

AUTHTREND

-The trend of Authentication-

Quick Guide for ATKey with RSA SecurID Access

Rev. 1.0



RSA SECURID® ACCESS

MODERN AUTHENTICATION FOR
TODAY'S IDENTITY CHALLENGES

The diagram illustrates the integration of various authentication methods with RSA SecurID Access. On the left, a box labeled "Admin Token" contains an icon of a hand holding a smartphone displaying "123 123" and the text "Enables you to test hard and soft tokens." To the right, a blue USB security key is shown above the "ATKey.Pro" logo. Below the USB key is the "fido CERTIFIED FIDO2" logo. At the bottom right, a white card with a fingerprint scanner and the "ATKey.Card" logo is shown.

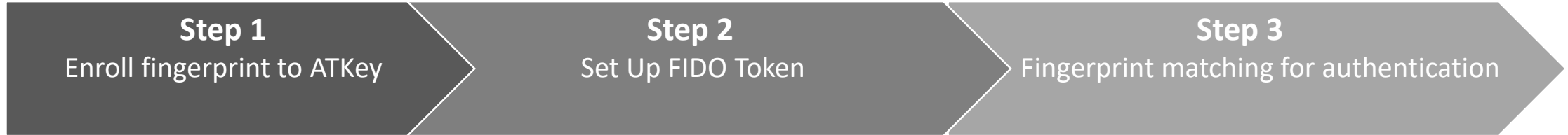
RSA SecurID Access supports using FIDO2-Certified and U2F-compliant security keys - *ATKey.Card (USB/BLE/NFC) and ATKey.Pro (USB)* as an authentication option.

Fingerprint enabled USB security key

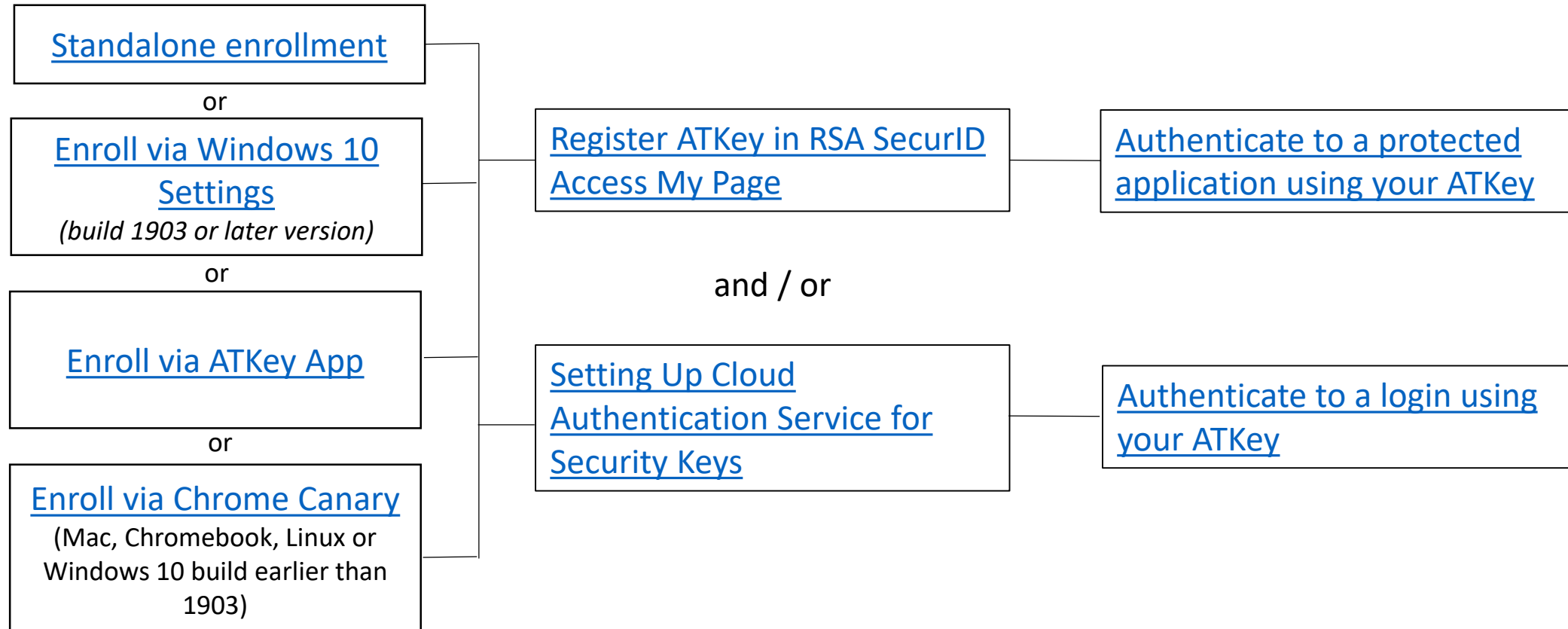
- HID device, no driver needs
- Portable key for any Windows, Mac or Chromebook
- Up to 10x fingerprints, matching < 1 sec., FAR < 1/50,000, FRR < 2 %
- FIDO2 certificate



 **KEY**.Pro
<https://authentrend.com/atkey-pro/>



Please enroll your fingerprint first!!



Standalone enrollment

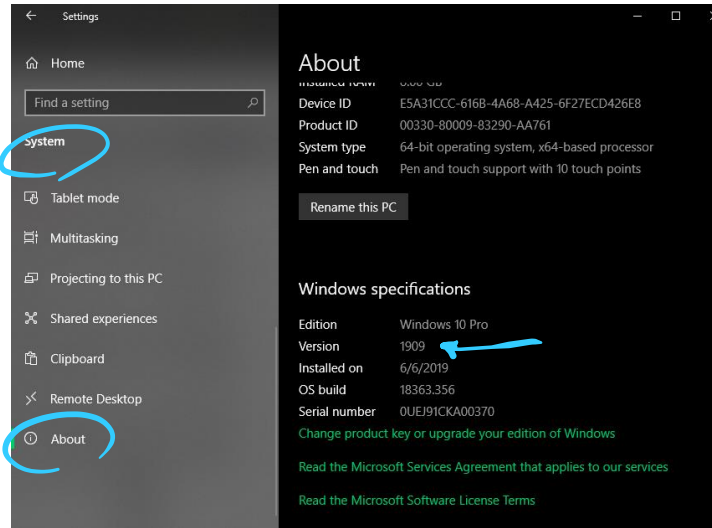
- Insert ATKey.Pro into USB port
- Check Youtube video here for the detail: <https://youtu.be/IDrcZxWXAL4>
- LED is BLUE ON, quick click side-button 3x times (by nail) to go into enrollment mode:
 - If there is no any fingerprint enrolled, LED turns to WHITE
 - If there are any enrolled fingerprints, 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.

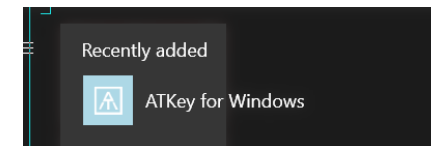
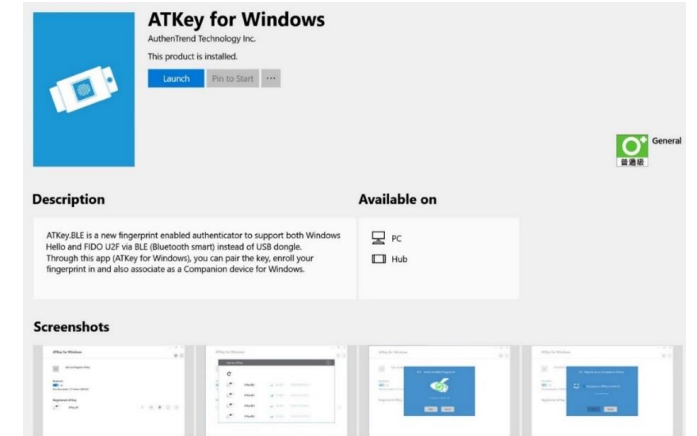
Enroll from Windows Settings

