



FIDO2 Fingerprint Security Key



Slimmest, Compact, Best fingerprint experience

- * Fingerprint Enabled USB Dongle for U2F and FIDO2
- * USB HID Device
- * Broadcom Secure SoC (FIPS 140-2 Level3 Certificate) with SecureBoot & SecureXIP Enabled
- * Patented Standalone Enrollment
- * Up to 10 Fingerprints
- * Bio-Safe™

A vertical line with circles at the top, bottom, and at the 'App' and 'FIDO' sections. The 'App' and 'FIDO' labels are positioned to the left of the line, aligned with their respective groups of items.

	About ATKey.Pro	Page 3
	Outlook	Page 4
	Functionalities	Page 5
	Fingerprint Enrollment	Page 6
	Windows Settings	Page 7
App	App – ATKey for Windows	Page 9
	Non – Windows 10 Users	Page 11
	Windows Hello	Page 14
FIDO	FIDO2 : Azure AD	Page 16
	FIDO2 : Microsoft Account	Page 18
	Bio-Safe™	Page 22
	Fingerprint Highlights	Page 24
	LED	Page 25

Fingerprint enabled USB security key

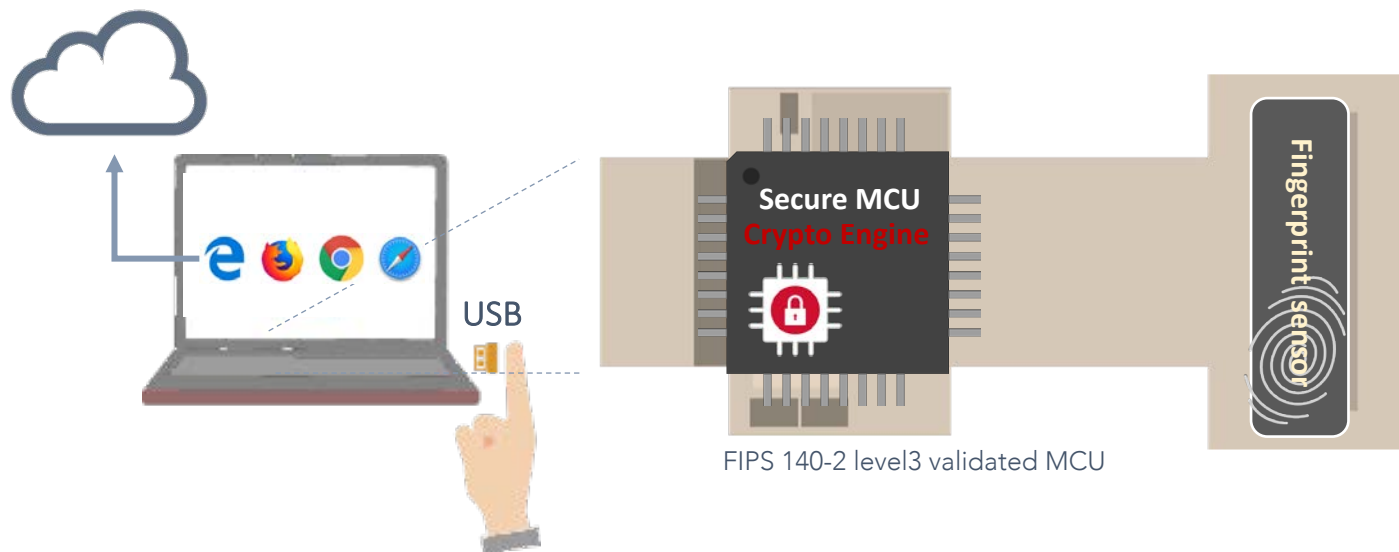
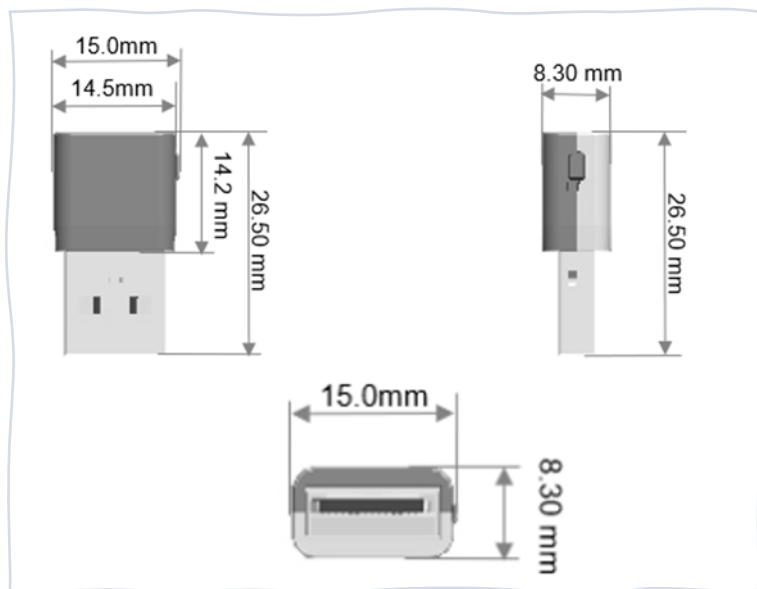
- HID device, no driver needs
- Portable key for any Windows, Mac or Chromebook
- Up to 10x fingerprints, matching < 1 sec., FAR < 1/50,000, FRR < 2 %
- FIDO2 certificate



I Outlook



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



▶ Please visit this following video for below 3 steps: <https://youtu.be/-9ZCtPG-1J0>

Step 1

Enroll Fingerprint to ATKey



Standalone Enrollment (Patent Filing) <https://youtu.be/IDrcZxWXAL4>
 or through Windows Settings (build 1903)
 or through "ATKey for Windows" app

Step 2

Register ATKey to Device or Service

FIDO2

FIDO U2F

Windows Hello (option)

OTP (option)

Bio-Safe™ (firmware is $\geq 1.0.9$)

Step 3

Fingerprint Matching for Authentication

Azure AD Passwordless logon

<https://youtu.be/Q1CylOa8IV8>

Passwordless login Microsoft account or other FIDO2 authentication via Browsers on Windows, Mac and Chromebook

You can find FIDO security key readiness services from here: <https://www.dongleauth.info/>

Login Google, Facebook, Dropbox, Salesforce, Gitlab via Chrome browser as 2nd factor

Windows Logon (via CDF)

* If your Windows joined Azure AD, don't enable this one

2FA via OTP

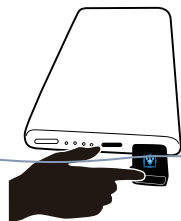
* This is only for customization projects or customers

<https://youtu.be/sM30S7yknHE>



Standalone Enrollment

No device or app required.

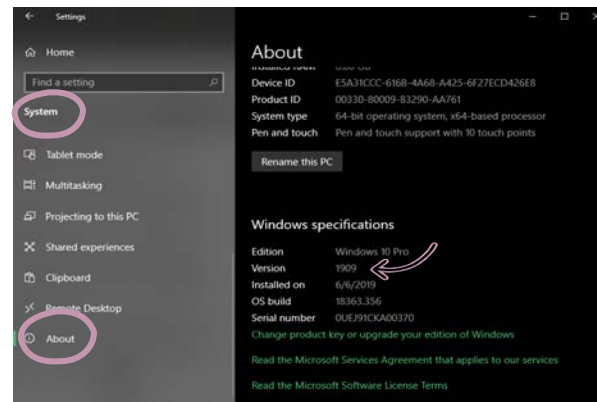


- Insert ATKey.Pro into USB port
- Check YouTube video here for the detail:
https://www.youtube.com/watch?v=uoSf_B9hTY8
- LED is BLUE ON, quick click side-button 3x times to get into enrollment mode:
 - If there is no any fingerprint enrolled, LED turns to WHITE.
 - If there are any enrolled fingerprints, 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.

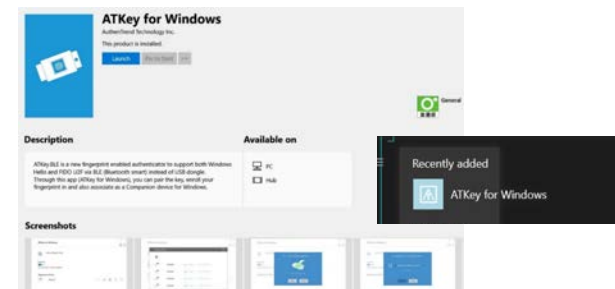


Enroll from Windows Settings

- 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
- If you are not Windows 10 build 1903 or later versions (Mac, Chromebook, Linux, ...), you can do standalone enrollment, or [using Chrome Canary to enroll and manage fingerprints.](#)
- Windows Settings => System => About

