NO MORE PASSWORD

Passwordless authentication for
Azure AD (Entra ID) by ATKey

AUTHENTREND

4 Steps

1. [Admin] Azure AD settings	a) by default, you will be asked to register your phone number or Microsoft Authenticator app, then register FIDO Key b) But if you just want FIDO key only, setting a temporary access pass, then enable FIDO Key
2. [User] ATKey Fingerprint	a) If you want following standard FIDO way: Fingerprint + PIN code through Windows Settings b) Or if you want Fingerprint only (Patent technology - Standalone enrollment) w/o PIN code
3. [User] Register ATKey to your Azure AD account	a) by default, you will be asked to register your phone number or Microsoft Authenticator app, then register FIDO Key b) But if you just want FIDO key only, setting a temporary access pass, then enable FIDO Key
4. [User] Login via ATKey	• Passwordless login to joined Azure AD Windows PC • Login Microsoft Services (Azure AD, Microsoft 365, OneDrive, Teams, …..)

Step 1.a [Admin] Azure AD Settings

a) by default, you will be asked to register your phone number or Microsoft Authenticator app, then register FIDO Key

1. Sign in to the Azure Portal (https://portal.azure.com/) with administrator privileges.
2. Browse to **Azure Active Directory** > **Security** > **Authentication methods** > **Authentication method policy**. Fig. 1-1
3. Under the method **FIDO2 Security Key**, click **All users**, or click **Add groups** to select specific groups. *Only security groups are supported*. Fig. 1-2 - *it may takes effect in a few minutes, not immediately*
4. **Save** the configuration.

Fig. 1-1

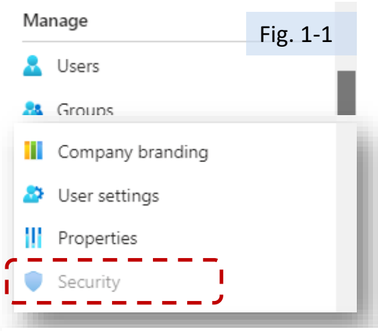
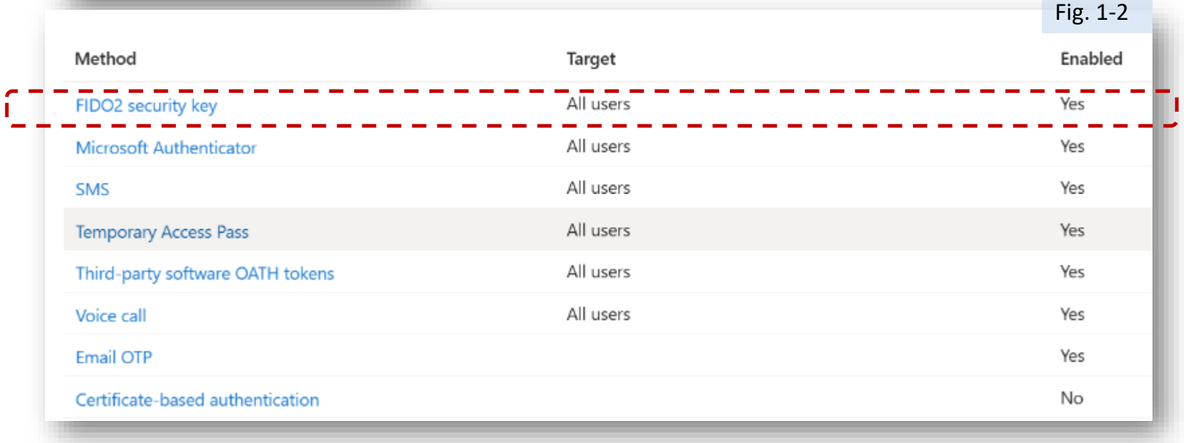
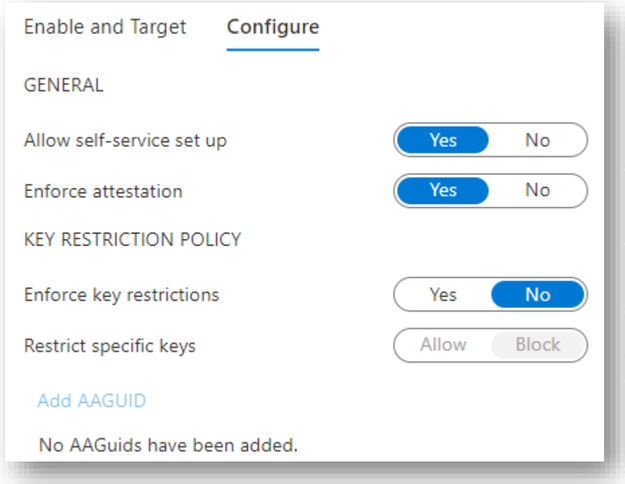


Fig. 1-2



Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Third-party software OATH tokens	All users	Yes
Voice call	All users	Yes
Email OTP		Yes
Certificate-based authentication		No

5. Fido Security Key optional Settings



- **Allow self-service set up** should remain set to **Yes**. If set to no, your users won't be able to register a FIDO key through the MySecurityInfo portal, even if enabled by Authentication Methods policy.
- **Enforce attestation** setting to **Yes** requires the FIDO security key metadata to be published and verified with the FIDO Alliance Metadata Service, and also pass Microsoft's additional set of validation testing.
- **Enforce key restrictions** should be set to **Yes** only if your organization wants to only allow or disallow certain FIDO security keys, which are identified by their AAGuids. You can work with your security key provider to determine the AAGuids of their devices. If the key is already registered, AAGUID can also be found by viewing the authentication method details of the key per user.
  - please check below link for ATKey AAGUID: https://authentrend.com/atkey-fido2-security-key-aaguids/

