).

- ATKey management – Companion with Windows (Windows Hello login via CDF)
- *If your Windows 10 joined Azure AD, please ignore this page since FIDO2 is ready for Azure AD login, it may conflict with Windows Hello*

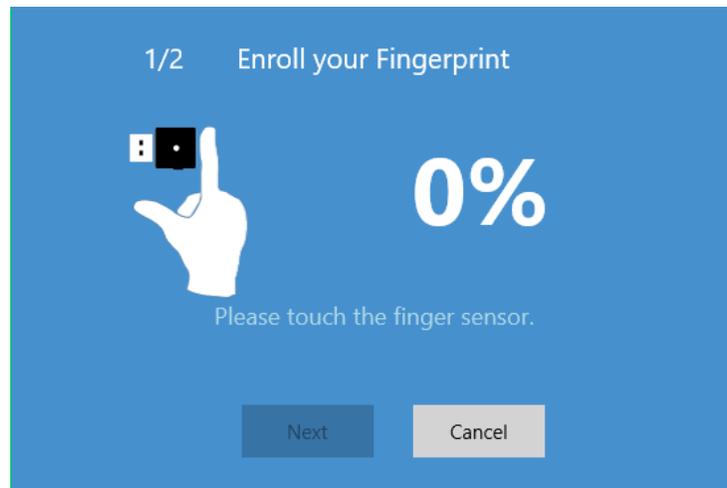
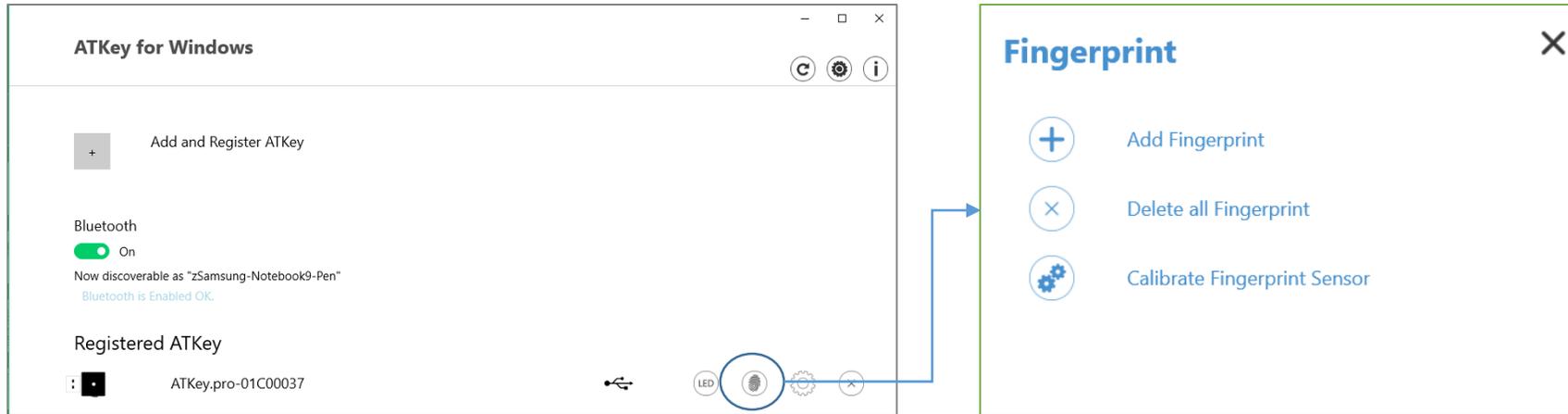


- **Type in "Windows Hello PIN" to allow the companion;**
- *Some Corp. or Org. may disable this group policy by IT Admin, if you saw the message, please contact your IT.*