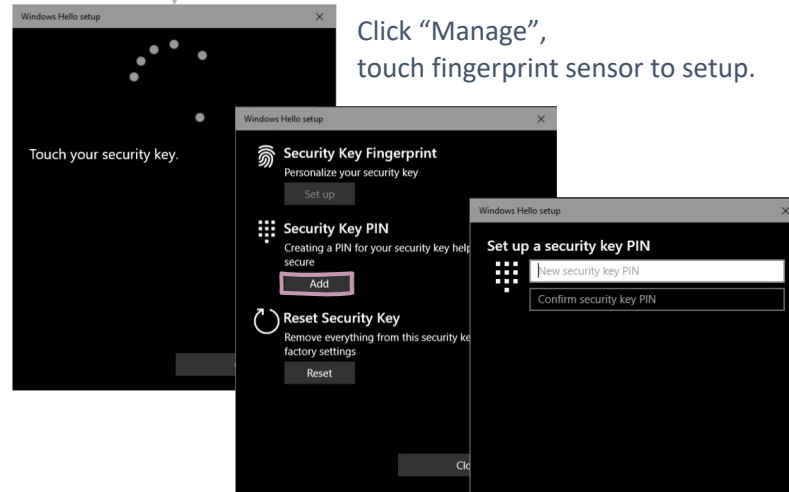
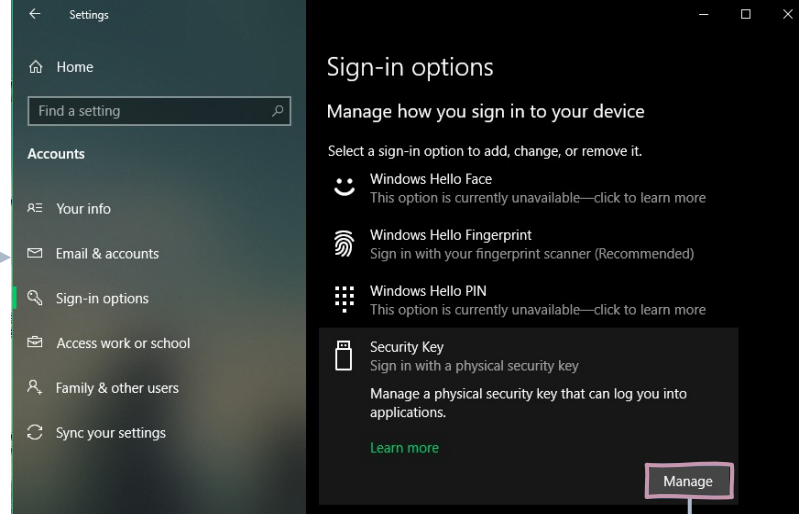
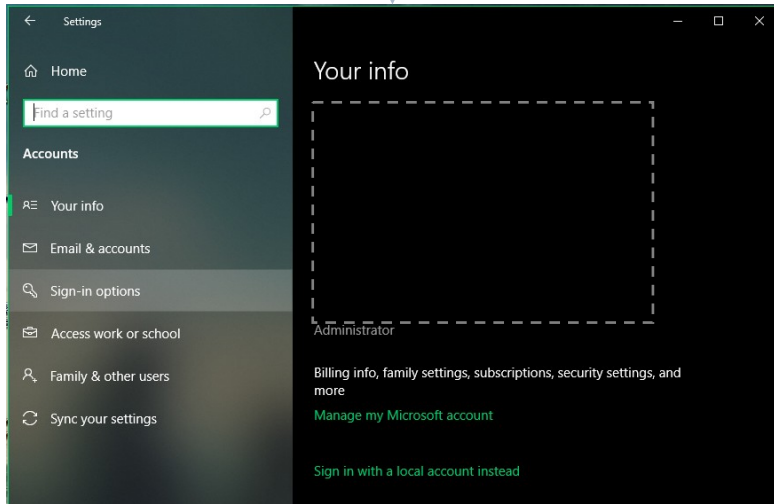
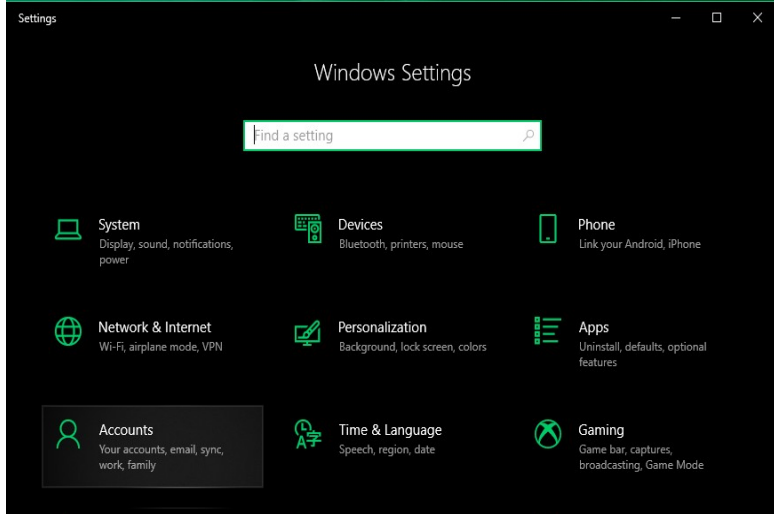


ATKey for Windows App

- 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)
 - Search “ATKey” or “AuthenTrend” from Windows Store to find the app, download and install.
- 
- Jump to [“ATKey for Windows” for the detail](#)



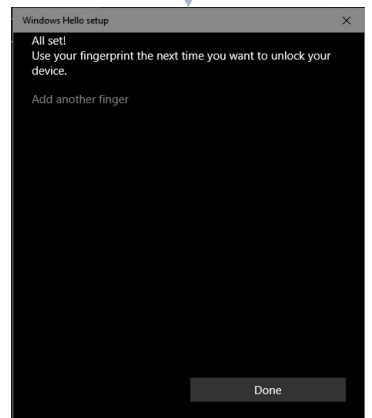
Windows Settings => Account => Sign-in Options => Security Key => Add "PIN Code" and Enroll "Fingerprints"



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

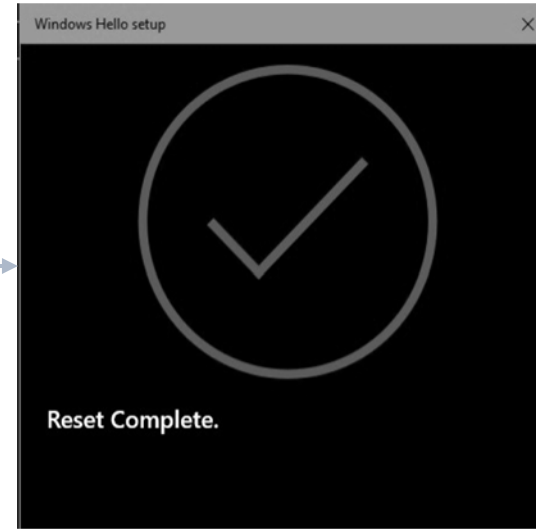
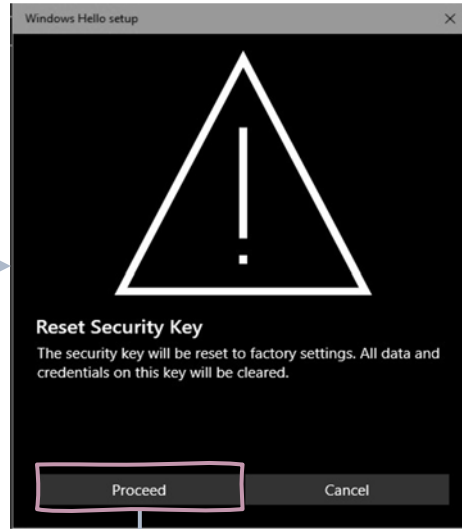
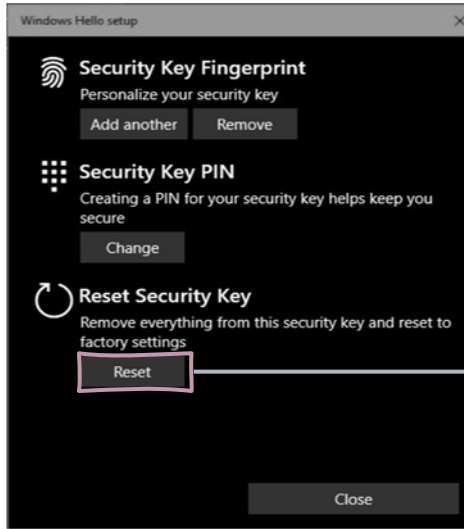


- Setup "Security Key Fingerprint"
- Type-in PIN code, following screen hint to enroll fingerprint til "All Set!"





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



Click "Process"

[Firmware 1.00.6 or later version]

1. Cyan LED is flashing
2. **Remove ATKey.Pro and re-insert to USB port**
3. Cyan LED is flashing
4. **Touch by any finger** to reset or cancel it - please make it done (Reset) within 10 sec

[Firmware 1.00.5 or previous version]