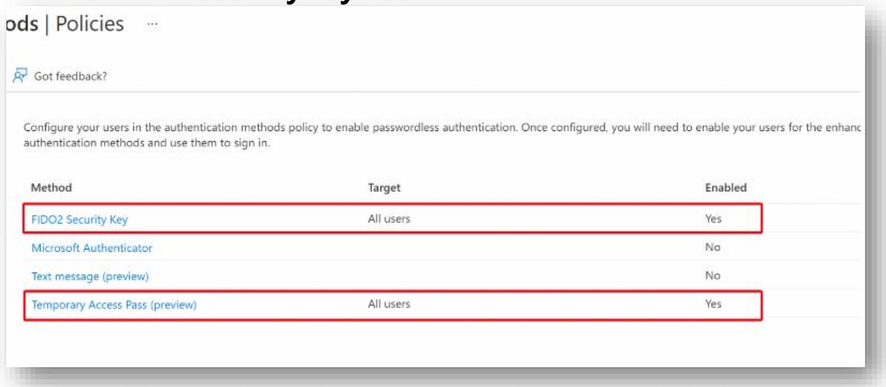
**please check below link for more details:*
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key

Step 1.b [Admin] Azure AD Settings

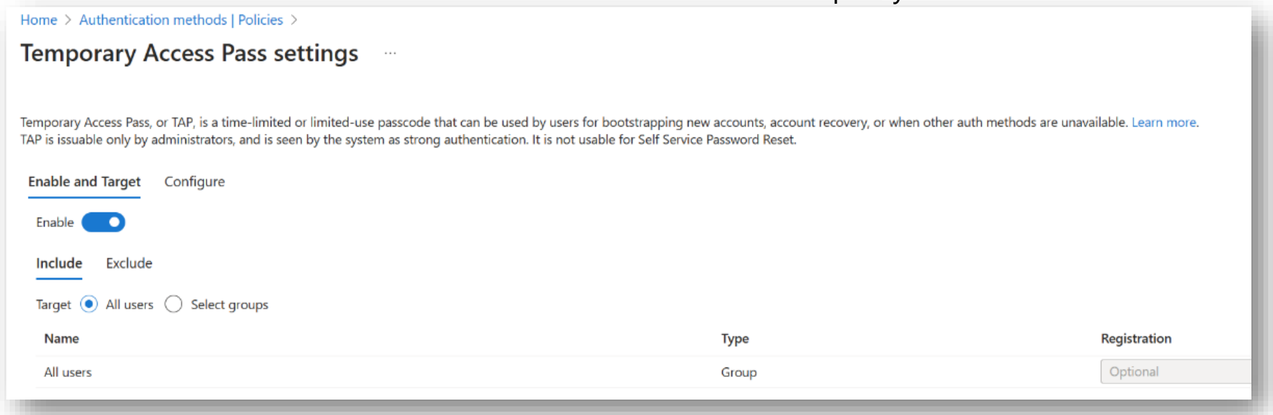
b) If you just want FIDO key only, setting a temporary access pass and enable FIDO security Key

A Temporary Access Pass is a time-limited passcode that can be configured for single use or multiple. Users can sign in with a Temporary Access Pass to onboard other authentication methods including passwordless methods such as Microsoft Authenticator, FIDO2 or Windows Hello for Business.

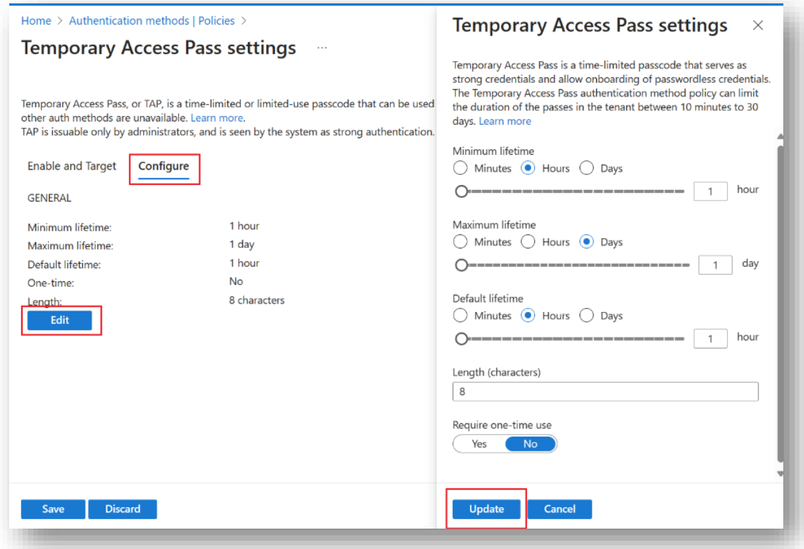
1. Sign in to the Azure portal using an account with *global administrator* permissions.
2. Search for and select **Azure Active Directory**, then choose **Security** from the menu on the left-hand side.
3. Under the **Manage** menu header, select **Authentication methods** > **Policies**.
4. From the list of available authentication methods, select **Temporary Access Pass** and **Enable FIDO2 security key** also