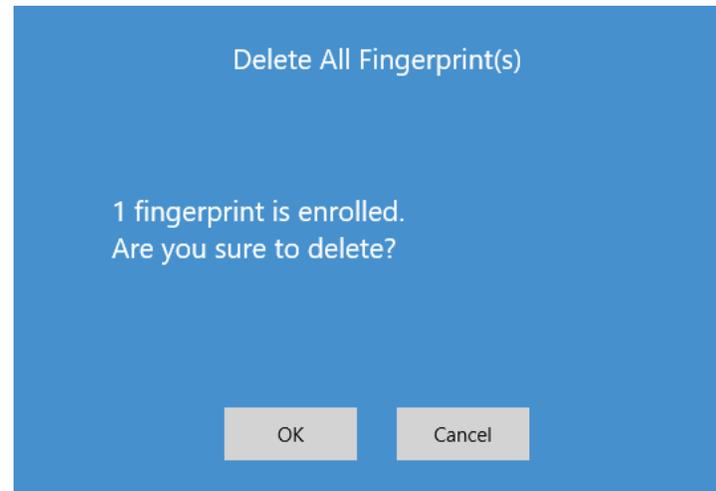


This icon means it's a companion key for Windows Hello via CDF (Companion Device Framework)

- ATKey management – Add/Delete fingerprints, fingerprint sensor calibration



- Enroll new fingerprint in by ~12 times touch, following UI message; up to 10x fingerprints



- Here will delete all enrolled fingerprints, "OK" to delete them
- It needs Windows PIN code to authorize.



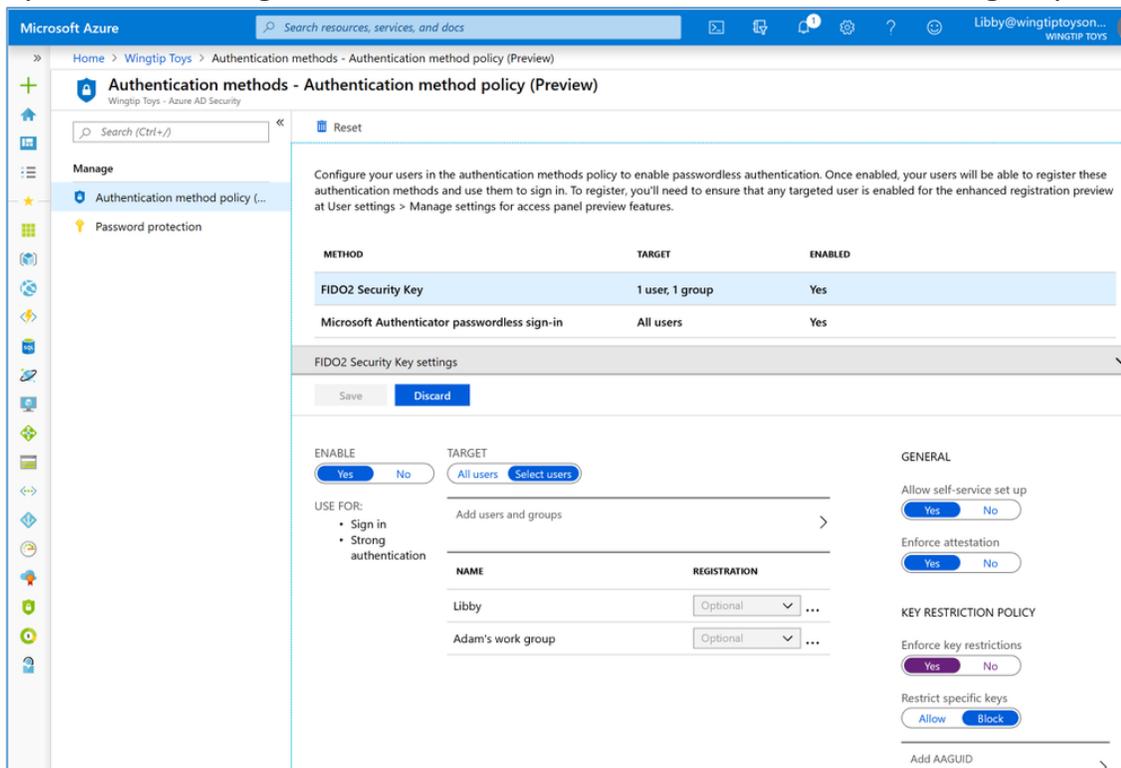
- If you feel something wrong of fingerprint, doing Calibration to re-calibrate the sensor
- Don't put your finger on during calibration; LED will be WHITE flashing then back to Blue