- 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



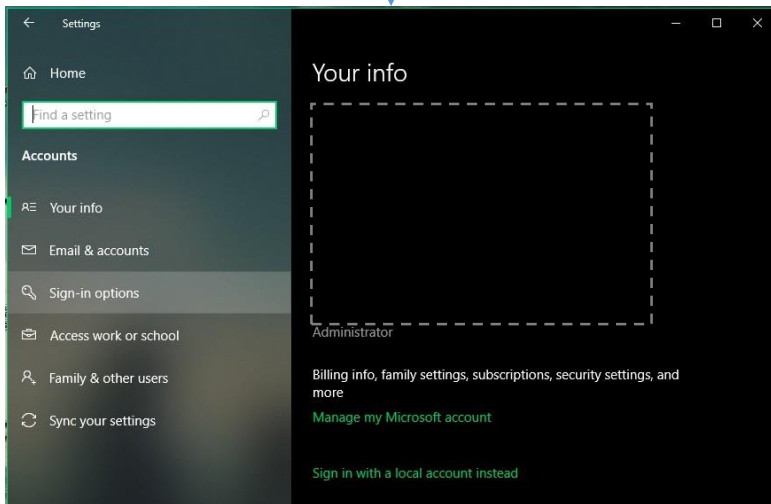
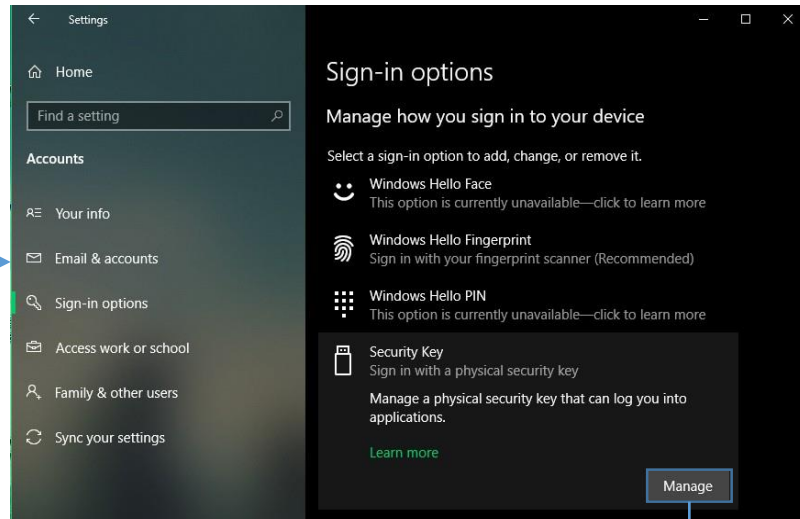
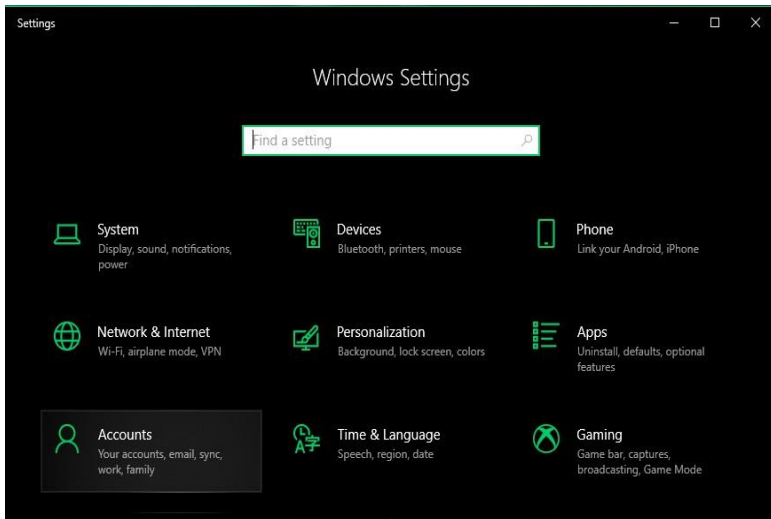
Enroll from ATKey for Windows app

- 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](#)

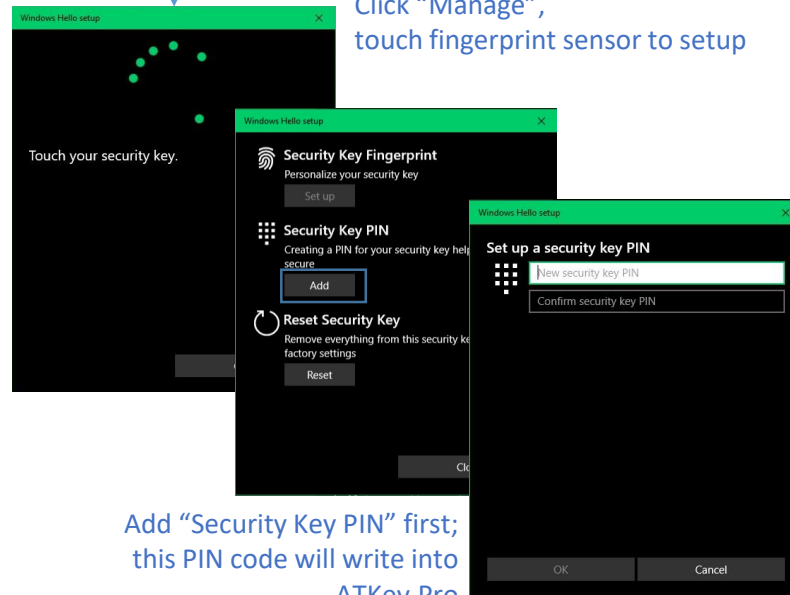
- Windows Settings => Account => Sign-in options => Security Key => add **“PIN code”** and enroll **“Fingerprints”**



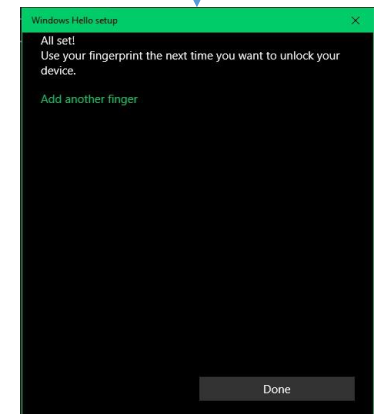
Click “Manage”, touch fingerprint sensor to setup



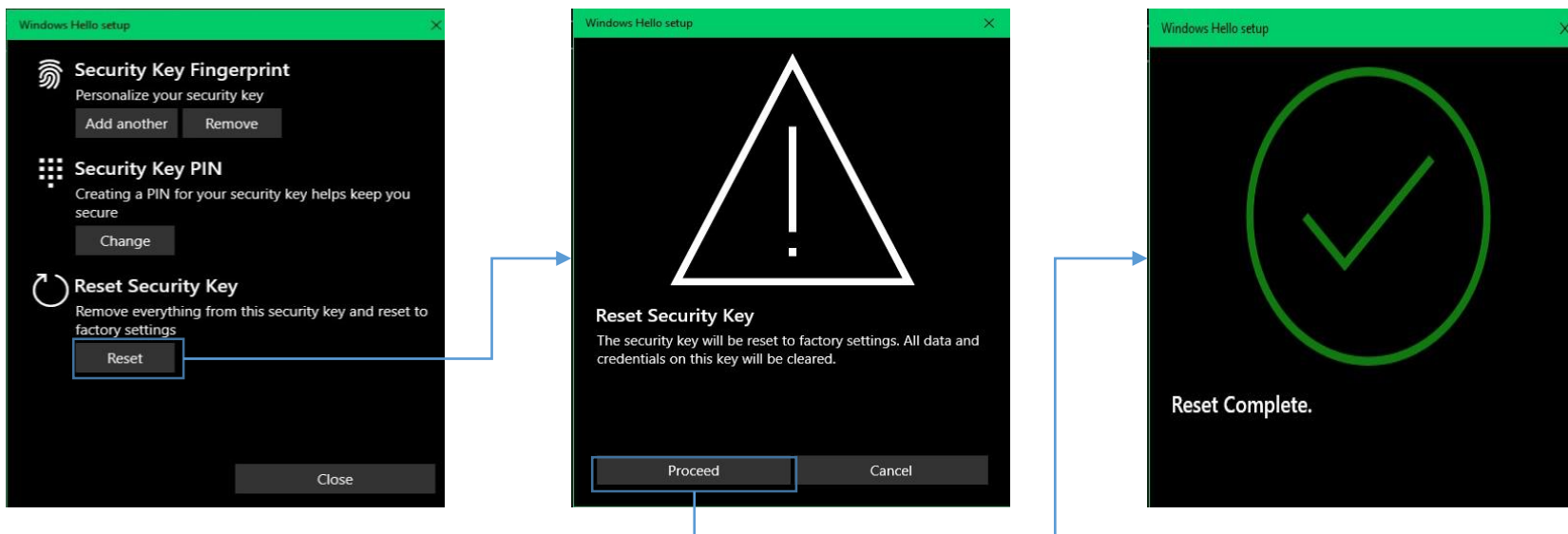
- Setup “Security Key Fingerprint”
- Type-in PIN code, following screen hint to enroll fingerprint, until “All Set!”