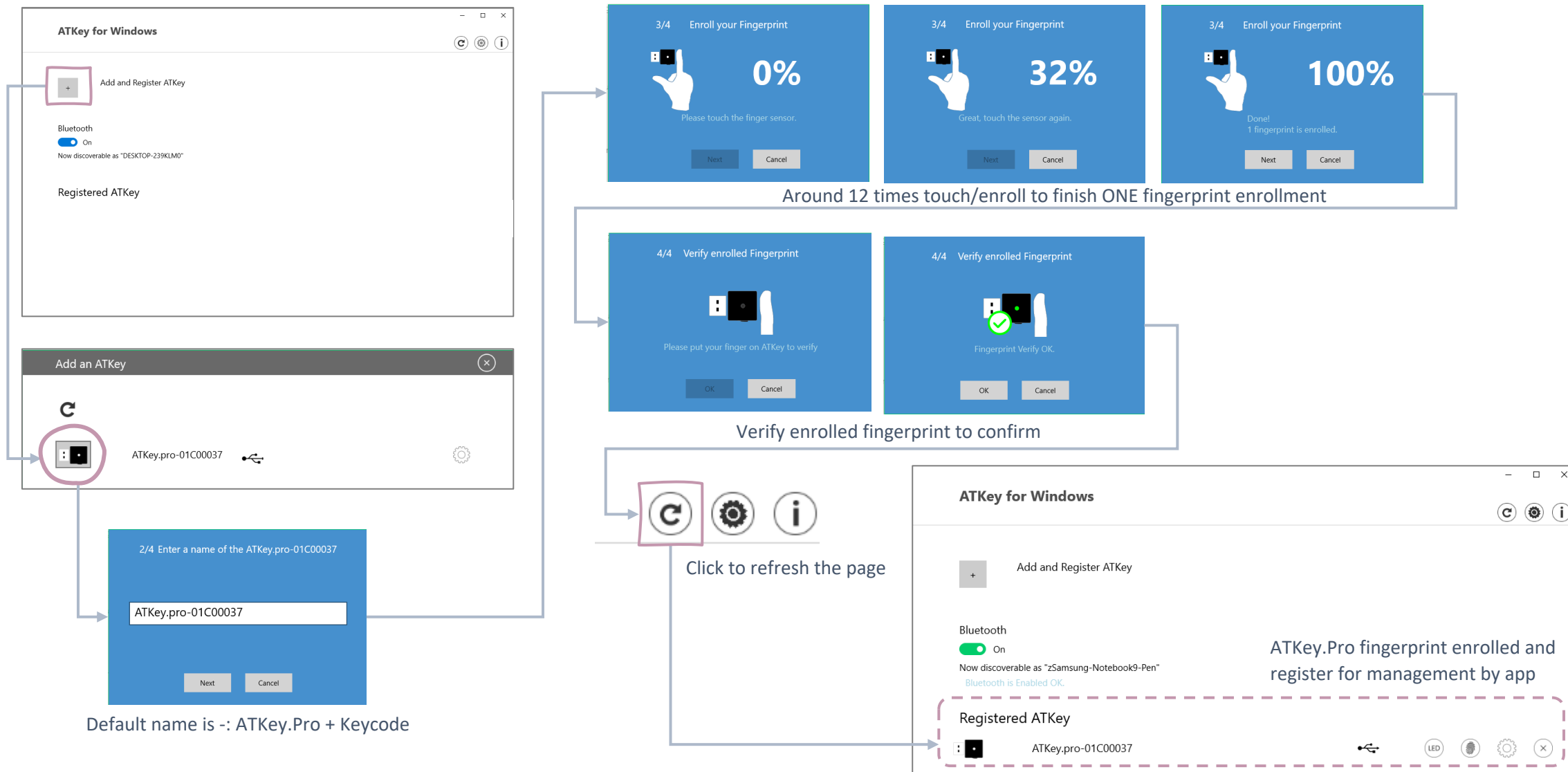
1. Blue LED is flashing
2. **Remove ATKey.Pro and re-insert to USB port**
3. Blue LED is flashing
4. Touch by any finger to reset or cancel it - please make it done (Reset) within 10 sec

Microsoft required spec.- for authenticator reset: in order to prevent accidental trigger of this mechanism, user presence is required. In case of authenticators with no display, request MUST have come to the authenticator within 10 seconds of powering up of the authenticator.

I App "ATKey for Windows" – Enroll Fingerprint

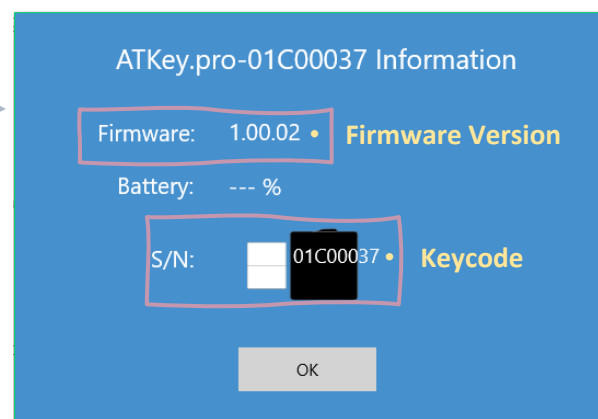
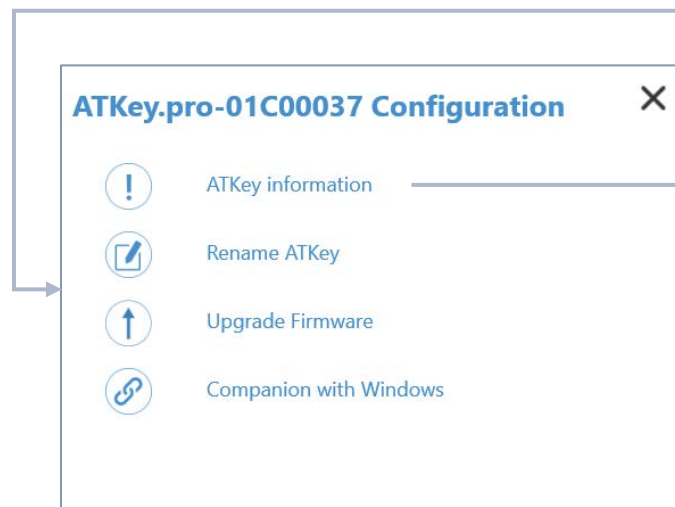
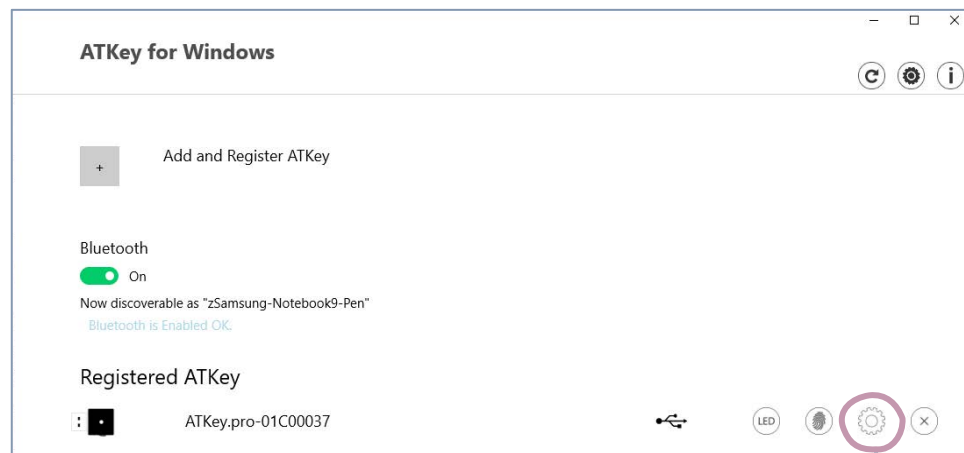


- Launch "ATKey for Windows" app (version 2.0.57.0 or later version)
- Click "Add and Register ATKey" – please make sure ATKey.Pro inserts to USB port and LED shows blue ON



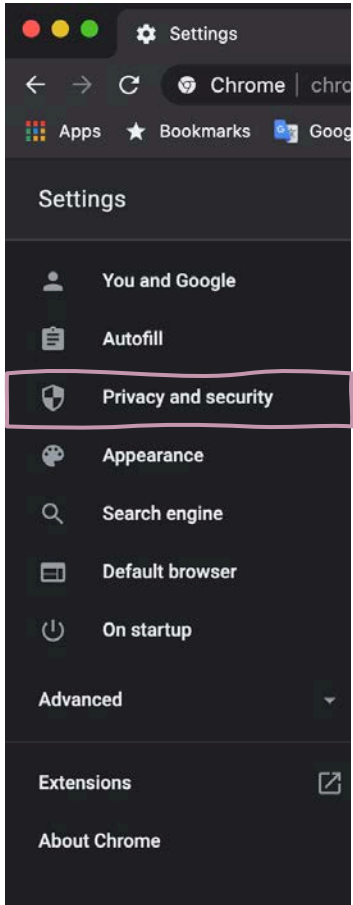


ATKey management – information, rename

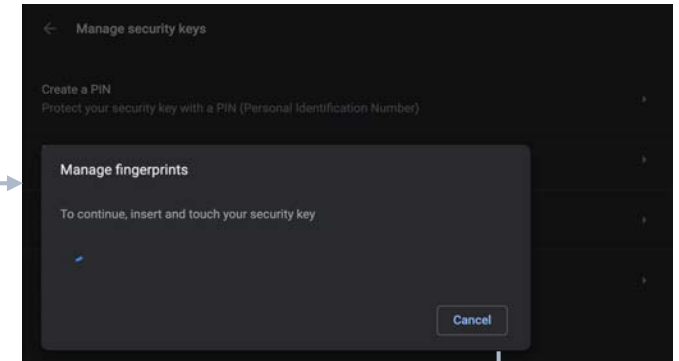
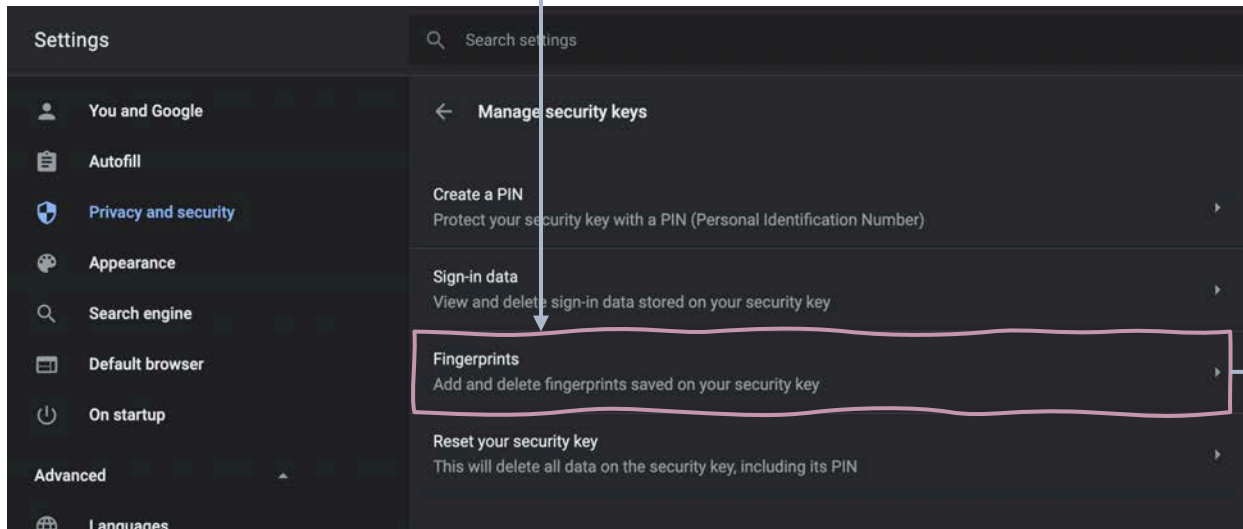
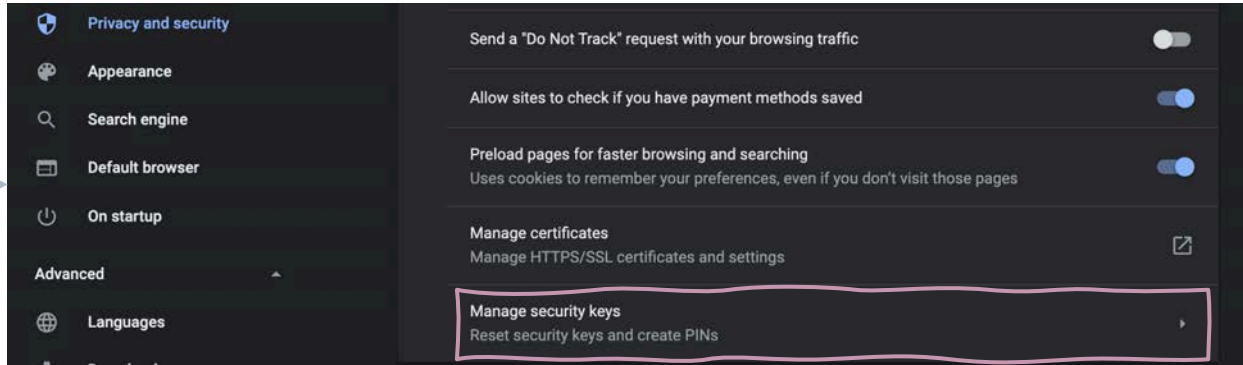