- Does your company/org. license Azure AD?
- If yes, does your authentication policy allow “add method” including “security key”?
- Please check below links to learn how to enable security key for Azure AD:
 - <https://cloudtotal.blog/2019/07/tutorial-configure-fido2-passwordless-authentication-in-azure-ad/>
 - <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-the-public-preview-of-Azure-AD-support-for-FIDO2/ba-p/746362>
 - <https://www.bleepingcomputer.com/news/microsoft/microsoft-azure-ad-fido2-passwordless-sign-in-in-public-preview/>

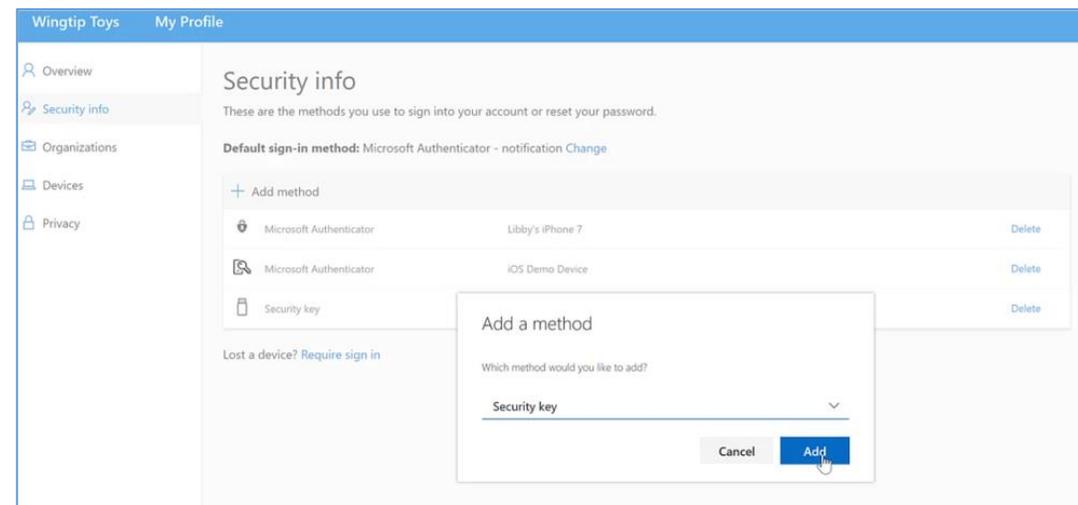
What you'll need:

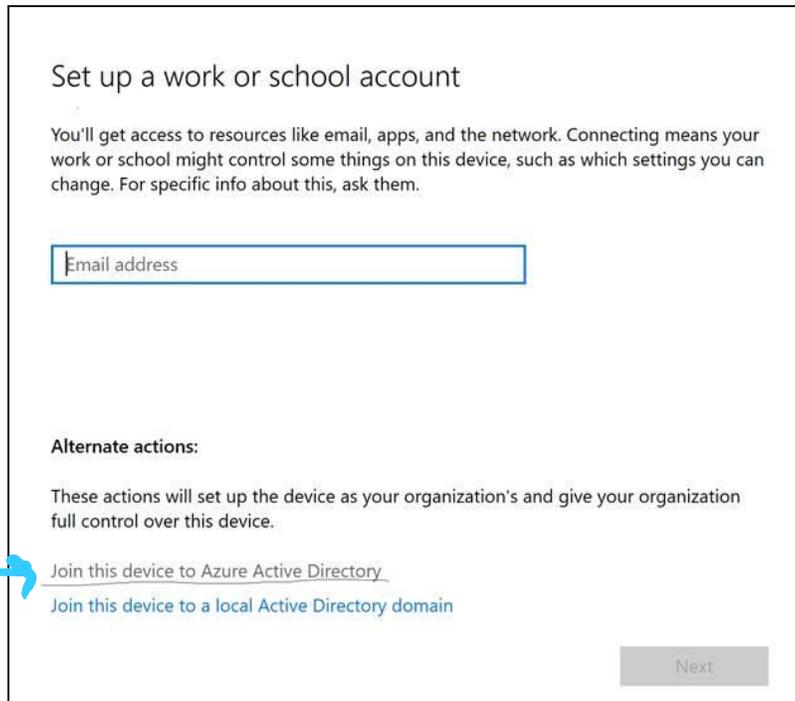
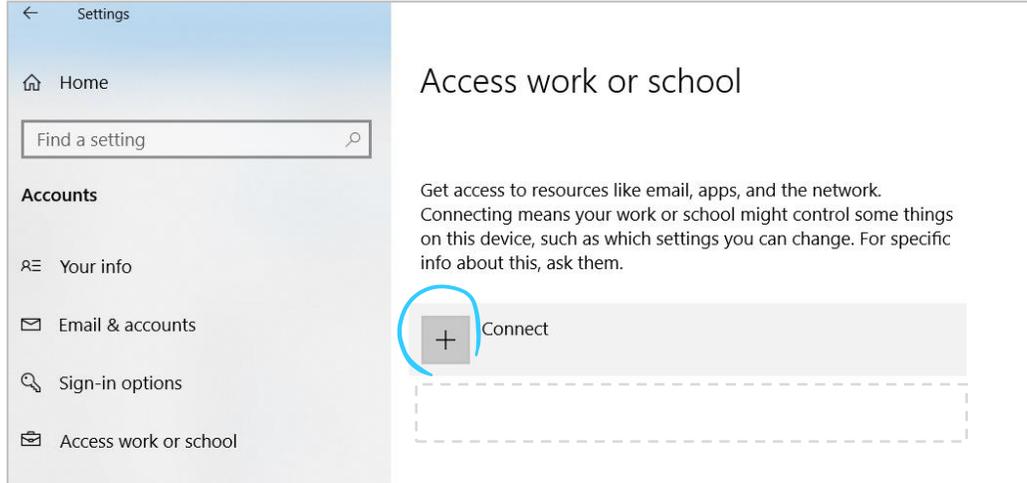
- An active Azure AD tenant which is able to leverage Azure MFA functions.
- A global admin account in Azure AD
- A test account with normal privileges in Azure AD
- ATKey.Pro - FIDO2 compatible security key.

1. A new Authentication methods blade in your Azure AD admin portal that allows you to assign passwordless credentials using FIDO2 security keys and passwordless sign-in with Microsoft Authenticator to users and groups.



2. Updated capabilities in the converged Registration portal for your users to create and manage FIDO2 security keys.

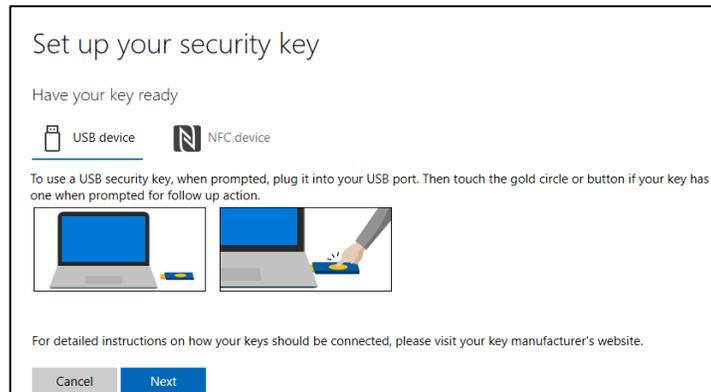




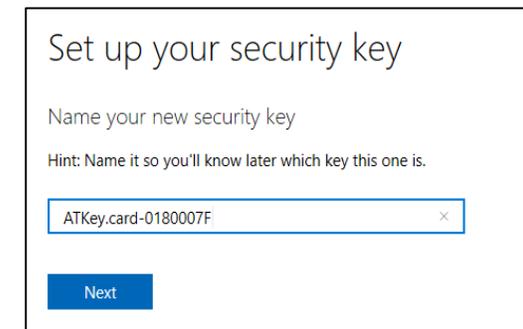
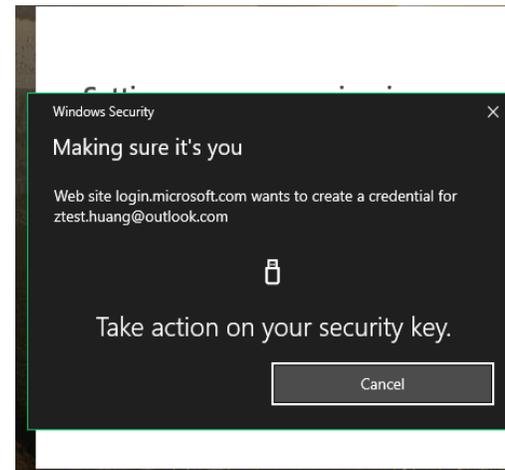
User registration and management of FIDO2 security keys