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



- 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

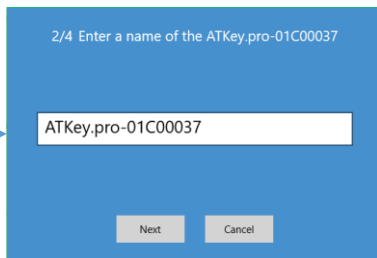
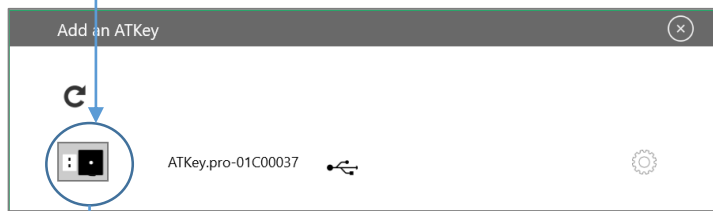
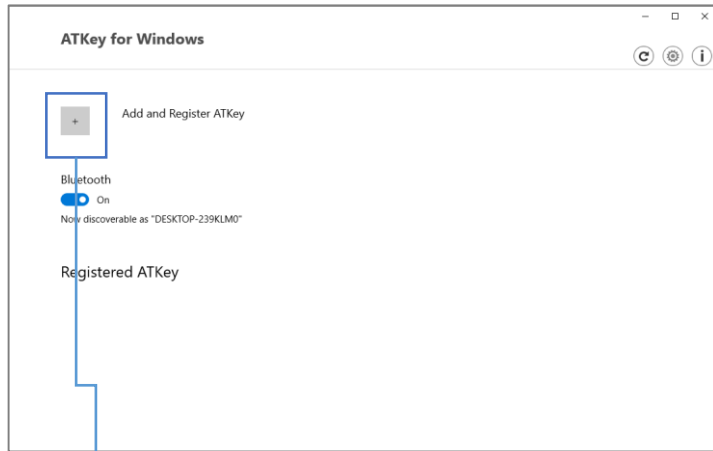
[firmware 1.00.5 or previous version]

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

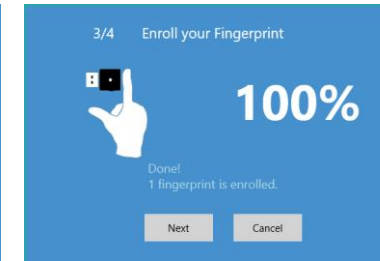
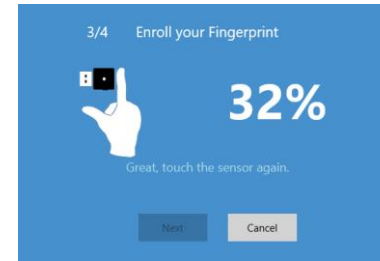
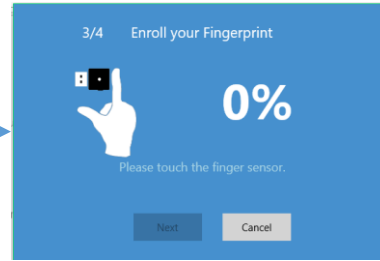
Microsoft required spec.- for authenticator reset: in order to prevent accidental trigger of this mechanism, user presence is required. In case of authenticators with no display, request MUST have come to the authenticator within 10 seconds of powering up of the authenticator.

KEY.Pro | (Step 1) App "ATKey for Windows" – Enroll fingerprint

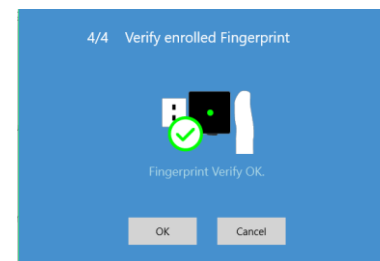
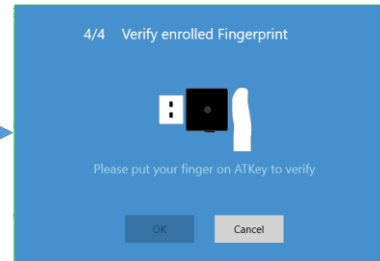
- Launch "ATKey for Windows" app (version 2.0.57.0 or later version)
- Click "Add and Register ATKey" – please make sure ATKey.Pro inserts to USB port and LED shows blue ON



Default name is -: ATKey.Pro + Keycode



around 12 times touch/enroll to finish ONE fingerprint enrollment



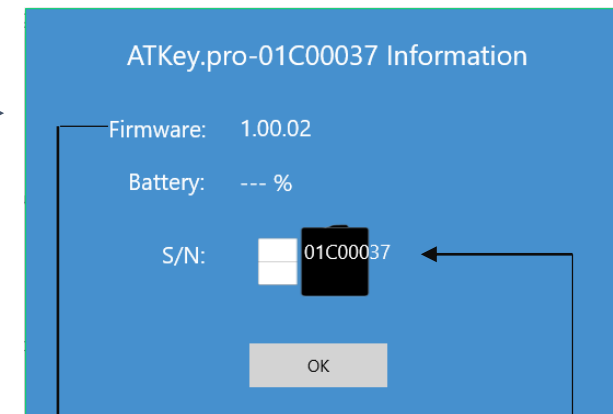
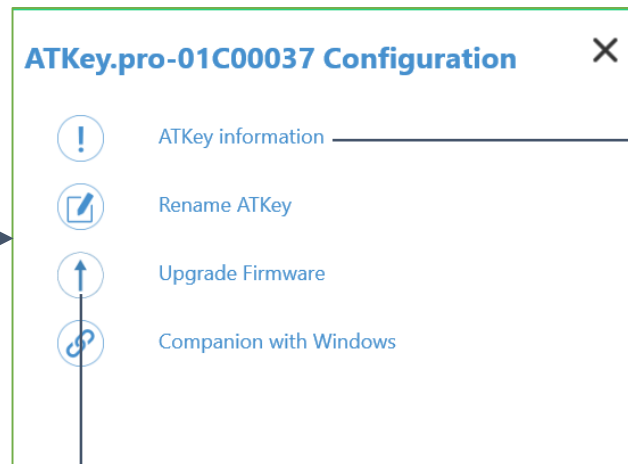
Verify enrolled fingerprint to confirm