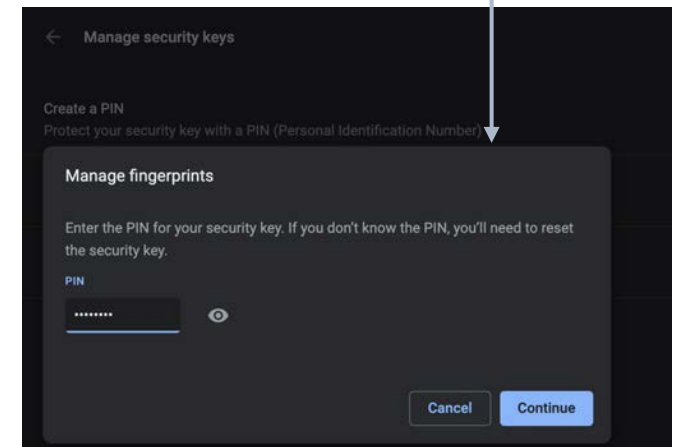
- If you are using non-Windows 10, or your Windows 10 is earlier than build 1903
 - Enroll fingerprint into ATKey.Pro via
 - [Standalone Enrollment](#)
 - Or Chrome Canary (<https://www.google.com/chrome/canary/>)



From "Settings" => "Privacy and security"



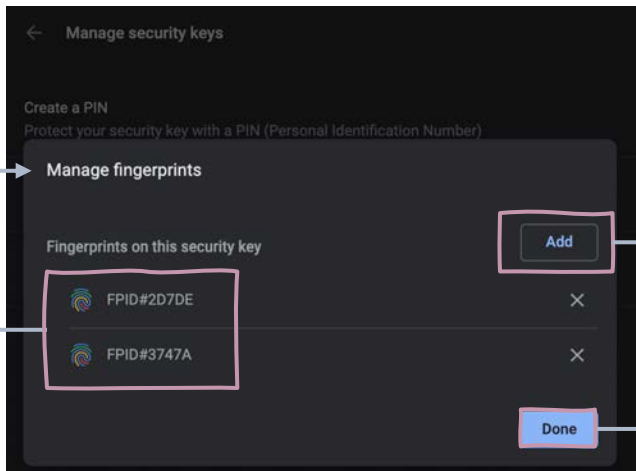
User presence needs - touch dongle by any finger



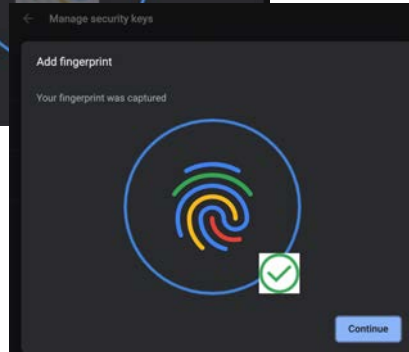
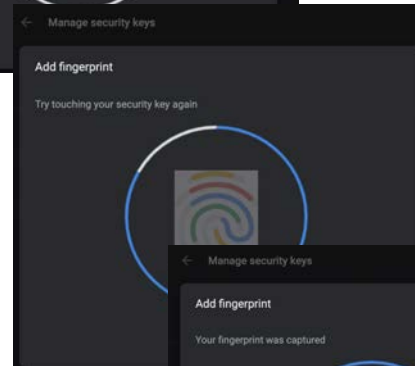
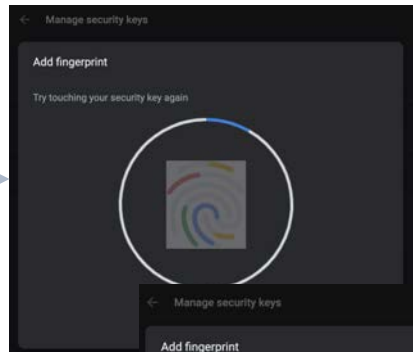
Assign PIN code into the key



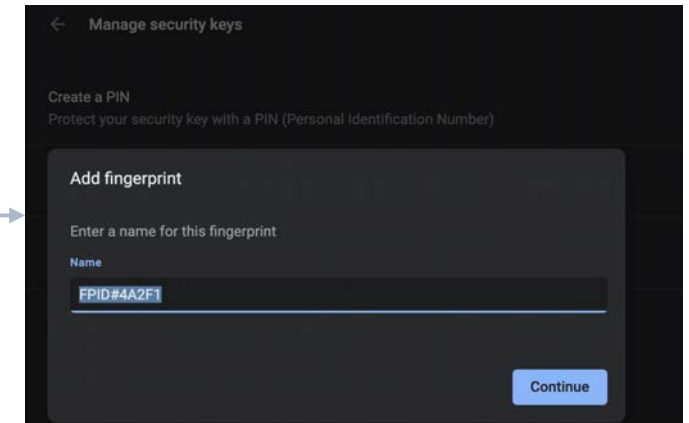
- If you are using non-Windows 10, or your Windows 10 is earlier than build 1903
 - Enroll fingerprint into ATKey.Pro via
 - [Standalone Enrollment](#)
 - Or Chrome Canary (<https://www.google.com/chrome/canary/>)



- Click "Add" to fingerprint (enroll new finger)
- Here lists enrolled fingerprints with assigned names



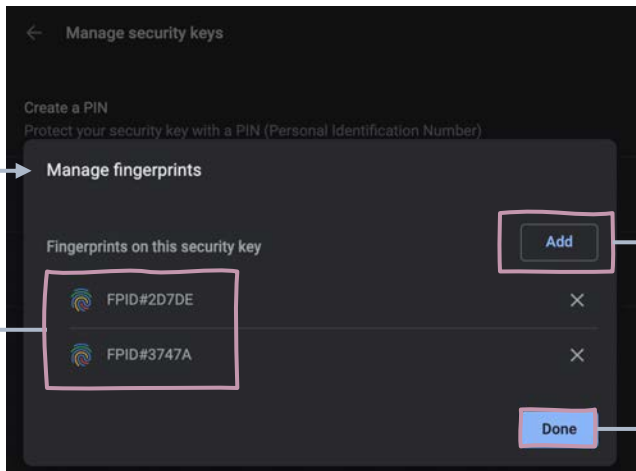
Enroll fingerprint till it's done



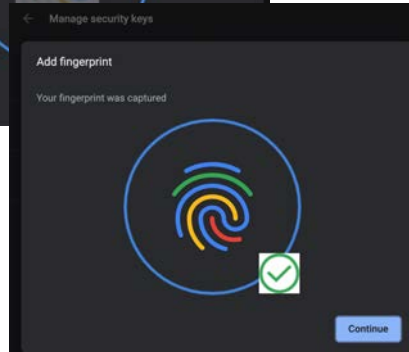
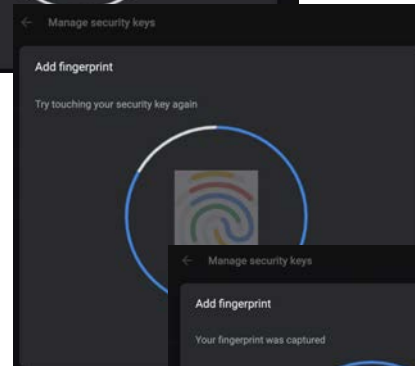
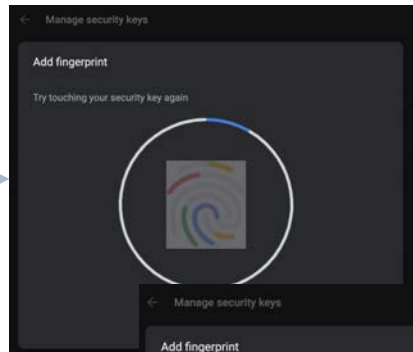
Assign the name of the enrolled fingerprint