1. Browse to <https://myprofile.microsoft.com>
2. Sign in by ID/Password or app
3. Click **Security Info**
 - If the user already has at least one Azure Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
 - If they don't have at least one Azure Multi-Factor Authentication method registered, they must add one.
4. Add a FIDO2 Security key by clicking **Add method** and choosing **Security key**
5. Choose **USB device** or **NFC device**
6. Have your key ready and choose **Next**
7. A box will appear and ask you to create/enter a PIN for your security key, then perform the required gesture for your key either biometric or touch.
8. You will be returned to the combined registration experience and asked to provide a meaningful name for your token so you can identify which one if you have multiple. Click **Next**.
9. Click **Done** to complete the process

- Passwordless login Microsoft account by security key:
 - For Password-less login to Microsoft account - **Windows 10 build 1809** or later version via **Edge browser, USB** mode:
 - You can login to add ATKey.Pro as security key for your Windows account from here:
<https://account.microsoft.com/account>
 - Login by ID/Password first
 - Step by step to setup security key
 - Click “Security” from banner bar
 - Click “**more security options**” from bottom
 - From “Windows Hello and security keys” section, click “**Set up a security key**”



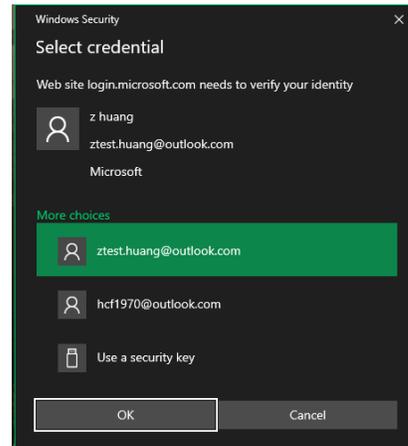
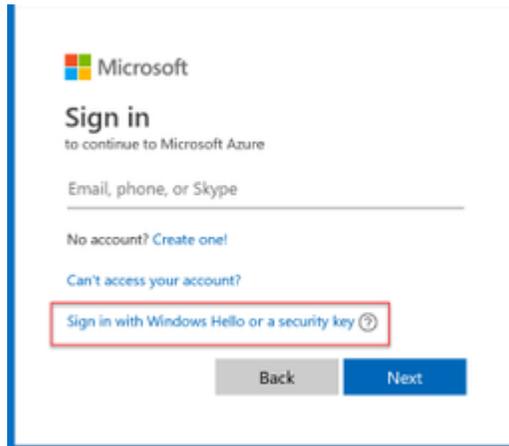
- Touch your enrolled fingerprint to verify
- Fingerprint matched, type in name of the key (default name following keycode)



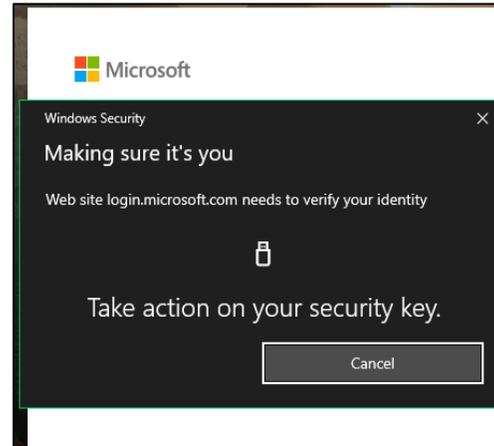
- You can find all your registered keys, click “**Manage your sign-in methods**”

Manage your sign-in methods			
NAME	SIGN-IN METHODS	ADDED ON	LAST USED
ATKey.card-0180007F	 Security key	1/16/2019 8:40 AM	1/16/2019 8:40 AM

- Sign-out to logon by security key (password-less)



Use security key



Fingerprint verified to login

- ATKey.Pro is FIDO U2F ready, it can be a security key for 2nd factor authentication.