5. Click **Enable** and then select users to include or exclude from the policy.



6. (Optional) Select **Configure** to modify the default Temporary Access Pass settings, such as setting maximum lifetime, or length, and click **Update**.



please check below link for more details:

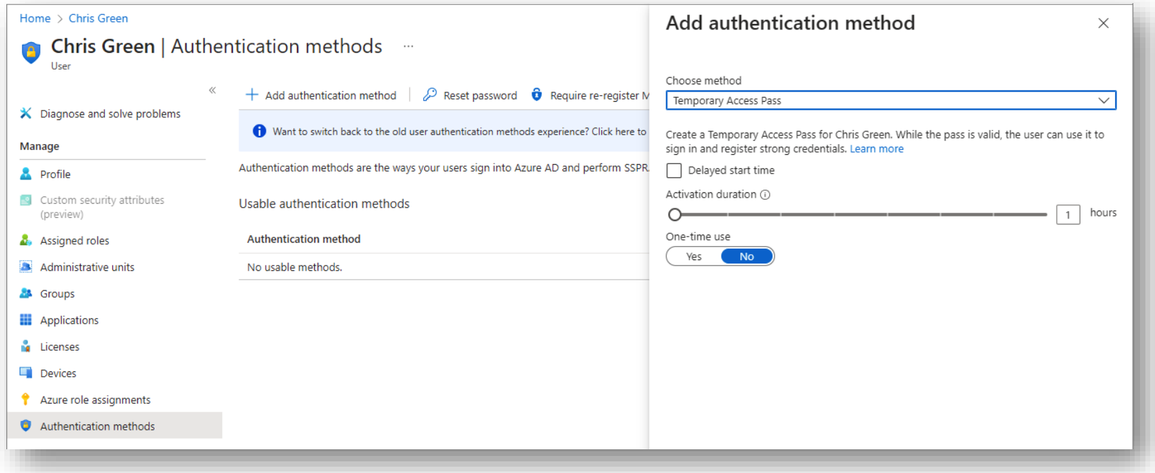
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass

Step 1.b [Admin] Issuing “Temporary Access Pass” to Users

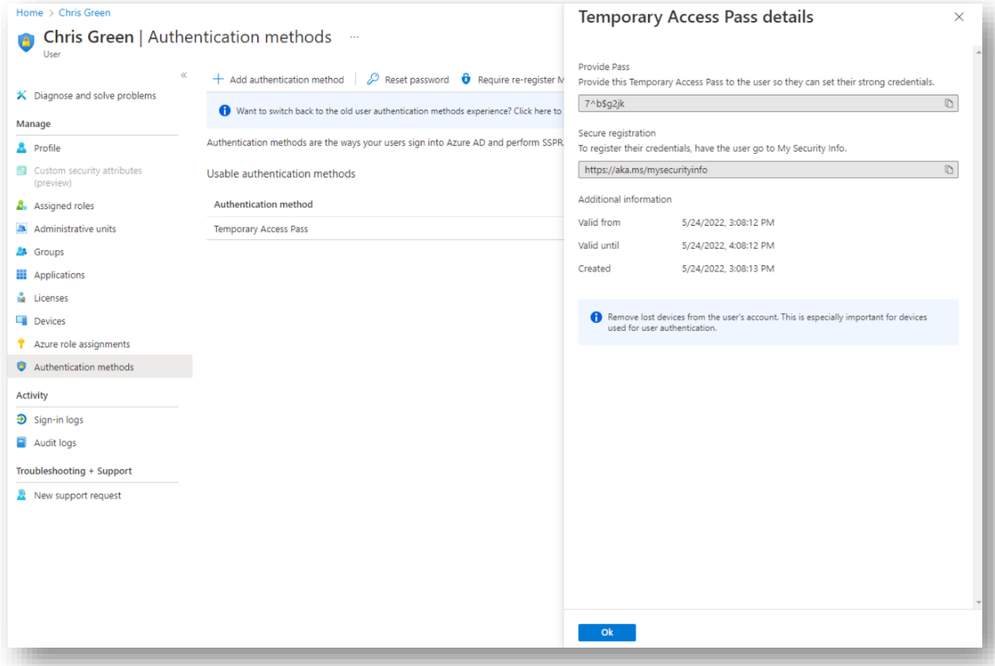
b) If you just want FIDO key only, setting a temporary access pass and enable FIDO security Key

A Temporary Access Pass is a time-limited passcode that can be configured for single use or multiple. Users can sign in with a Temporary Access Pass to onboard other authentication methods including passwordless methods such as Microsoft Authenticator, FIDO2 or Windows Hello for Business.

1. Sign in to the Azure portal by using one of the preceding roles.
2. Select **Azure Active Directory**, browse to Users, select a user, such as *Chris Green*, then choose **Authentication methods**.
3. If needed, select the option to **Try the new user authentication methods experience**.
4. Select the option to **Add authentication methods**.
5. Below **Choose method**, select **Temporary Access Pass**.
6. Define a custom activation time or duration and select **Add**.



7. Once added, the details of the Temporary Access Pass are shown. Make a note of the actual Temporary Access Pass value. You provide this value to the user. You can't view this value after you select **Ok**.