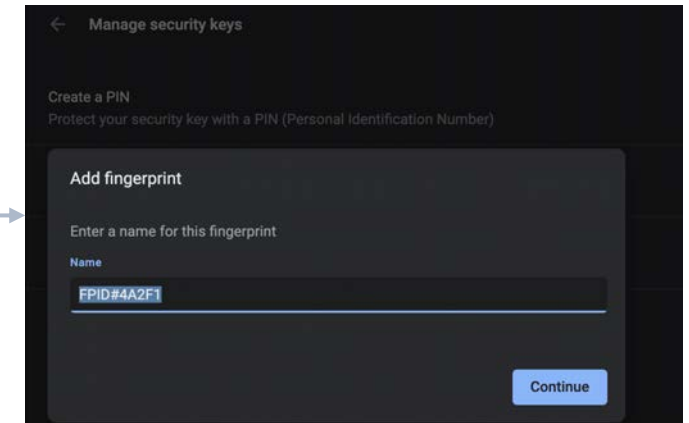
- If you are using non-Windows 10, or your Windows 10 is earlier than build 1903
 - Enroll fingerprint into ATKey.Pro via
 - [Standalone Enrollment](#)
 - Or Chrome Canary (<https://www.google.com/chrome/canary/>)



- Click "Add" to fingerprint (enroll new finger)
- Here lists enrolled fingerprints with assigned names



Enroll fingerprint till it's done



Assign the name of the enrolled fingerprint

I App "ATKey for Windows" – Windows Hello

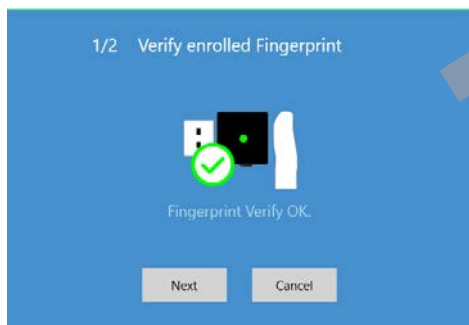
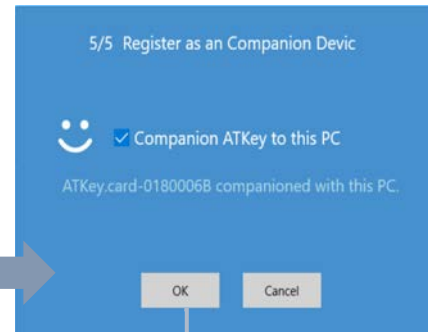
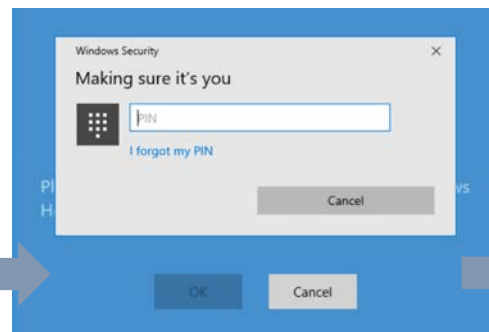
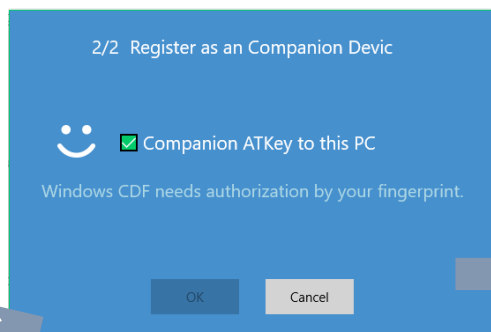
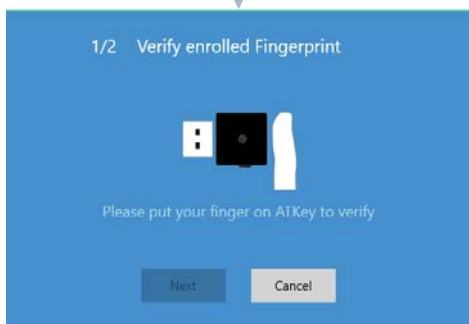


- ATKey management – Companion with Windows (Windows Hello login via CDF)
- *If your Windows 10 joined Azure AD, please ignore this page since FIDO2 supports Azure AD login.*

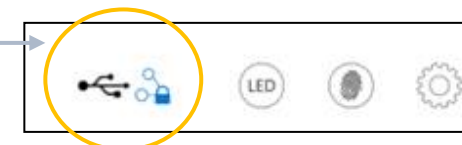


Guidelines for Windows Hello:

- [Windows Unlock with Windows Hello companion devices](#)
- [How to Enable or Disable users to use Companion device to sign in to Windows 10](#)
- [Enable or disable Domain users to sign in with PIN to Windows 10](#)



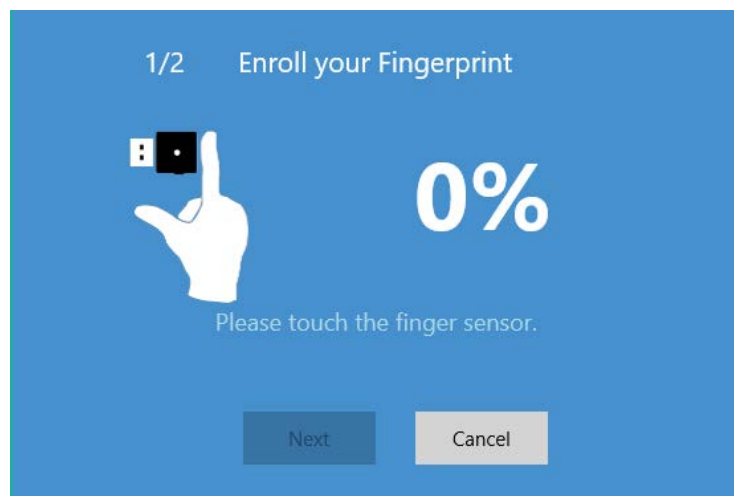
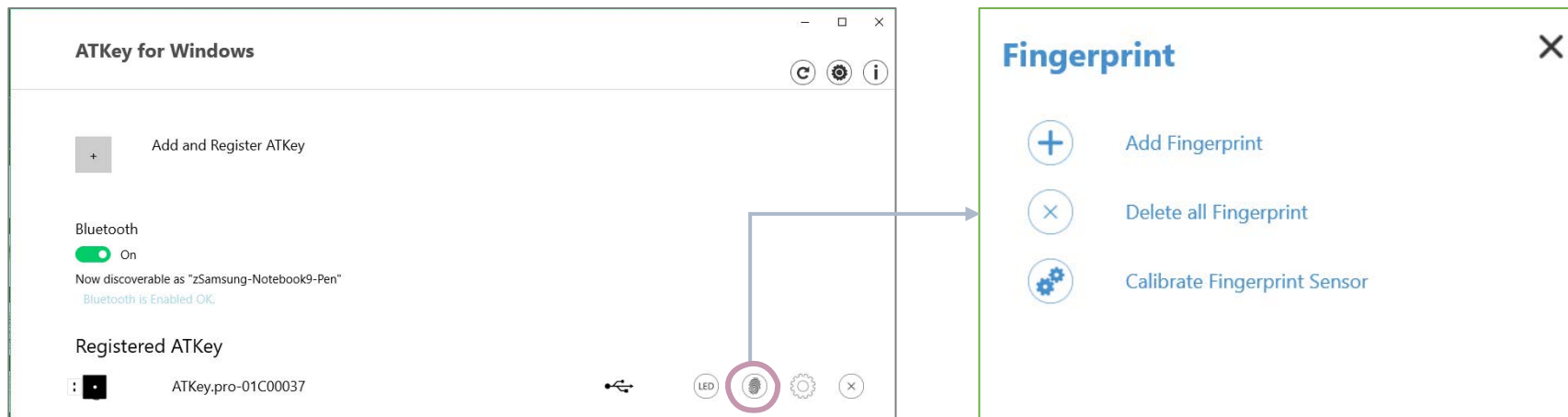
- **Type in "Windows Hello PIN" to allow the companion;**
- *Some Corp. or Org. may disable this group policy by IT Admin, if you saw the message, please contact your IT.*



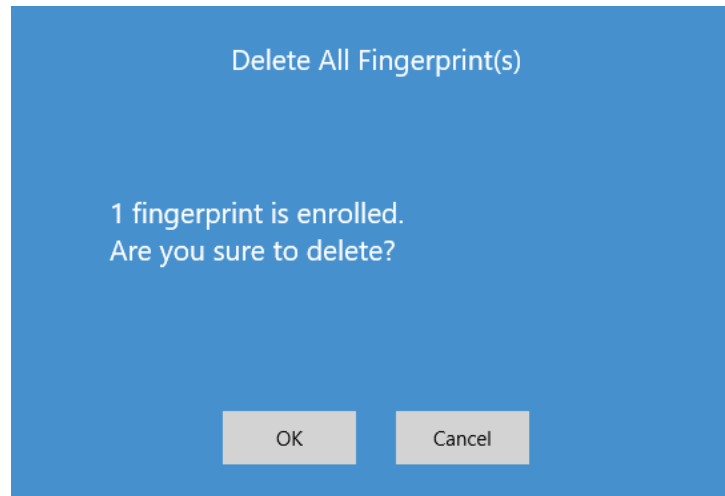
This icon means it's a companion key for Windows Hello via CDF (Companion Device Framework)



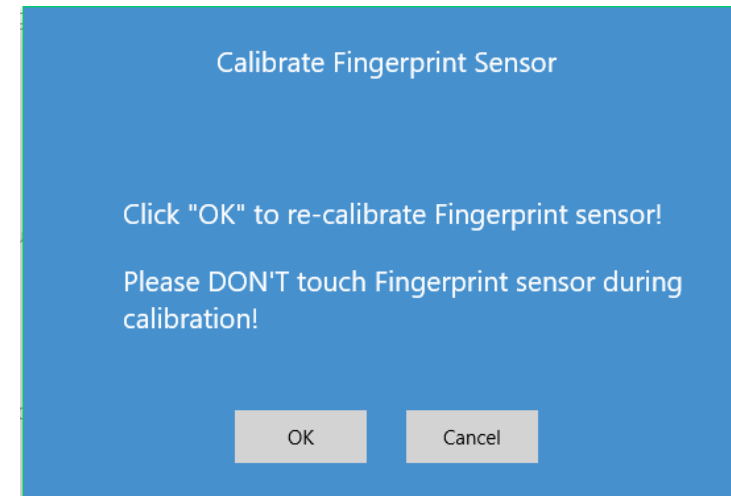
ATKey management – Add/Delete fingerprints, fingerprint sensor calibration



- 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.