- Here are FIDO2 U2F ready service:



- Or you can search and find available FIDO U2F certified server here: <https://fidoalliance.org/certification/fido-certified-products/?appSession=8YT7Z25V0DOH6M41OQG26WI22NOF6D5MF9W19F58545OZWKJPBOH5XMB874A6596S8432G491GGF12B5Y7PIAM6PKR09S5G9Z3Q9TOFLK91C5445079DO1NWZFP8714Q>

- **But, Chrome browser only**

- **Google:**

- Turn on 2-Step Verification, <https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en>
- Use a security key for 2-Step Verification, <https://support.google.com/accounts/answer/6103523?co=GENIE.Platform%3DAndroid&hl=en>

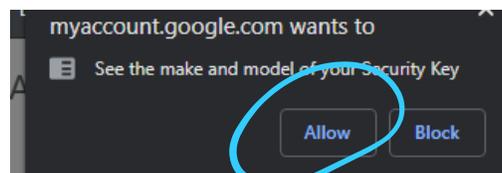
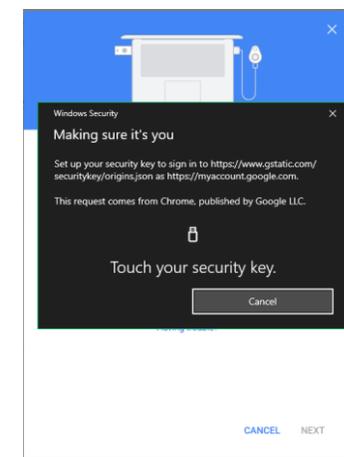
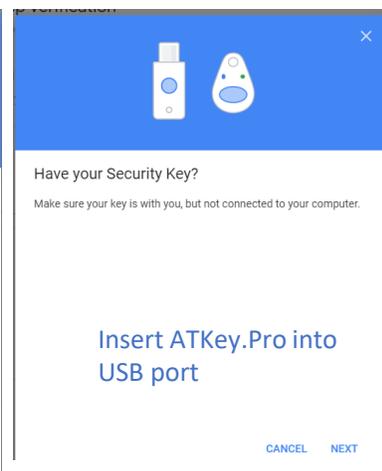
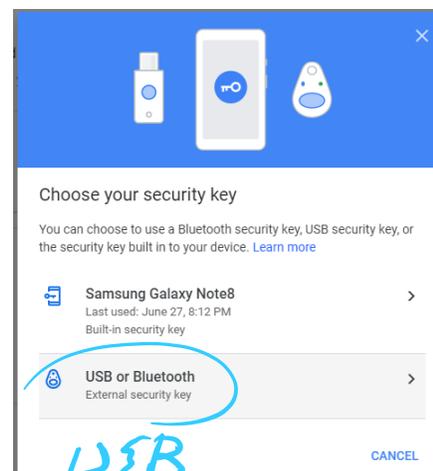
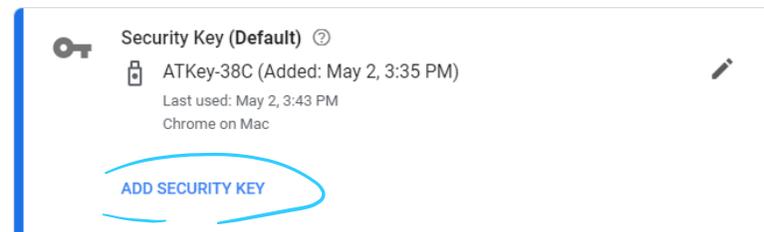
- **Facebook:** <https://www.facebook.com/help/148233965247823>

- **Gitlab:** Enable 2FA via U2F device, https://docs.gitlab.com/ee/user/profile/account/two_factor_authentication.html