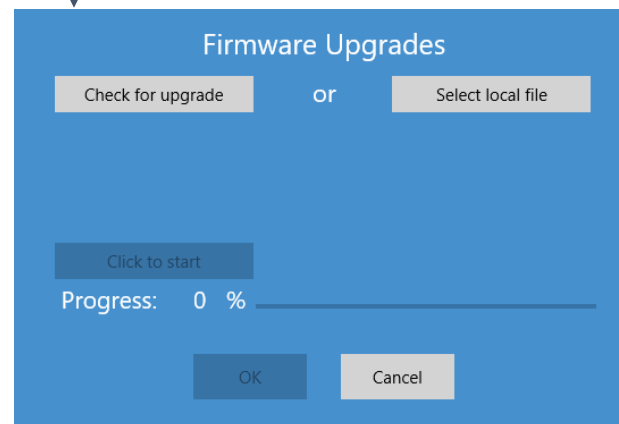
Click to refresh the page



- ATKey management – information, rename, firmware upgrade

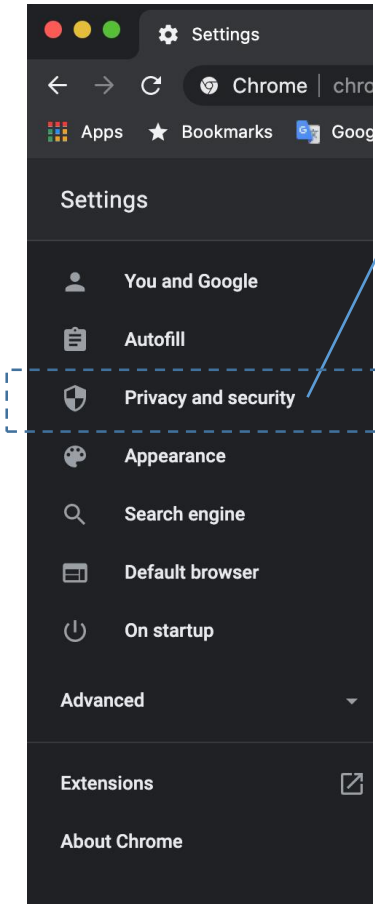


- read firmware version here
- Read “keycode” here

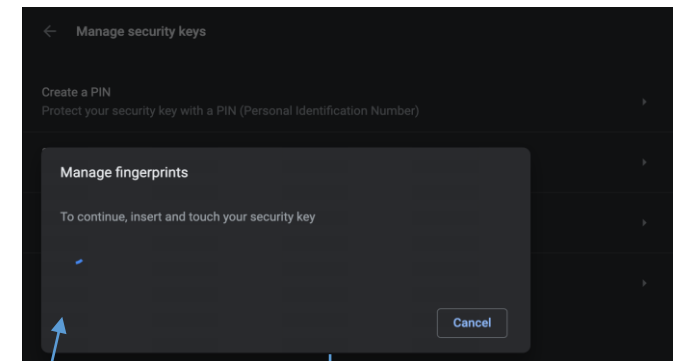
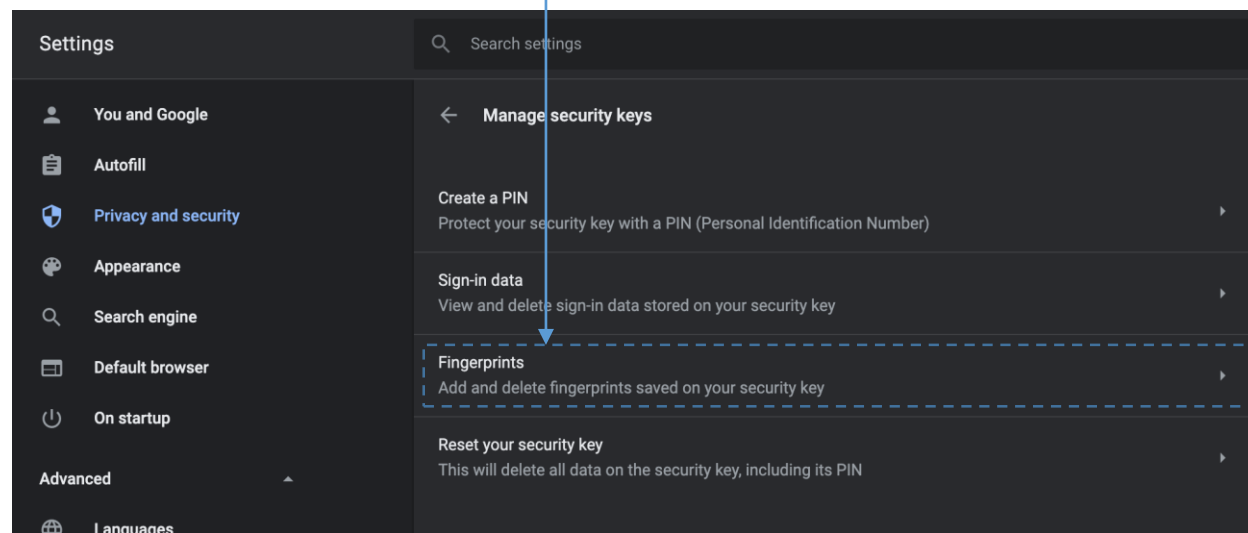
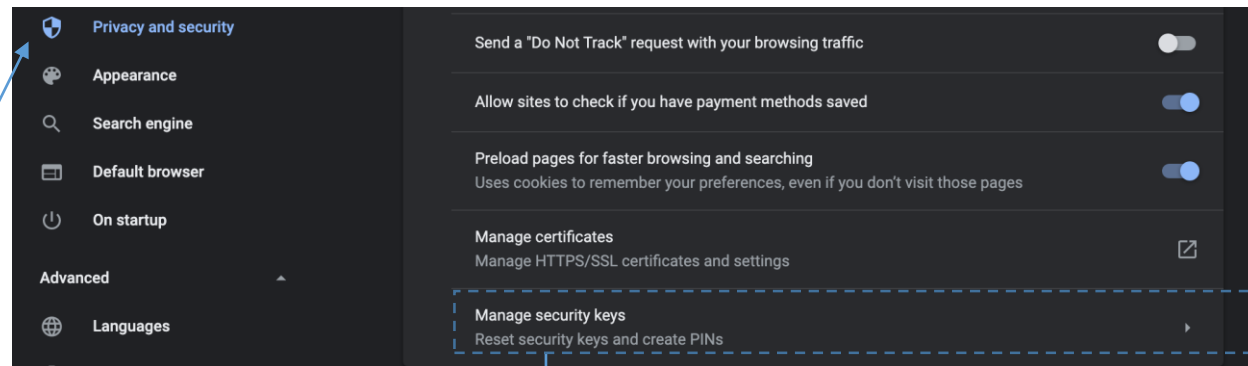


- “Check for Update”
- Select encrypted firmware image to upgrade manually
- Please wait till 100% done, then plug ATKey.Pro off USB port; re-insert to USB port, waiting ~15 sec to boot to new firmware (LED from White to Blue ON).

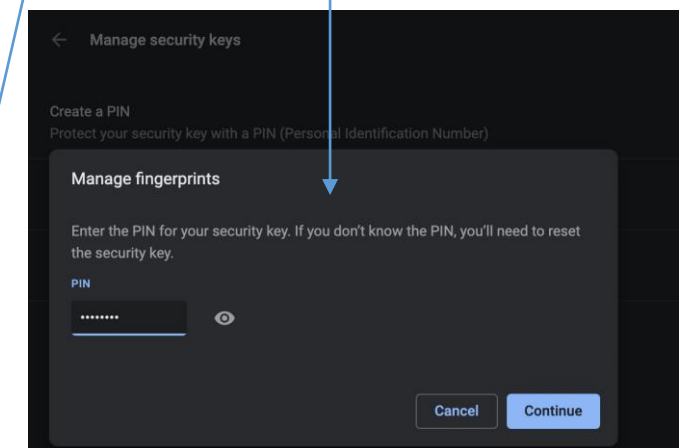
- If you are using non-Windows 10, or your Windows 10 is earlier than build 1903
 - Enroll fingerprint into ATKey.Pro via
 - [Standalone enrollment](#)
 - Or Chrome Canary (<https://www.google.com/chrome/canary/>)
 - Here is quick guide for Chrome Canary:



From "Settings" =>
"Privacy and security"