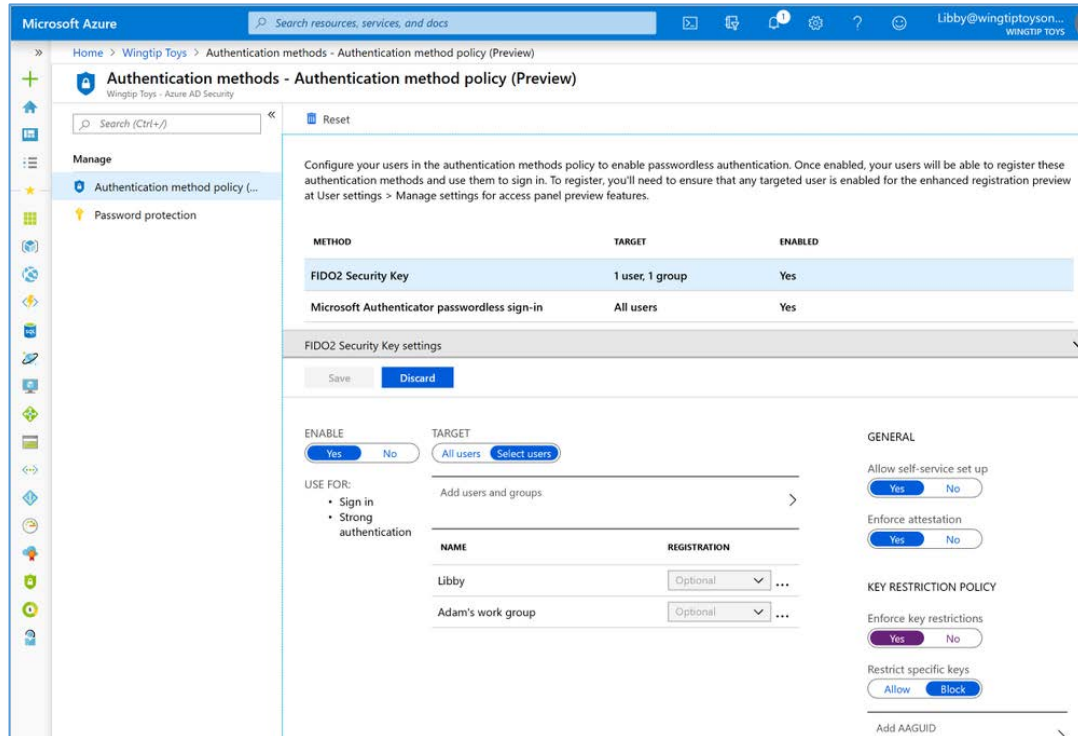


- If you feel something wrong of fingerprint, doing Calibration to re-calibrate the sensor
- **Don't put your finger on during calibration; LED will be WHITE flashing then back to Blue**

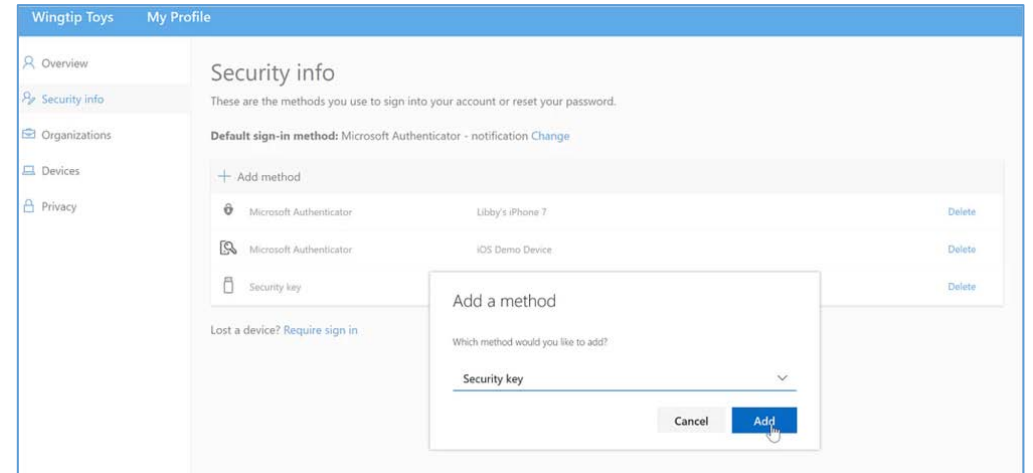
I ATKey for Azure AD Passwordless Login (Admin-Backend)

- 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:
 - [Passwordless Security Keys](#)
 - [Passwordless Windows 10](#)
 - [Passwordless On-premises](#)
 - [Passwordless authentication options – 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.



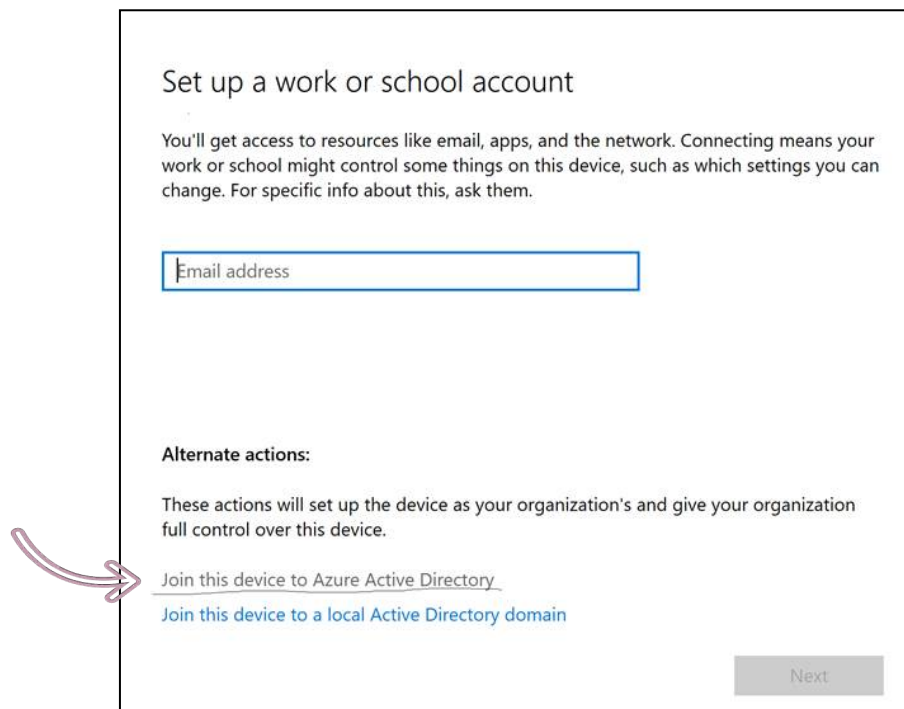
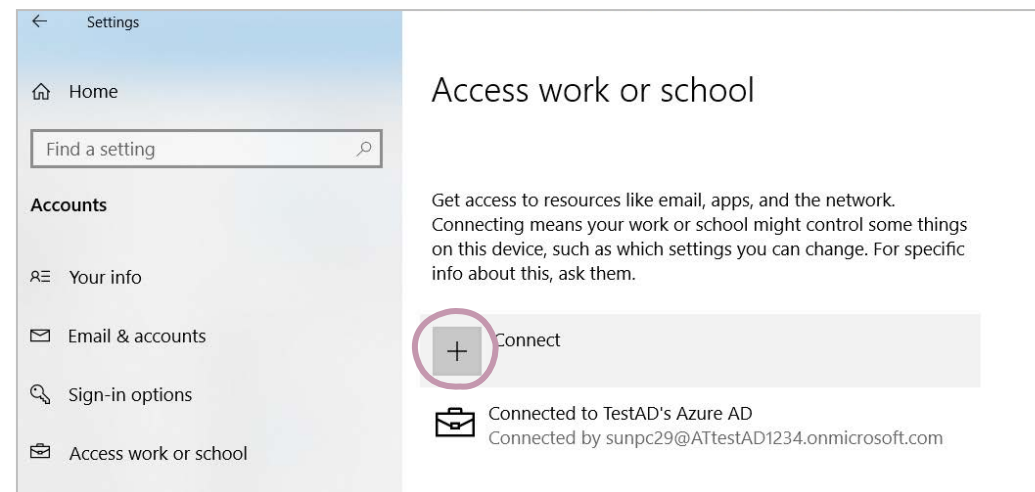
2 Updated capabilities in the converged Registration portal for your users to [create and manage FIDO2 security keys](#).