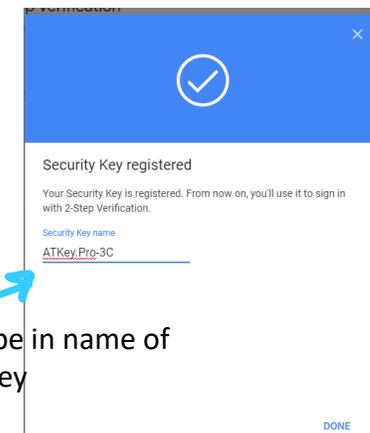
- **Salesforce:** https://help.salesforce.com/articleView?id=security_u2f_enable.htm&type=5

- **Dropbox:** <https://help.dropbox.com/teams-admins/team-member/enable-two-step-verification>

- **(e.g.) Google account – add ATKey.Pro as security to Google account:**



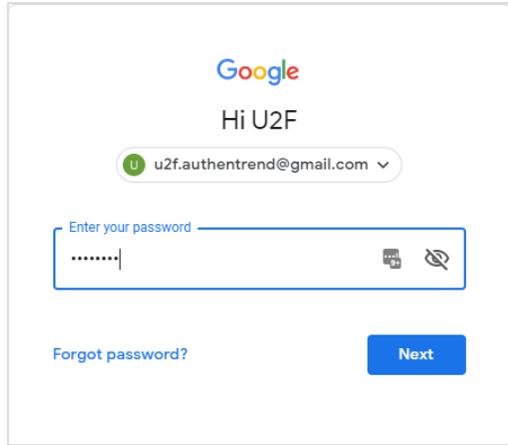
Click "Allow"



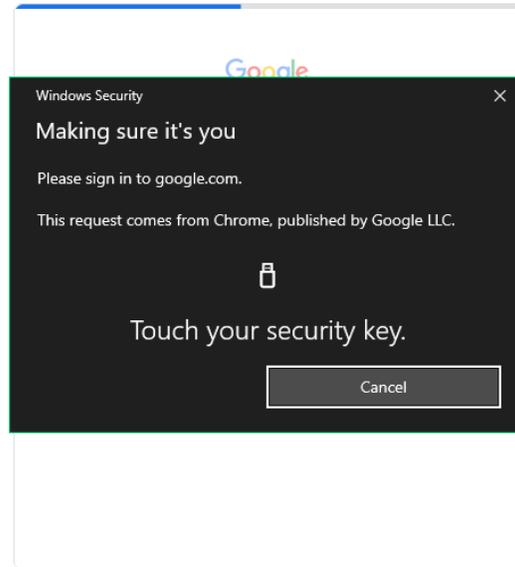
Ready, type in name of security key

Touch enrolled fingerprint to verify

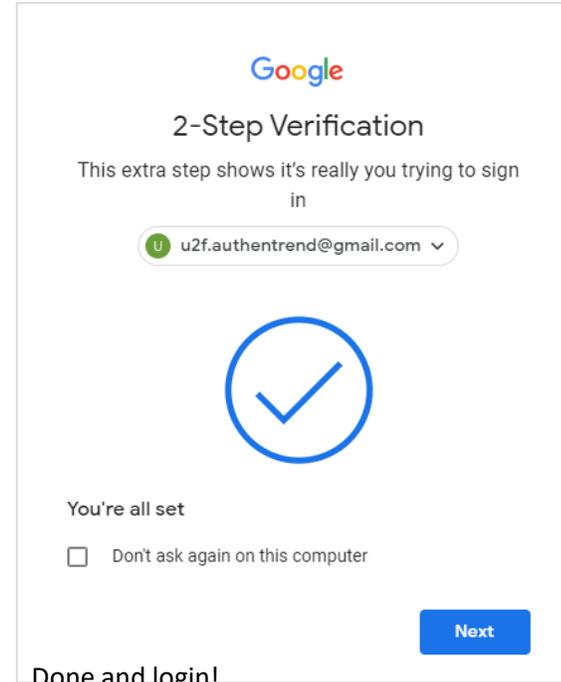
- (e.g.) Google account – login via ATKey.Pro