*please check below link for more details:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass

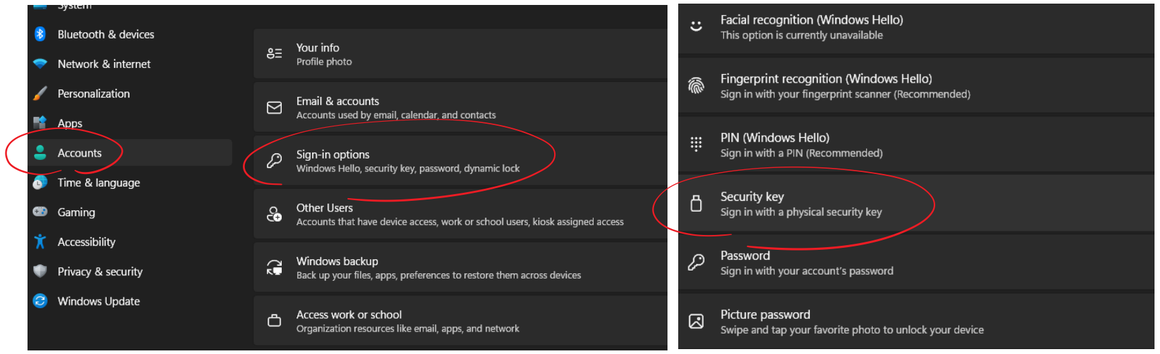
Step 2.a [User] ATKey Fingerprint

a) If you want following standard FIDO way: Fingerprint + PIN code through Windows Settings

1 Open Windows Settings

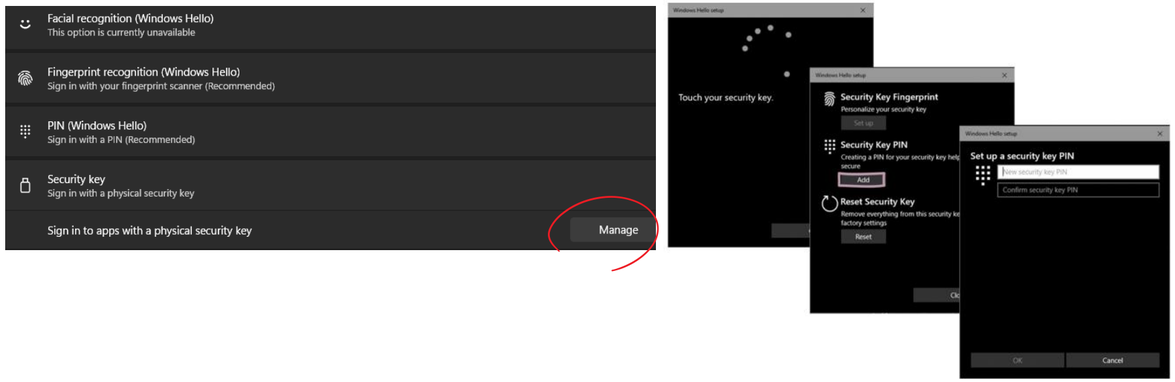
"Settings" > "Accounts" > "Sign-in options" > "Security Key"

Availability: In Windows 1903 and above.



2 Set the PIN of ATKey

Add "Security key PIN" first, the PIN will write into ATKey.Pro.



3 Add Your Fingerprint

Set up "Security Key Fingerprint", type-in PIN code and follow the hints to enroll fingerprint until "All Set!"

Helpful Tips

Fingerprint good enrollment can help for verification much quick and easier, please check below video as the tips for good enrollment:

https://youtu.be/bCLPMtZJhkM (English)

https://youtu.be/G-p30PEBUQc (Japanese)

Step 2.b [User] ATKey Fingerprint

b) Or if you want Fingerprint only (Patent technology - Standalone enrollment) w/o PIN code

1 Enroll Fingerprints through Standalone Enrollment

With no need for any device or application download.

- Availability: Power supply from any USB port (USB port of PC or Power bank are both fine)
- Please enroll a fingerprint at the same/similar finger position

- Insert ATKey.Pro into the USB port.
- LED Cyan ON.
- Press the side button 3 times quickly to get into Standalone enroll mode.
  - ✓LED White flash: please touch your fingerprint, after touch, LED turns to Green means this enrollment is good, LED turns to RED means this enrollment not good.
  - ✓So touch fingerprint at every White Flash, it may need 12 times good enrollments, until LED stays on "Cyan", then the enrollment is done.

Tutorial video

- If you want to quit "standalone enrollment", press the button and the LED will turn to Blue, back to the normal state.
- If there are any enrolled fingerprints in your ATKey.Pro, LED will Green flash first on step 4, that you need to verify registered fingerprint to start enrolling new finger.