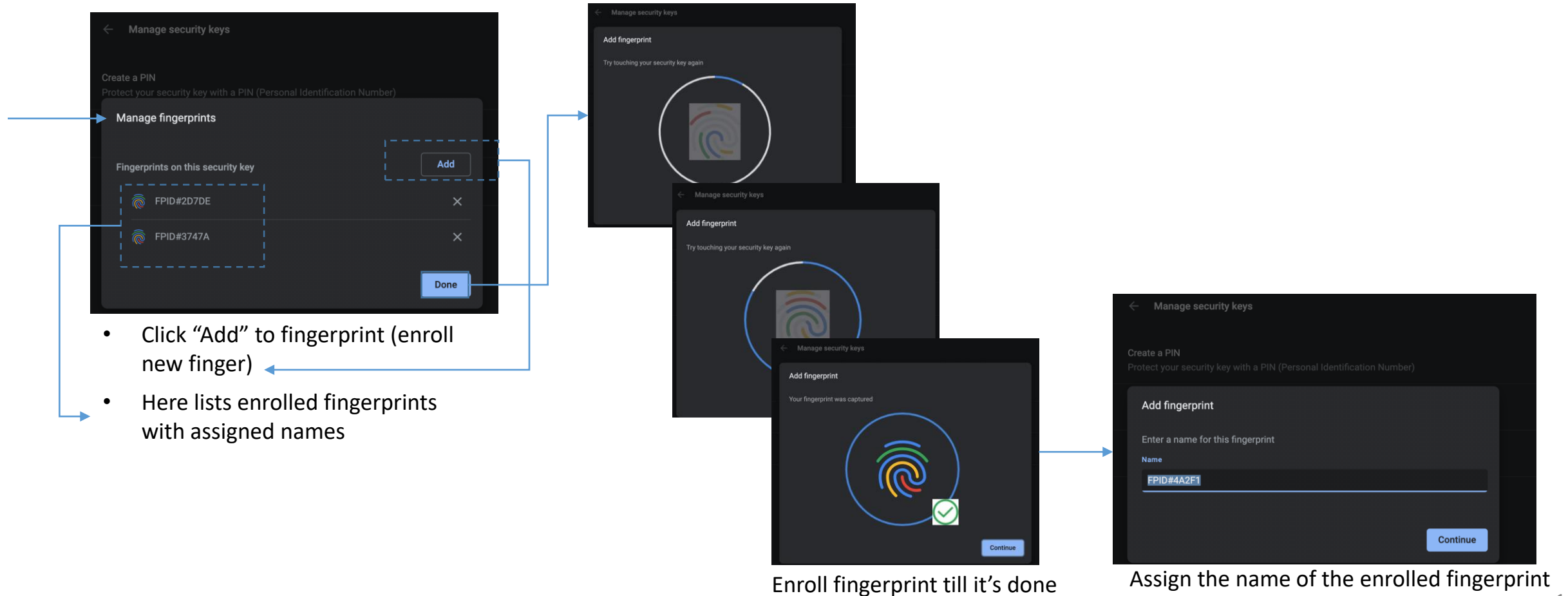


User presence needs - touch dongle by any finger

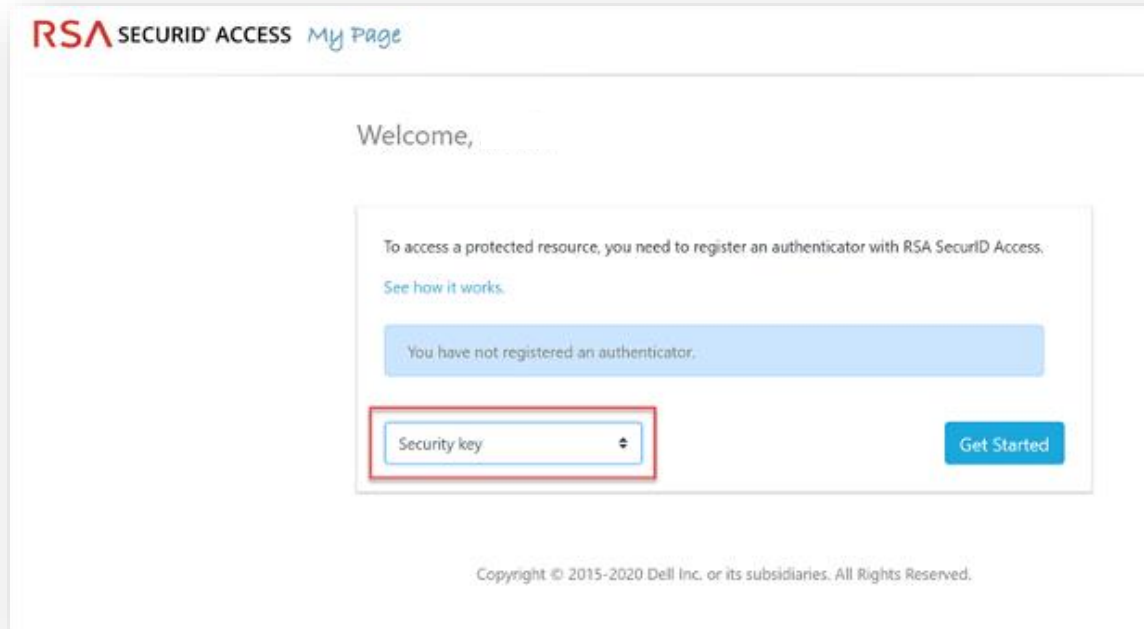


Assign PIN code into the key

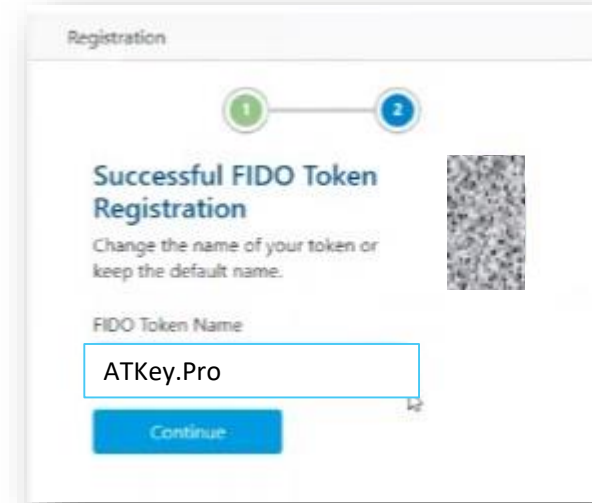
- If you are using non-Windows 10, or your Windows 10 is earlier than build 1903
 - Enroll fingerprint into ATKey.Pro via
 - [Standalone enrollment](#)
 - Or Chrome Canary (<https://www.google.com/chrome/canary/>)
 - **Here is quick guide for Chrome Canary:**



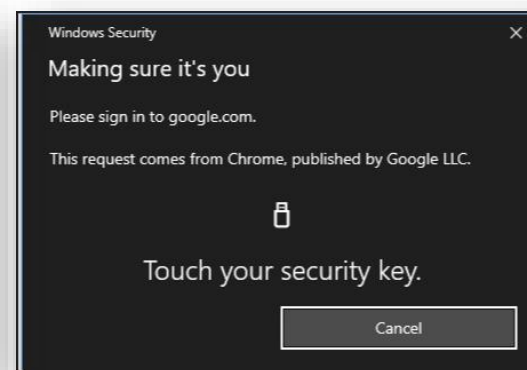
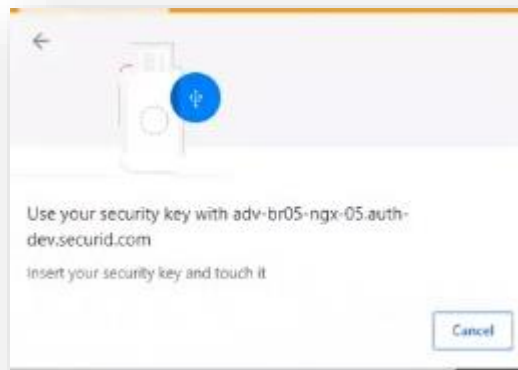
1. Sign into My Page. Your IT administrator sends the My Page URL to you.
2. Select **Security key** from the drop-down list, and click **Get Started**.