User registration and management of FIDO2 security keys

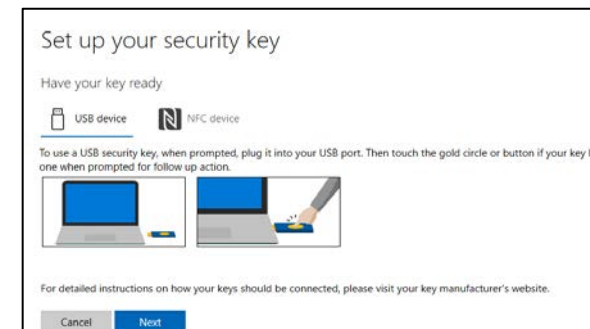
1. Browse to <https://myprofile.microsoft.com>
2. Sign in by ID/Password or app
3. Click **Security Info**
 - If the user already has at least one Azure Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
 - If they don't have at least one Azure Multi-Factor 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:

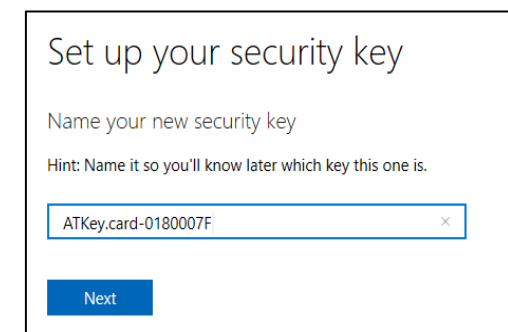
- For Password-less login to Microsoft account - **Windows 10 build 1809** or later version via **Edge/Chrome browser, USB** mode:
 - You can login to add ATKey.Pro as security key for your Windows account from here: <https://account.microsoft.com/account>
 - Login by ID/Password first
 - Step by step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



- 4) Touch your enrolled fingerprint to verify



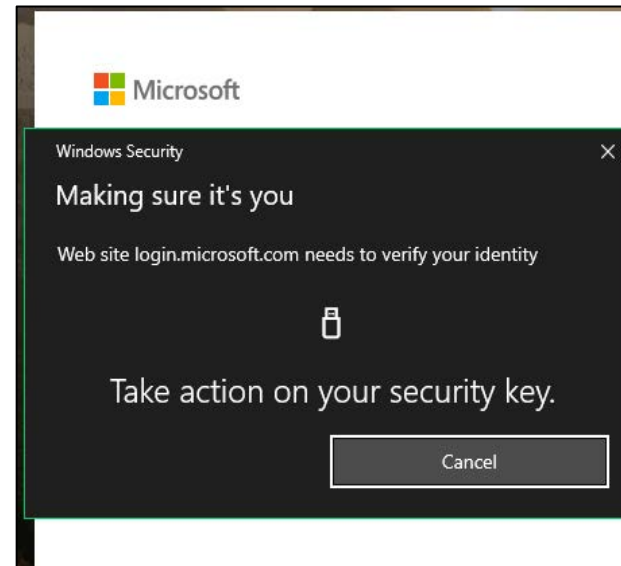
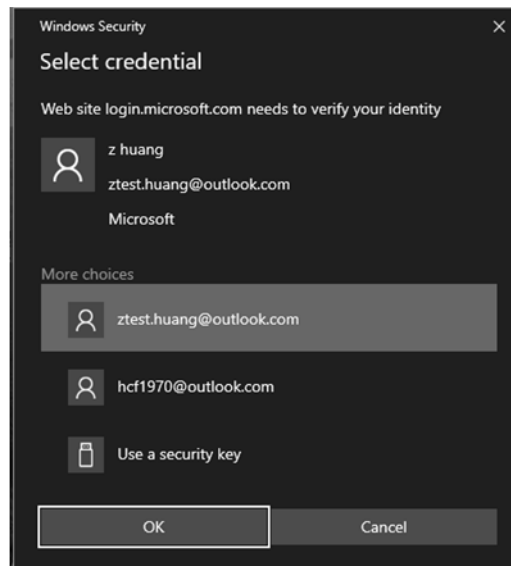
- 5) Fingerprint matched, type in name of the key (default name following keycode)



▶ You can find all your registered keys, click "Manage your sign-in methods"

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 login by security key (password-less)





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=8YT7Z25V0DOH6M41OQG26WI22N0F6D5MF9W19F58545OZWKJPBOH5XMB874A6596S8432G491GGF12B5Y7PIAM6PKR09S5G9Z3Q9T0FLK91C5445079DO1NWZFP8714Q>

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,

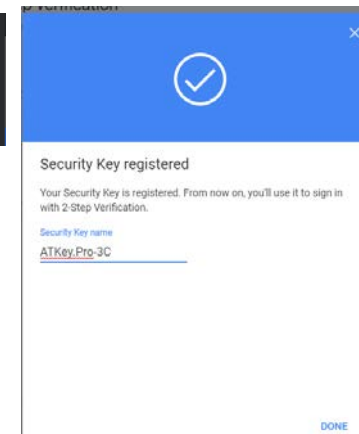
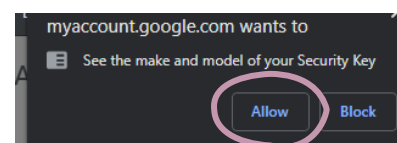
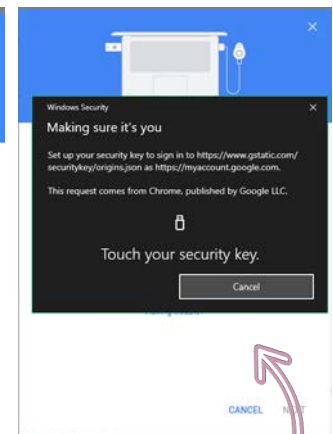
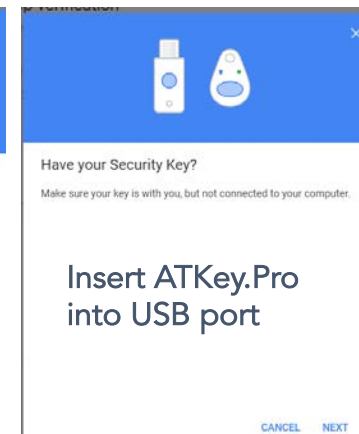
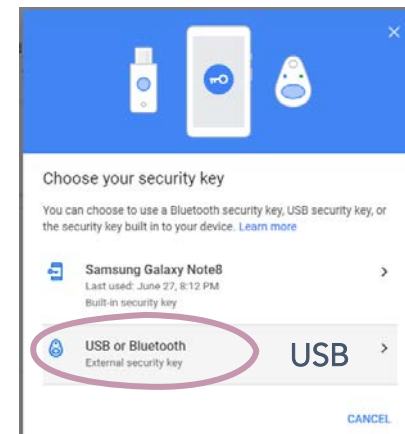
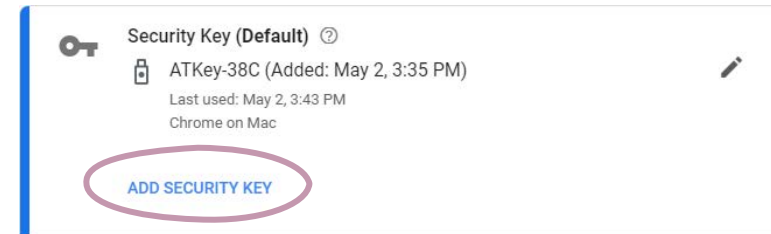
https://docs.gitlab.com/ee/user/profile/account/two_factor_authentication.html

Salesforce:

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

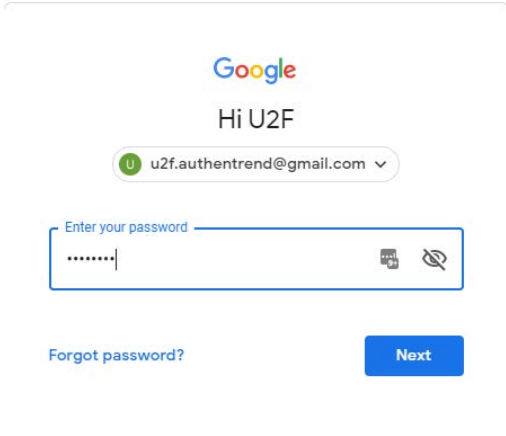
Dropbox: <https://help.dropbox.com/teams-admins/team-member/enable-two-step-verification>

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

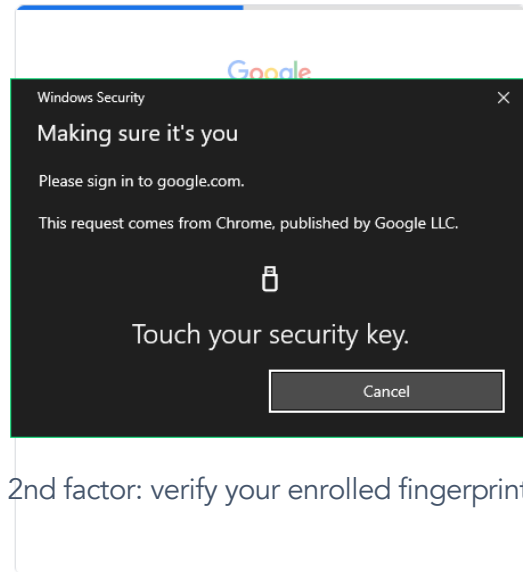


Touch enrolled fingerprint to verify

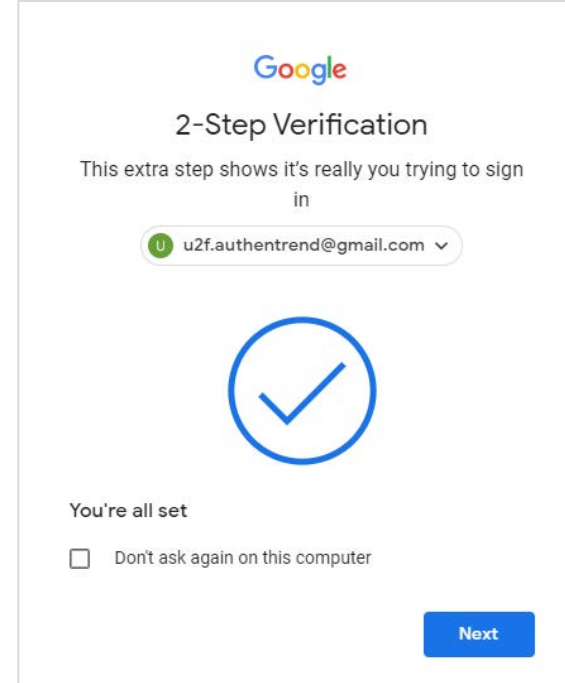
- (e.g.) Google account – login via ATKey.Pro