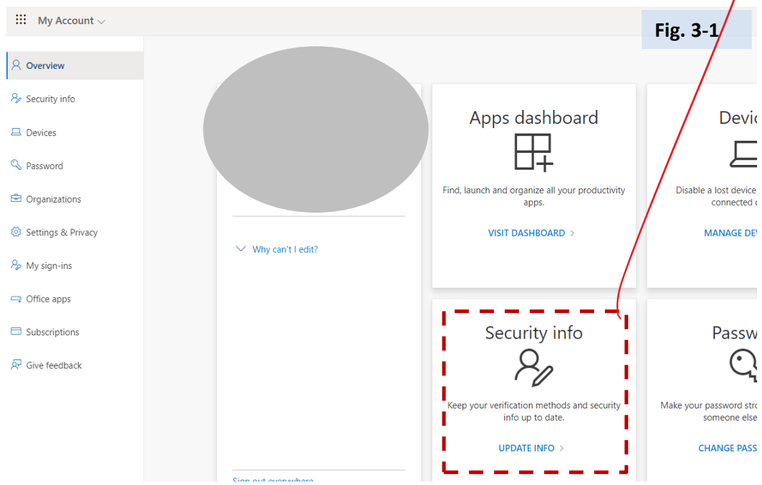
Helpful Tips

Fingerprint good enrollment can help for verification much quick and easier, please check below video as the tips for good enrollment:
https://youtu.be/bCLPMtZJhkM (English)
https://youtu.be/G-p30PEBUQc (Japanese)

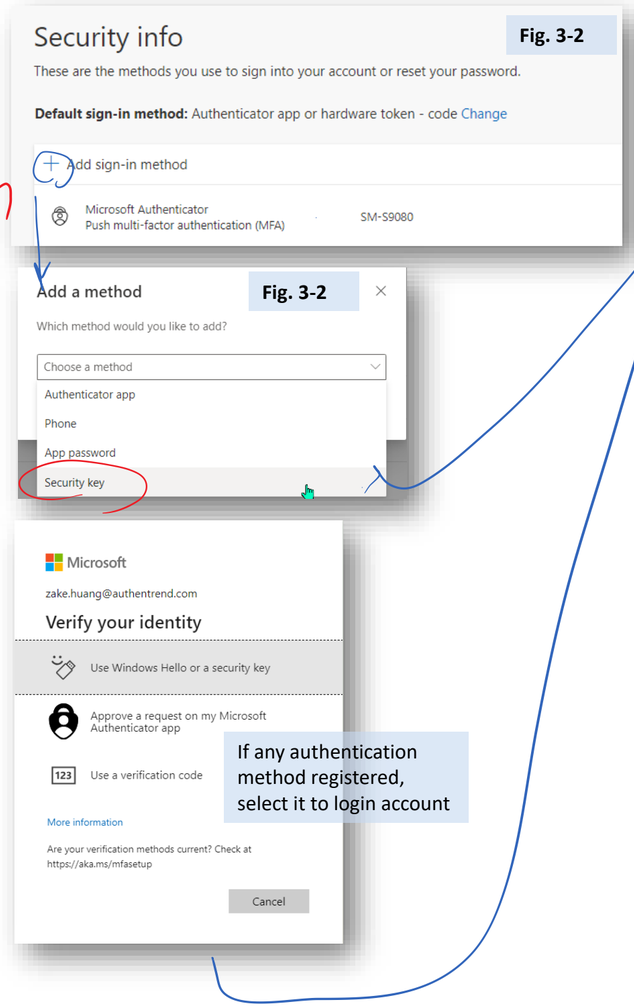
Step 3.a [User] Register ATKey to your AD Account

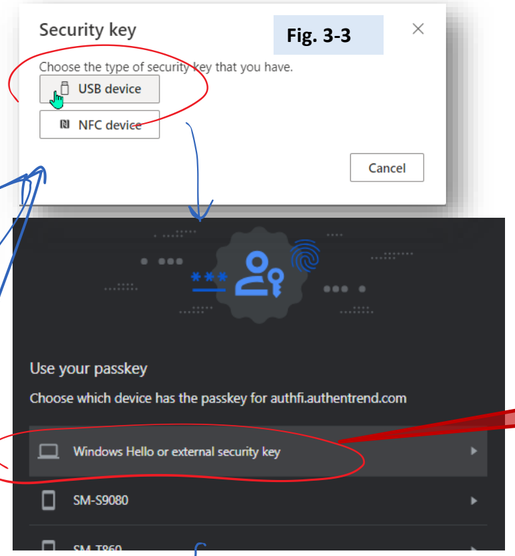
a) by default, you will be asked to register your phone number or Microsoft Authenticator app, then register FIDO Key

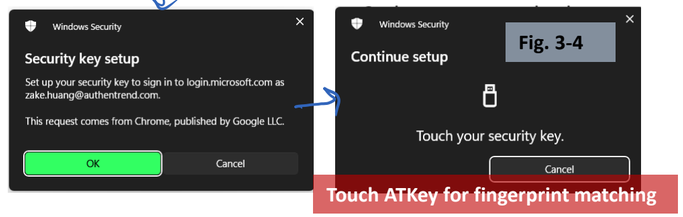
1. Browse to https://myprofile.microsoft.com, Sign in if not already
2. Click **Security Info**. Fig. 3-1
    1) If the user already has at least one Azure AD Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
    2) If they don't have at least one Azure AD Multi-Factor Authentication method registered, they must add one.
    3) An Administrator can issue a Temporary Access Pass to allow the user to register a Passwordless authentication method. (next page)
    4) Add a FIDO2 Security key by clicking **Add method** and choosing **Security key**. Fig. 3-2
    5) Choose **USB device** or **NFC device**. Fig. 3-3
    6) Have your key ready and choose **Next**.
    7) perform the required gesture for the key, either biometric or touch.
    8) The user will be returned to the combined registration experience and asked to provide a meaningful name for the key to identify it easily. Click **Next**. Fig. 3-4
    9) Click **Done** to complete the process.