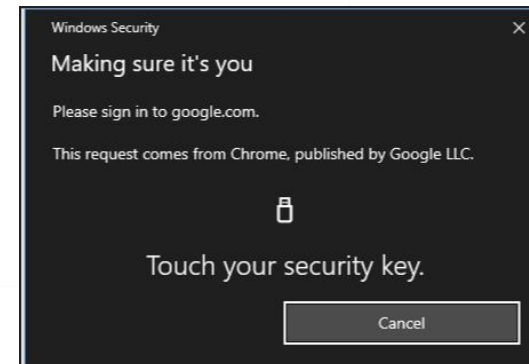
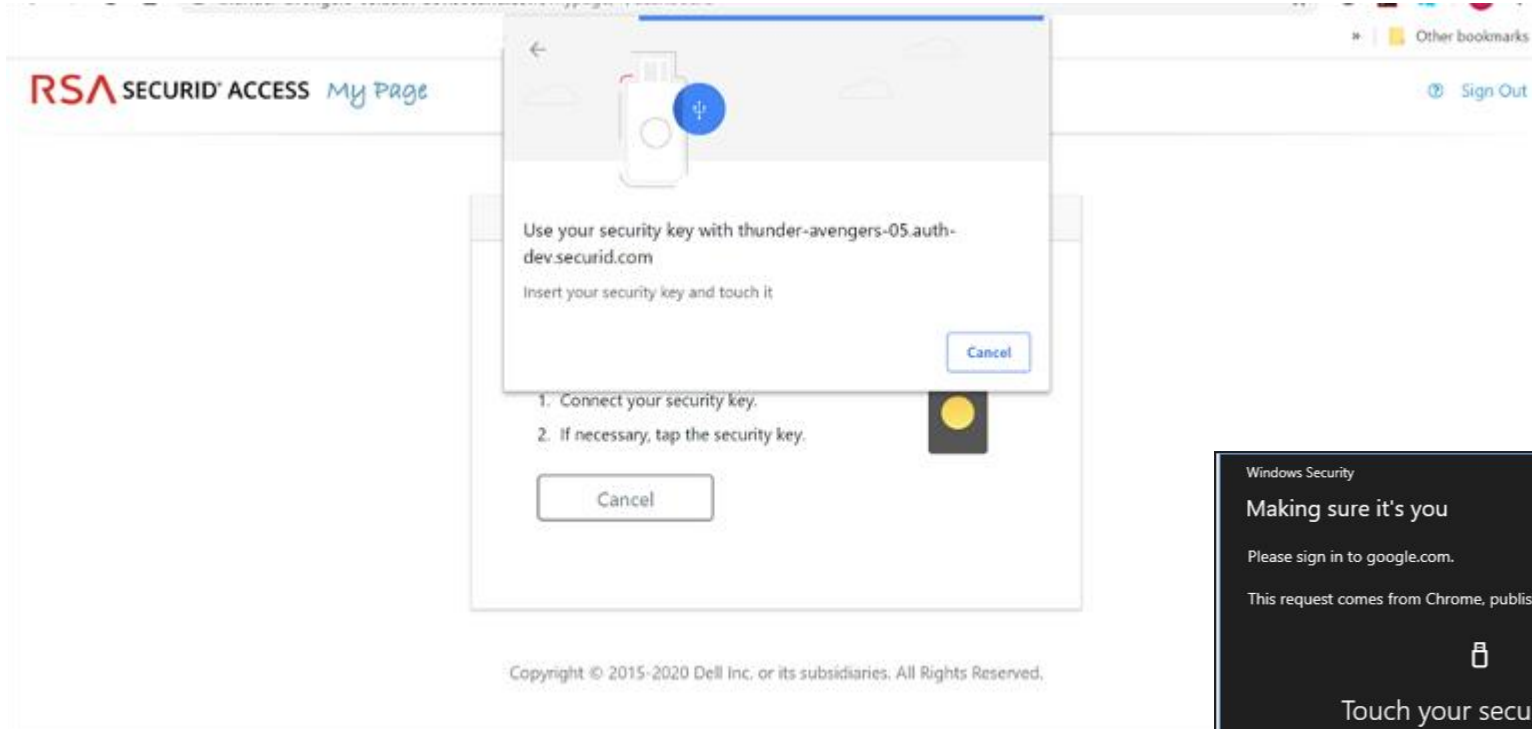
4. Change the name of the key if you like



3. Connect the security key and follow the instructions – insert ATKey.Pro USB port and touch fingerprint for matching

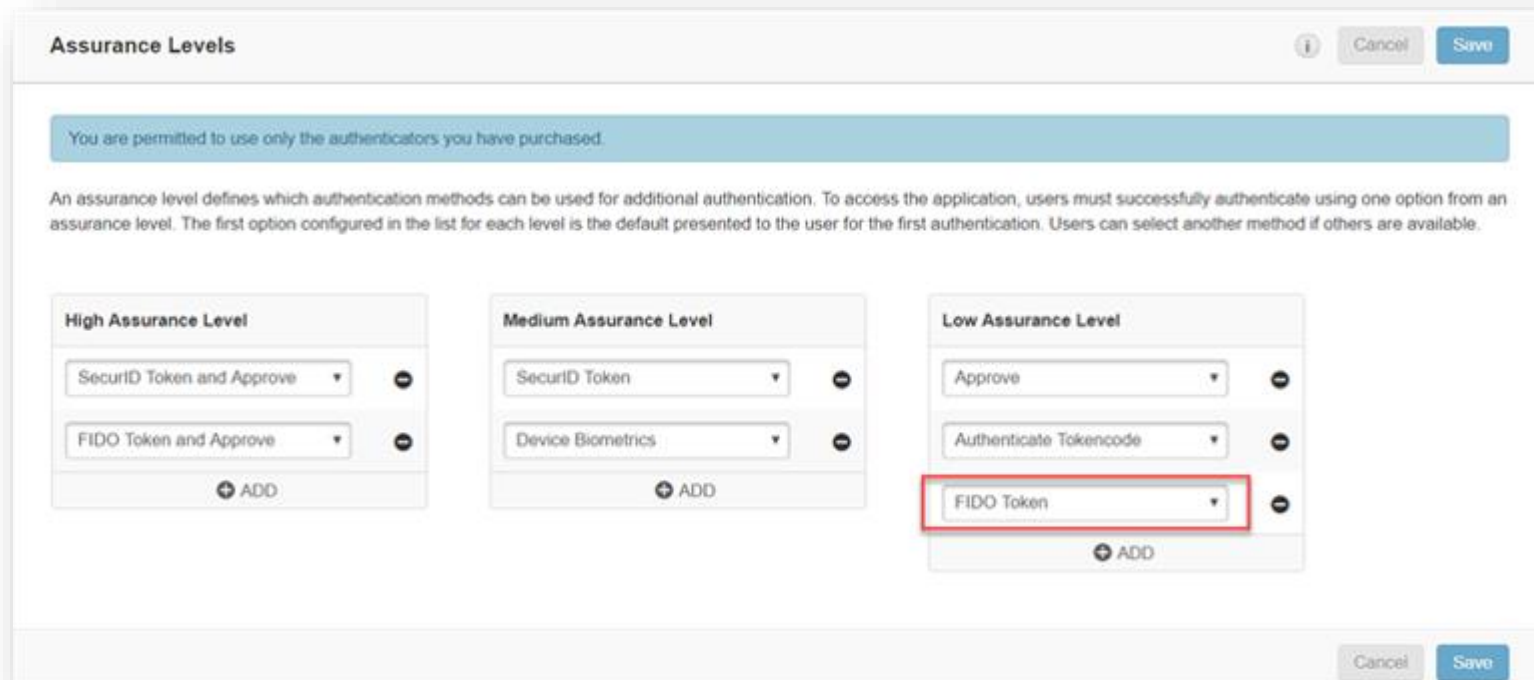


1. Open the protected application.
2. Insert ATKey.Pro into the USB port and touch fingerprint for matching



If you are an administrator, perform these steps to start using security keys with Cloud Authentication Service. These steps assume that you have an existing Cloud Authentication Service deployment.

1. Confirm that FIDO Token is in the desired assurance level:
 - In the Cloud Administration Console, click **Access > Assurance Levels**.
 - Add or move FIDO Token to the desired assurance level.



Assurance Levels Cancel Save

You are permitted to use only the authenticators you have purchased.