1st factor: ID and password still



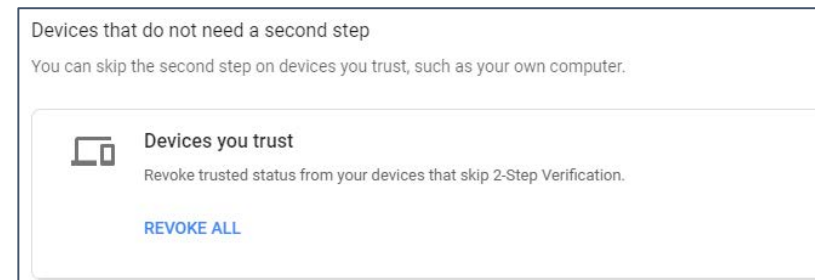
2nd factor: verify your enrolled fingerprint

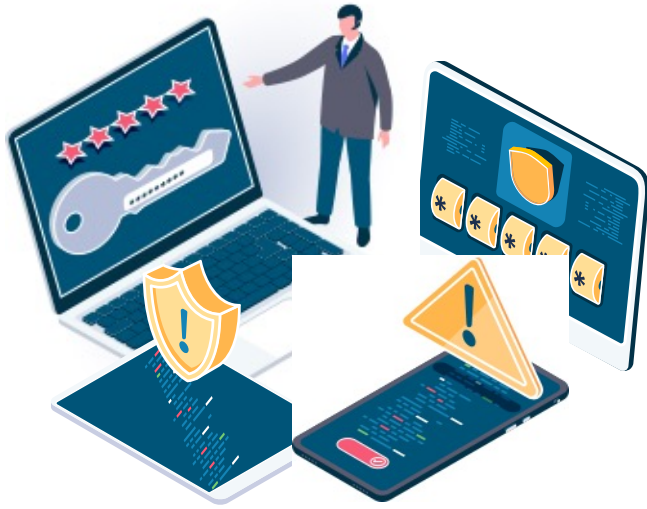


Done and Login!

*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:





Too many credentials (ID and passwords) for your different kind of web services.



Take notes or leverage password management SaaS to store them on 3rd party cloud

But is it secure?



Partner with Broadcom to provide Bio-Safe™ to encrypted and store credentials into ATKey.Pro instead of public cloud; login web services via fingerprint matching, secure and convenience.

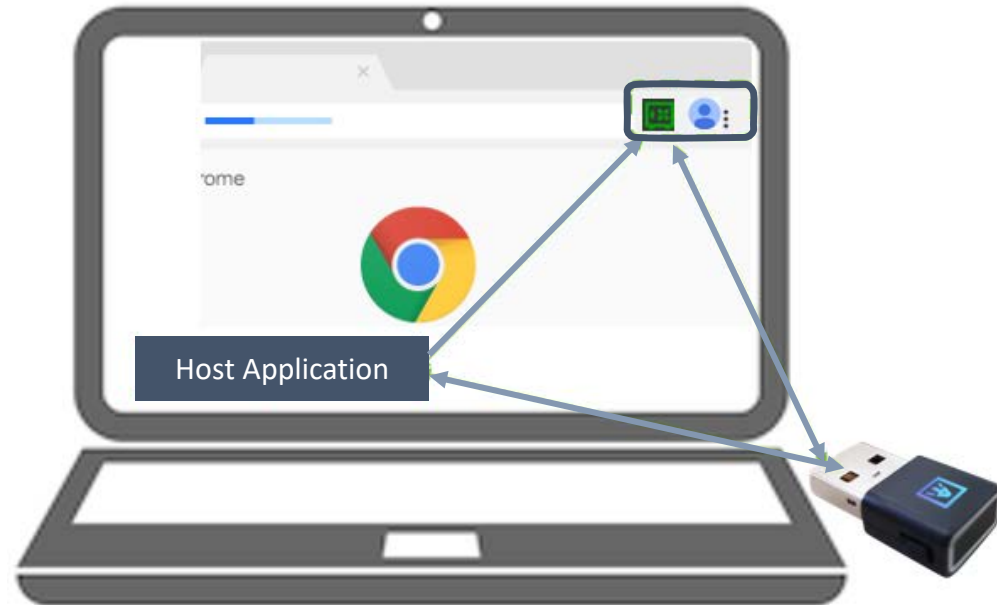


Please check or download user steps to setup Bio-Safe™ with ATKey.Pro:
https://www.authentrend.com/download/ATKey.Pro_Bio-Safe_user_steps.pdf

- **Before start, please make sure below things are ready:**
 - Check your ATKey.Pro's firmware is 1.00.9 or later version
 - ATKey.Pro is ready with fingerprint enrolled

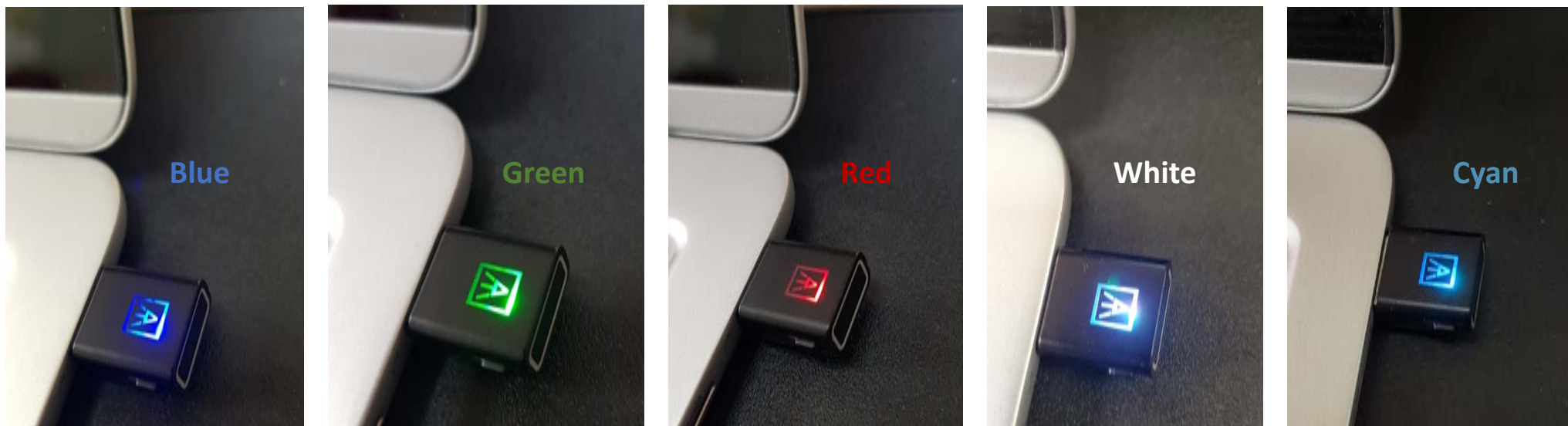


Here is the detail user guide:
<https://docs.broadcom.com/docs/BIO-SAFE-UG>





- Up to 10x fingerprints, when it's full (10x fingerprints), user can't enroll new fingers in.
- For new fingerprint enrollment, it always needs authorization from enrolled fingerprints (verify by enrolled fingerprint first).
- For fingerprint enrollment, users need to touch sensor continuously around 12 times to complete the "template".
- Following FIDO2 spec., adding PIN code into ATKey.Pro is preferred; user can add PIN code into ATKey.Pro through Windows Settings (1903 or later builds) or adding from ATKey for Windows (2.0.58.0 or later version)
- Following FIDO2 spec., it allows 3 times continuous failure during one "cycle" (LED will be static RED), user needs to remove the dongle from Host and re-insert for another cycle; if it fails 5 cycles continuously, Key will re-format and reset.



Flashing	Touch your enrolled fingerprint to verify			Standalone enrollment (flashing from slow to fast, then done by GREEN meaning enrolled fingerprint verified PASS); Fingerprint calibration (white flashing, done back to blue)	User touch needs (but any finger is ok)
Static ON	Power on, normal state	Fingerprint verified PASS (for a second)	<ul style="list-style-type: none"> • Fingerprint verified • Failed • Erase fingerprint • Reset key 	<ul style="list-style-type: none"> • Fingerprint sensor calibration • Power on, but firmware booting failed 	

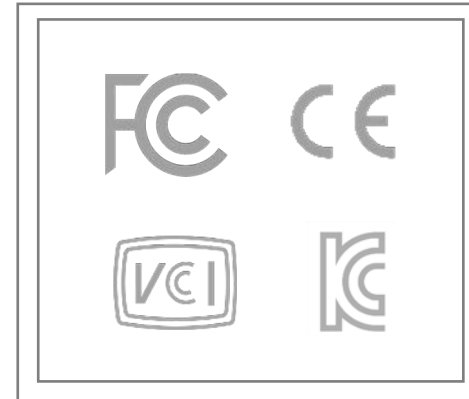
Certification

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