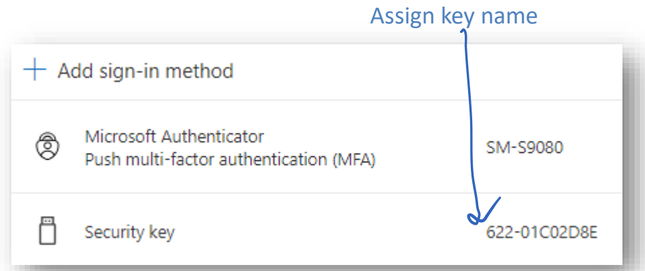


- Security info => "+ Add sign-in method"





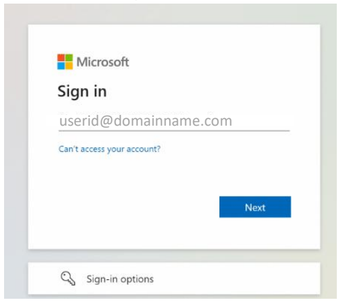




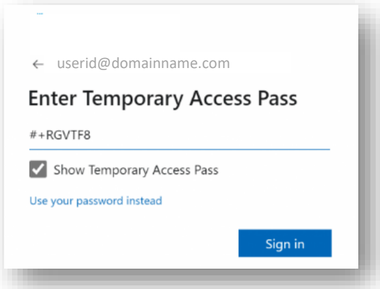
Step 3.b [User] Register ATKey to your AD Account

b) If you just want FIDO key only, setting a temporary access pass and enable FIDO security Key

1. Please make sure Temporary Access Pass enabled at Step 1.b
2. go to https://aka.ms/mysecurityinfo. Make sure it's a fresh session, meaning that the user is not signed in. Enter the username, and click ***Next***.

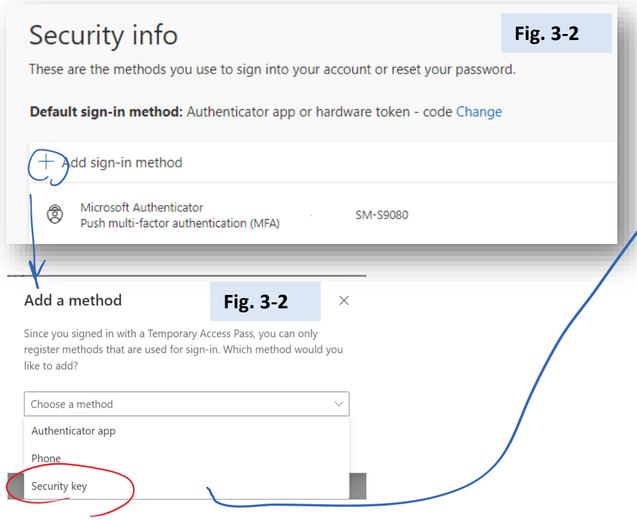


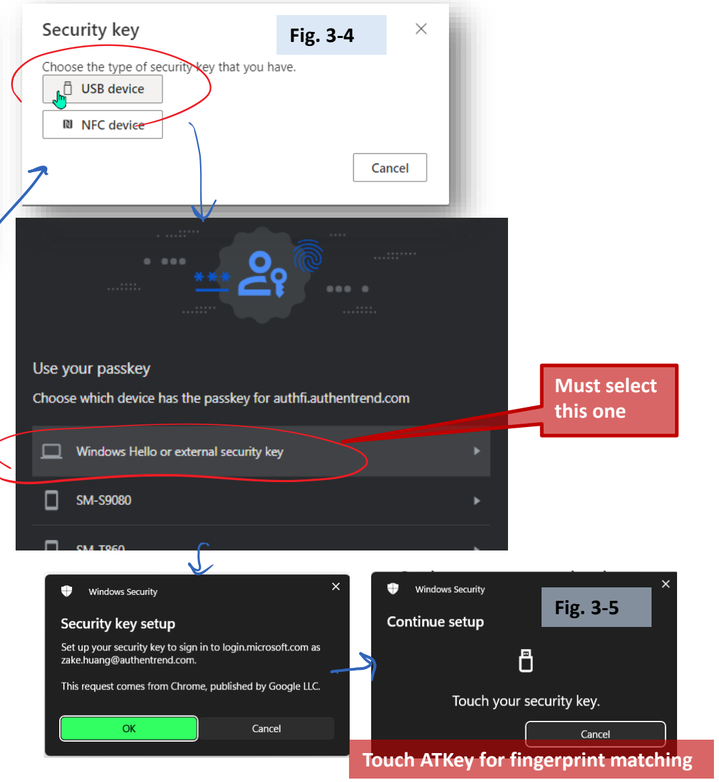
3. Now, instead of the password, the user is asked to enter the Temporary Access Pass that was displayed in the Azure porta

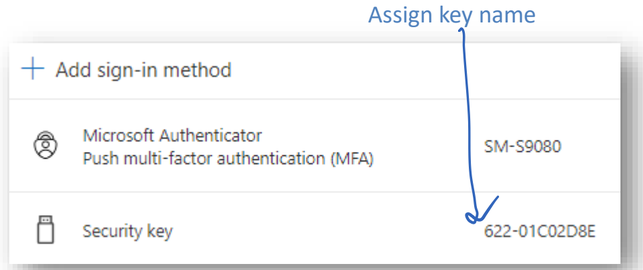


4. After you've signed-in, select "Security info", then click "***+ Add method"***, and select Security key from the dropdown menu.