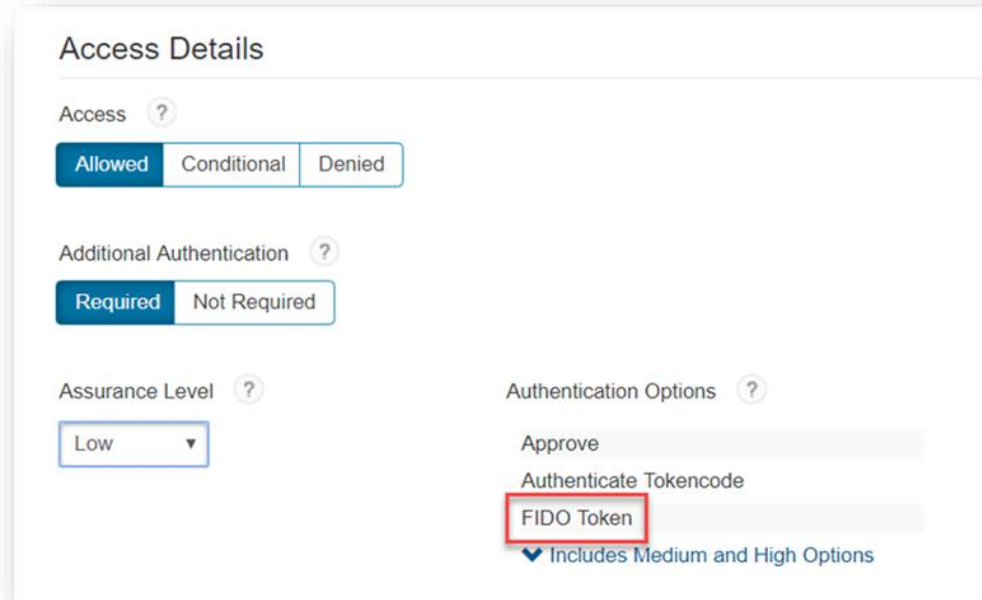
An assurance level defines which authentication methods can be used for additional authentication. To access the application, users must successfully authenticate using one option from an assurance level. The first option configured in the list for each level is the default presented to the user for the first authentication. Users can select another method if others are available.

High Assurance Level	Medium Assurance Level	Low Assurance Level
SecurID Token and Approve	SecurID Token	Approve
FIDO Token and Approve	Device Biometrics	Authenticate Tokencode
+ ADD	+ ADD	+ ADD

Cancel Save

2. Confirm that you have an access policy that uses that assurance level:

- Click **Access > Policies**.
- Click **Edit** for the policy.
- In the Rules Sets tab, confirm that FIDO Token is listed in Authentication Options.



Access Details

Access ?

Allowed Conditional Denied

Additional Authentication ?

Required Not Required

Assurance Level ?

Low

Authentication Options ?

Approve

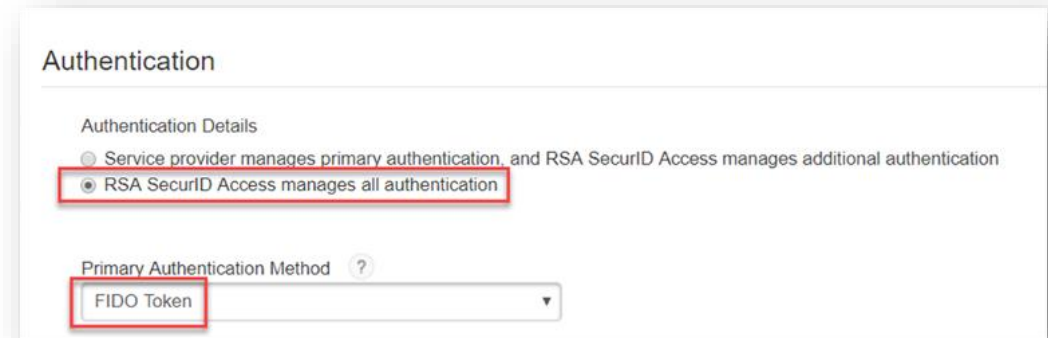
Authenticate Tokencode

FIDO Token

Includes Medium and High Options

3. Add a service provider:

- Click **Authentication Clients > Relying Parties > Add a Relying Party > Add** next to Service Provider.
- Determine if you want to use FIDO Token for primary authentication or additional authentication, or both. If you want to use FIDO for primary authentication, add a service provider and specify FIDO as the primary authentication method. In the Authentication tab, select **RSA SecurID Access manages all authentication**. In the Primary Authentication Method drop-down list, select **FIDO Token**.



Authentication

Authentication Details

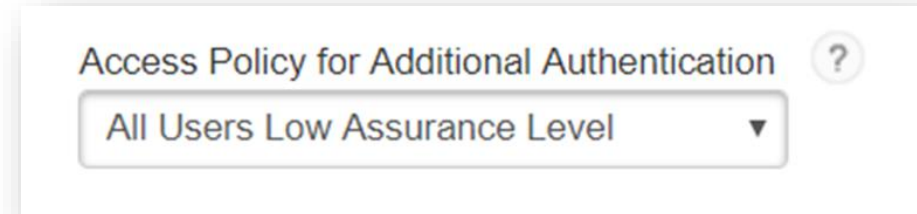
Service provider manages primary authentication, and RSA SecurID Access manages additional authentication

RSA SecurID Access manages all authentication

Primary Authentication Method ?

FIDO Token

- If you are using FIDO for additional authentication, in the Access Policy for Additional Authentication, select the policy that contains FIDO Token

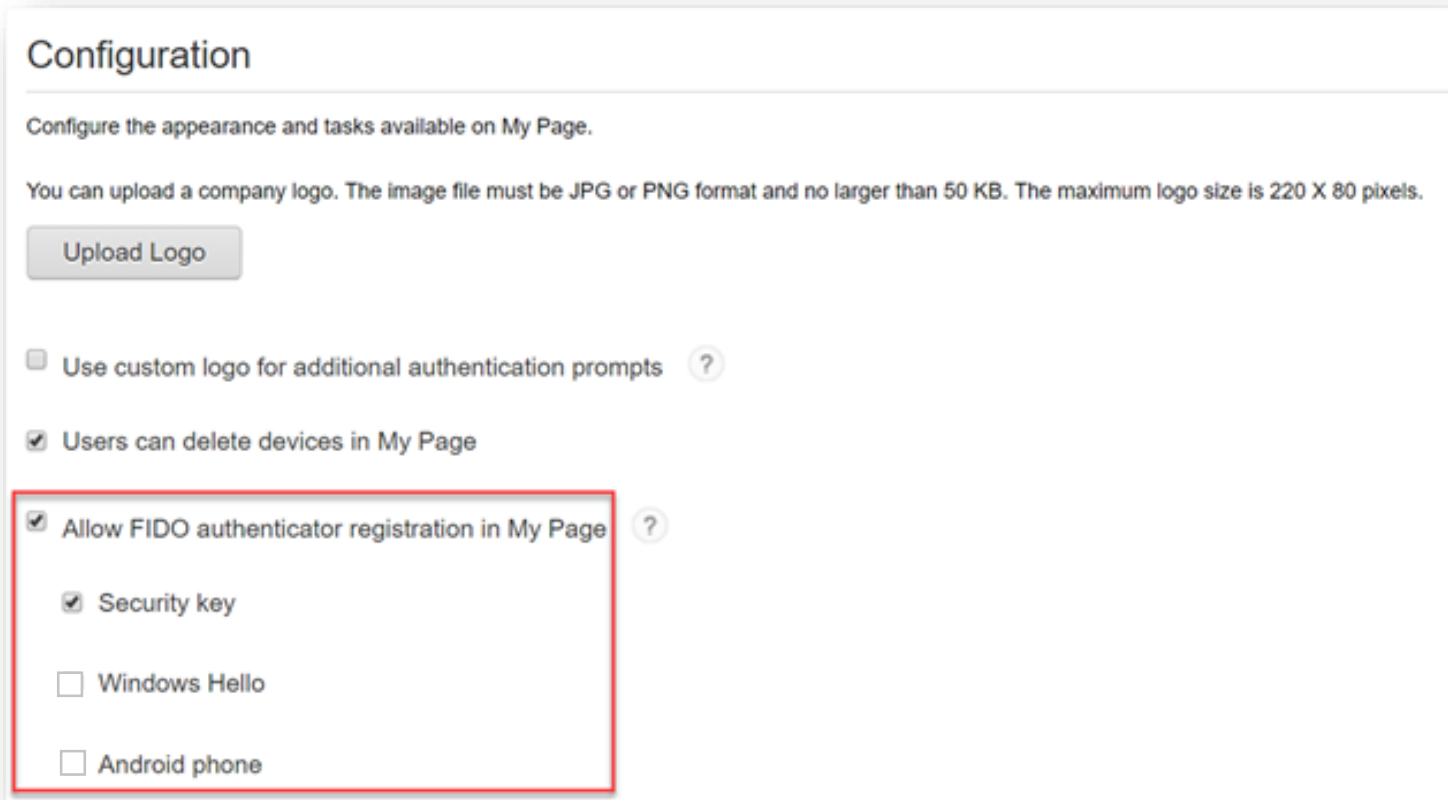


Access Policy for Additional Authentication ?