1st factor: ID and password still



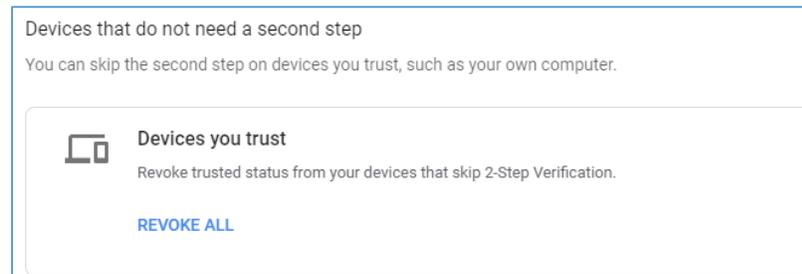
2nd factor: verify your enrolled fingerprint



Done and login!

If you want to login your google account with ATKey.Pro later, please uncheck "Don't ask again on this computer" (default is checked).

But if you checked and login, but you want to use ATKey.Pro as 2nd factor to login again, please revoke all "device you trust" as below:





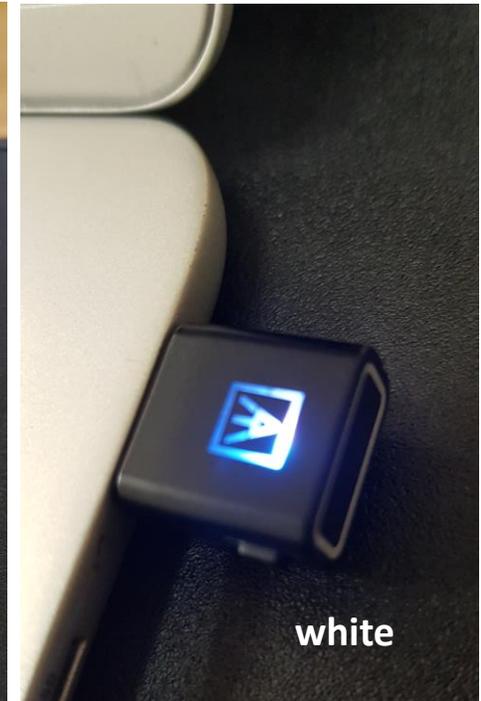
blue



green



red



white

<p>Flashing</p>	<p>Touch enrolled fingerprint to verify</p>			<p>Standalone enrollment (flashing from slow to fast, then done by GREEN meaning enrolled fingerprint verified PASS)</p>
<p>Static ON</p>	<p>Power on, normal state</p>	<p>Fingerprint verified PASS (for a second)</p>	<ul style="list-style-type: none"> • Fingerprint verified Failed (for 1 second) • Erase fingerprint or reset key 	<ul style="list-style-type: none"> • Fingerprint sensor calibration • Power on, but firmware booting failed

Certification

In recognition of Authentrend's achievement of FIDO2® Certification

Company: Authentrend
Product: ATKey.Pro
Specification: FIDO2
Specification Version: 2.0 (2018-07-02)
Implementation Class: Authenticator
Level: L1
Functional Policy Version: 1.3.7
Authenticator Policy Version: 1.1.1
Security Requirements Version: 1.3
Interoperability Date: September 10th, 2019
Conformance Self-Validation Date: September 9th, 2019
VQ Approval Date: October 8th, 2019
Derivative: No
Source Certificate(s): N/A

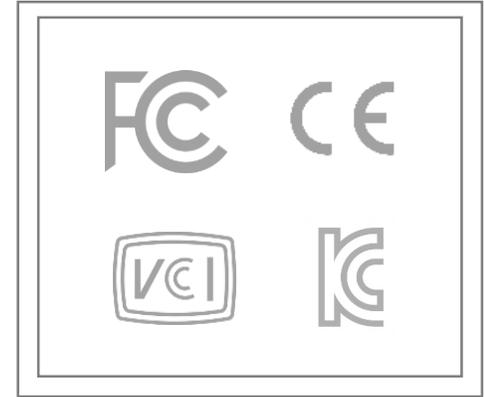


Certificate No.

FIDO20020191008001

Issued

October 8th, 2019



THANK YOU!

 www.authentrend.com

 contact@authentrend.com

 [AuthenTrend](#)

 [AuthenTrend](#)

AUTHENTREND