- Security info => "+ Add sign-in method"







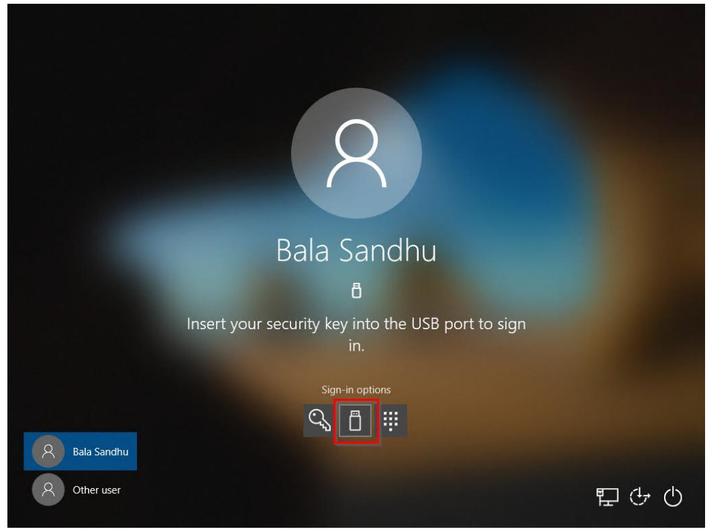
Step 4 [User] Login via ATKey

a) Passwordless login to joined Azure AD Windows PC

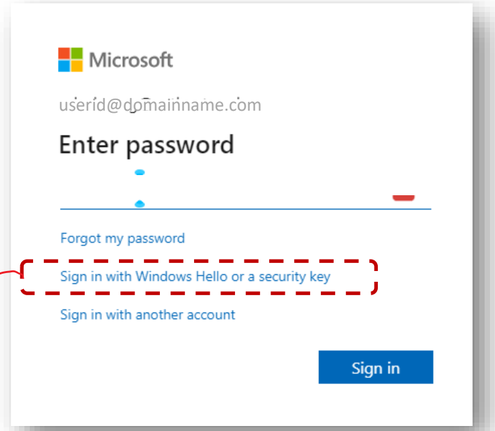
a user named “Bala Sandhu” has already provisioned their FIDO2 security key using the steps in the previous pages, Enable passwordless security key sign in.

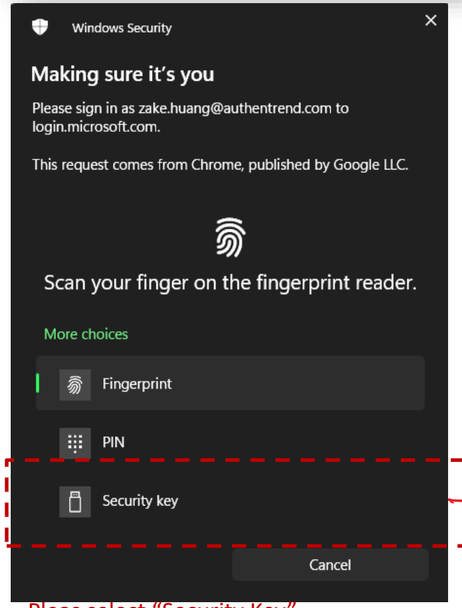
For hybrid Azure AD joined devices, make sure you have also enabled passwordless security key sign-in to on-premises resources.

“Bala” can choose the security key credential provider from the Windows 10 lock screen and insert the security key to sign into Windows. *(Windows 10 build 1903+, Windows 11)*

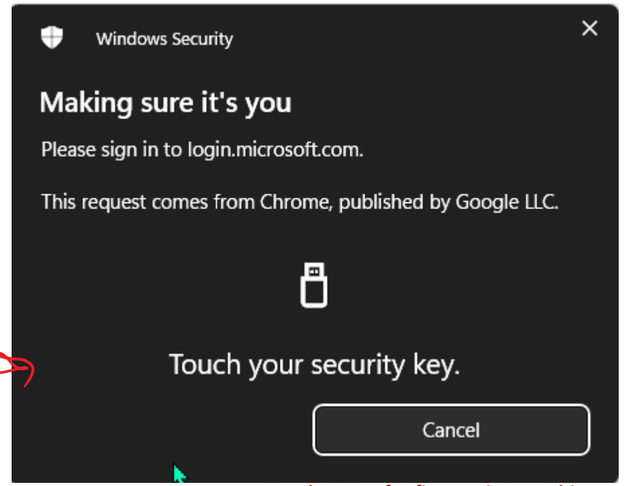


b) Login Microsoft Services (Azure AD, Microsoft 365, OneDrive, Teams, …..)





Pleas select “Security Key”



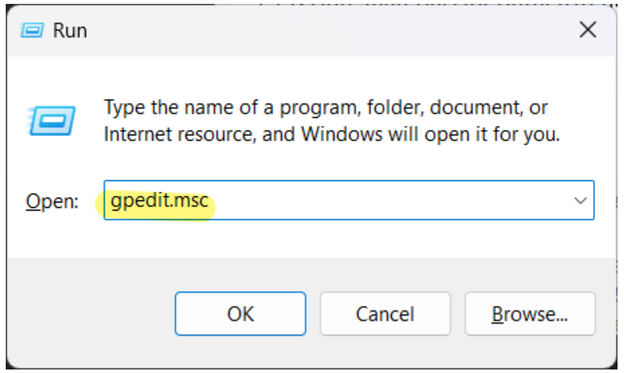
Touch ATKey for fingerprint matching

When the LED of ATKey is blue flashing, that means touch your fingerprint for matching

Enable Security Key in Windows

If you can’t see “security key icon” on your Windows login screen, please follow below steps to enable it from your Windows.