All Users Low Assurance Level

4. Enable FIDO authenticator registration in My Page:

- Click **Platform > My Page**.
- Under Configuration, select **Users can register FIDO authenticators in My Page** and select **Security key**.



Configuration

Configure the appearance and tasks available on My Page.

You can upload a company logo. The image file must be JPG or PNG format and no larger than 50 KB. The maximum logo size is 220 X 80 pixels.

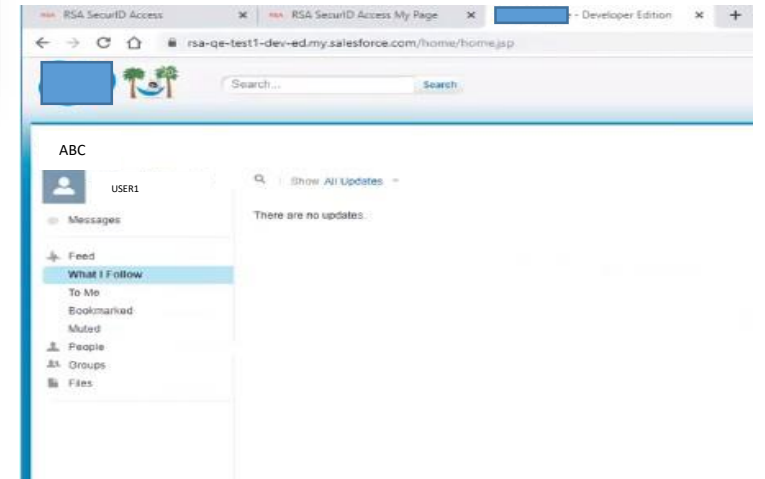
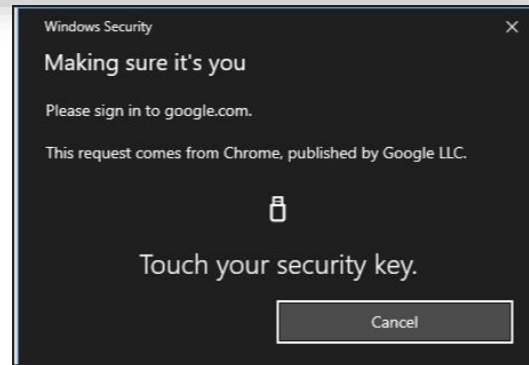
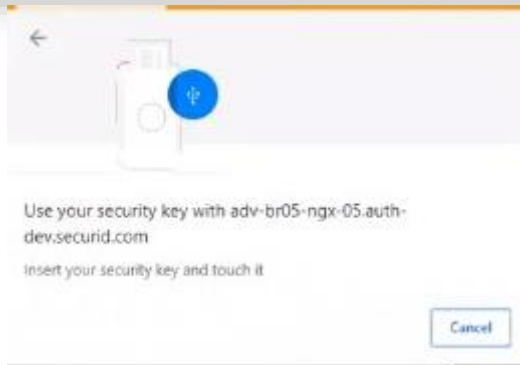
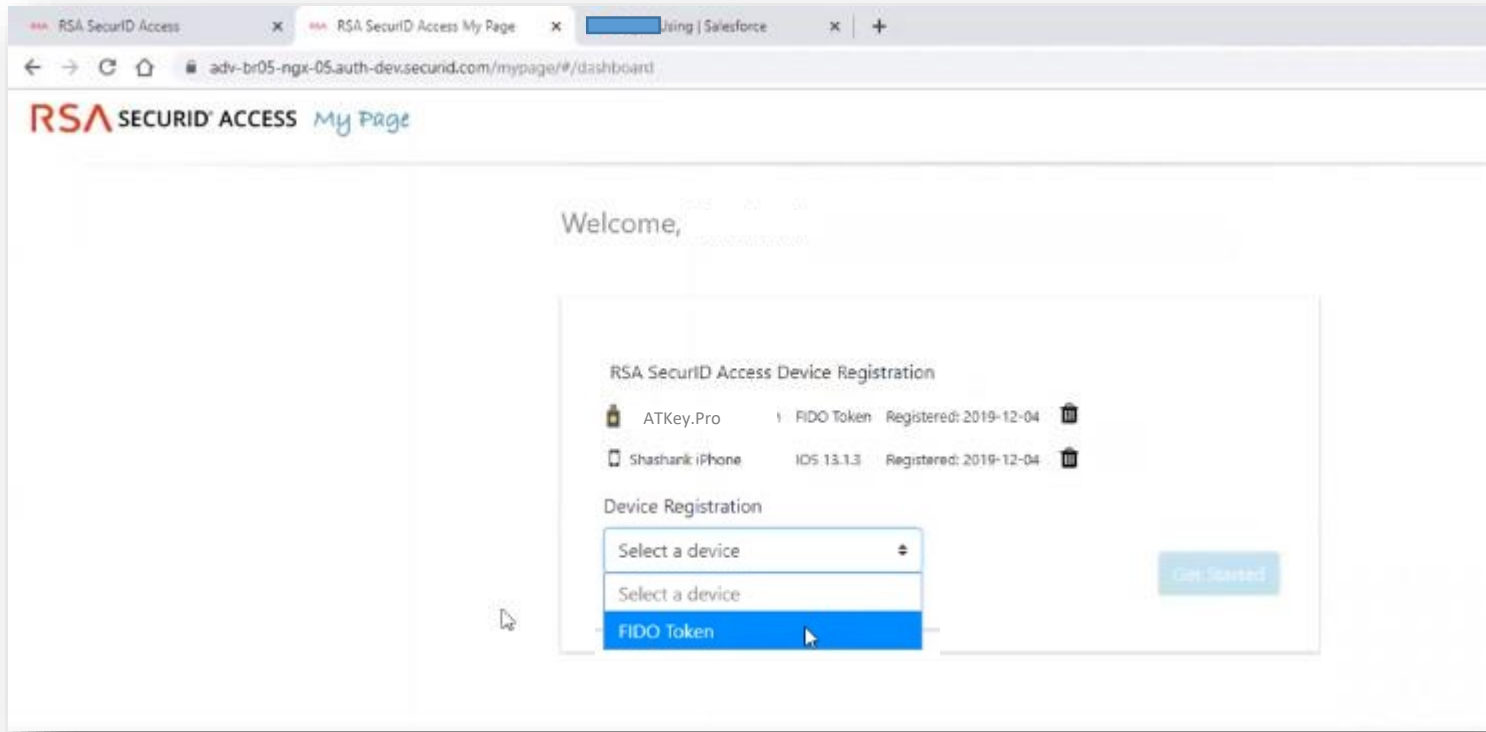
Use custom logo for additional authentication prompts ?

Users can delete devices in My Page

Allow FIDO authenticator registration in My Page ?

- Security key
- Windows Hello
- Android phone

1. For your service login page, select FIDO token; insert ATKey.Pro to USB port, touch fingerprint for matching to login



- 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.





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

THANK YOU!



www.authentrend.com



contact@authentrend.com



[AuthenTrend](#)



[AuthenTrend](#)

AUTHENTREND