1. Launch the "Run" command by pressing the "Windows+R" simultaneously > Type "gpedit.msc" > press "OK“

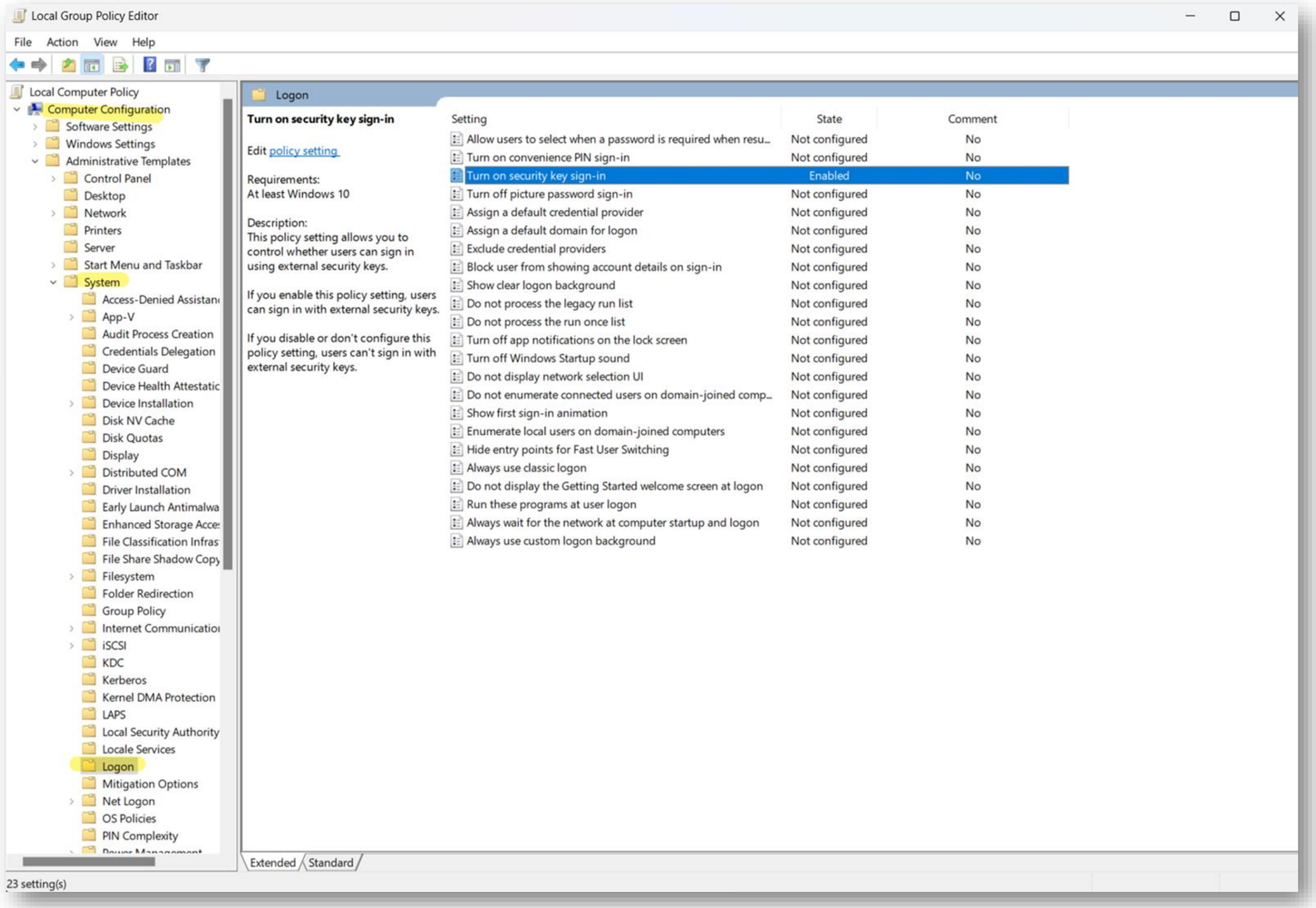


2. In the left pane of Local Group Policy Editor, navigate to: Computer Configuration > Administrative Templates > System > Logon

3. Set the state of "Turn on security key sign-in" to "Enabled“ (next page)

Enable Security Key in Windows

3. Set the state of "Turn on security key sign-in" to "Enabled“ (next page)



LED of ATKey.Pro

What the LEDs mean

Blue LED ON	Power ON
Green LED ON	Fingerprint verification success
Red LED ON	Fingerprint verification fail / Erase fingerprint / Reset key
Cyan LED ON	OS has not yet recognized this key
Blue LED flashes	Need to verify fingerprint
Cyan LED flashes	Need to touch
White LED flashes	Standalone enrollment (flashes from slow to fast)
Green LED flashes	Verify fingerprint to start 'Standalone Enrollment' (If there is any registered fingerprint)

ATKEY.Pro

AUTHENTREND

Start passwordless with your company.

www.AuthenTrend.com


contact@authentrend.com


AuthenTrend


AuthenTrend technology inc.