NO MORE PASSWORD

Passwordless authentication for Azure AD (Entra ID) by ATKey

AUTHENTREND







- 1. [Admin] Azure AD settings
- a) app, then register FIDO Key
- b)

- 2. [User] ATKey Fingerprint
- a)
- b)

- 3. [User] Register ATKey to your Azure AD account
- a) app, then register FIDO Key
- b)

4. [User] Login via ATKey

- Passwordless login to joined Azure AD Windows PC
- Login Microsoft Services (Azure AD, Microsoft 365, OneDrive, Teams,)

by default, you will be asked to register your phone number or Microsoft Authenticator

But if you just want FIDO key only, setting a temporary access pass, then enable FIDO Key

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

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

by default, you will be asked to register your phone number or Microsoft Authenticator

But if you just want FIDO key only, setting a temporary access pass, then enable FIDO Key

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 (<u>https://portal.azure.com/</u>) 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

Manage

💄 Users

Groups

Company branding

User settings

Properties

| | | Fig. 1 |
|----------------------------------|-----------|--------|
| Method | Target | Enabl |
| 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 |

Enable and Target Con GENERAL Allow self-service set up Enforce attestation KEY RESTRICTION POLICY Enforce key restrictions Restrict specific keys Add AAGUID No AAGuids have been added.

AUTHENTREND

5. Fido Security Key optional Settings

| figure | | |
|--------|-------|-------|
| | Yes | No |
| | Yes | No |
| | Yes | No |
| | Allow | Block |

•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/atkeyfido2-security-key-aaguids/

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 <u>Azure portal</u> 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

| Got feedback? | | |
|--|---|---|
| nfigure your users in the authentication method thentication methods and use them to sign in. | is policy to enable passwordless authentication. Once c | onfigured, you will need to enable your users for the |
| fethod | Target | Enabled |
| IDO2 Security Key | All users | Yes |
| ficrosoft Authenticator | | No |
| ext message (preview) | | No |
| extinessage (preview) | | |

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

| Home > Authentication methods Policies > | | |
|--|--|----------------------|
| Temporary Access Pass settings | | |
| | | |
| Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service | w accounts, account recovery, or when other auth methods are unaverage Password Reset. | ailable. Learn more. |
| Enable and Target Configure | | |
| Enable | | |
| Include Exclude | | |
| Target 💿 All users 🔘 Select groups | | |
| Name | Туре | Registration |
| All users | Group | Optional |

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

| Home > Authentication meth | ods Policies > | Temporary Access Pass settings \times |
|--|---|---|
| Temporary Access Pass, or TAP, is other auth methods are unavaila TAP is issuable only by administration. Enable and Target Config GENERAL | s Pass settings s a time-limited or limited-use passcode that can be used ble. Learn more. ators, and is seen by the system as strong authentication. ure | Temporary Access Pass is a time-limited passcode that serves as strong credentials and allow onboarding of passwordless credentials. The Temporary Access Pass authentication method policy can limit the duration of the passes in the tenant between 10 minutes to 30 days. Learn more Minimum lifetime Minutes • Hours Days |
| Minimum lifetime: Maximum lifetime: Default lifetime: One-time: Length: Edit | 1 hour 1 day 1 hour No 8 characters | Maximum lifetime Minutes Hours Days Minutes Hours Days Menutes Hours Note Minutes |
| Save Discard | | Update Cancel |

*please check below link for more details: https://learn.microsoft.com/en-us/azure/activedirectory/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.

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

| | | Choose method |
|--|--|--|
| | Add authentication method | Temporary Access Pass 🗸 |
| Manage | Want to switch back to the old user authentication methods experience? Click here to | Create a Temporary Access Pass for Chris Green. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more |
| 🚨 Profile | Authentication methods are the ways your users sign into Azure AD and perform SSPR. | Delayed start time |
| Custom security attributes (preview) | Usable authentication methods | Activation duration ① O 1 hours |
| Assigned roles | Authentication method | One-time use |
| Administrative units | No usable methods. | Yes No |
| A Groups | | |
| Applications | | |
| 🔓 Licenses | | |
| Devices | | |
| Azure role assignments | | |
| Authentication methods | | |
| | | |

AUTHENTREND

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**.

| me > Chris Green | | Temporary Access Pass details | \times | |
|--------------------------------------|--|---|--------------|---|
| Chris Green Auther | ntication methods | | | J |
| User « | + Add authentication method 🛛 🖉 Reset password 🏮 Require re-register N | Provide Pass Provide this Temporary Access Pass to the user so they can set their strong credentials. | | |
| Diagnose and solve problems | Want to switch back to the old user authentication methods experience? Click here to | 7^b\$g2jk | \mathbb{D} | |
| nage | | Secure registration | | |
| Profile | Authentication methods are the ways your users sign into Azure AD and perform SSPR. | To register their credentials, have the user go to My Security Info. | | |
| Custom security attributes (preview) | Usable authentication methods | https://aka.ms/mysecurityinfo | \mathbb{D} | l |
| Assigned roles | Authentication method | Additional information | | |
| Administrative units | Temporary Access Pass | Valid from 5/24/2022, 3:08:12 PM | | |
| Groups | | Valid until 5/24/2022, 4:08:12 PM | | |
| Applications | | Created 5/24/2022, 3:08:13 PM | | |
| Licenses | | | | |
| Devices | | Remove lost devices from the user's account. This is especially important for devices used for user authentication. | | |
| Azure role assignments | | | | |
| Authentication methods | | | | |
| tivity | | | | l |
| Sign-in logs | | | | |
| Audit logs | | | | |
| ubleshooting + Support | | | | |
| New support request | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | ٣ |
| | | Ok | | |
| | | | | |

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

Step 2.a [User] ATKey Fingerprint

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

Open Windows Settings

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

Availability: In Windows 1903 and above.



Add Your Fingerprint 3

2

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



AUTHENTREND



Set the PIN of ATKey

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



Step 2.b [User] ATKey Fingerprint

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

) 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 <u>12</u> <u>times</u> good enrollments, until LED stays on "Cyan", then the enrollment is done.
- If you want to quit "standalone enrollment", press the button and the LED will turn to

AUTHENTREND



Blue, back to the normal state. step 4, that you need to verify



Fingerprint good enrollment can help for verification much quick and easier, please check below video as the tips for good enrollment: <u>https://youtu.be/bCLPMtZJhkM</u> (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

- Browse to https://myprofile.microsoft.com, Sign in if not already
- 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 Fig. 3-2 choosing Security key.
 - Choose USB device or NFC device. Fig. 3-3 5)
 - Have your key ready and choose **Next**. 6)
 - perform the required gesture for the key, either biometric or touch. 7)
 - The user will be returned to the combined registration experience 8) 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.

| ::: My Account \lor | | | Fig. 3-1 |
|-----------------------|---------------------------------------|--|---|
| A Overview | | | |
| ♀ Security info | | | |
| □ Devices | | | |
| 💊 Password | | | / L |
| 🖻 Organizations | | Find, launch and organize all your productivity apps. | Disable a lost device connected (|
| 🐯 Settings & Privacy | N.C. Milliou camife Landit? | VISIT DASHBOARD > | MANAGE DE' |
| ℅ My sign-ins | wity can be edite | / | |
| - Office apps | | | |
| Subscriptions | | Security info | Passw |
| 🖗 Give feedback | | ~ 20 | Q |
| | | Keep your verification methods and security info up to date. | Make your password stre someone else |
| | | UPDATE INFO > | CHANGE PASS |

| JCC | anty into =2 | - Auu s | л <u>ө</u> н п |
|---------------------|---|--|-----------------------------------|
| Sec | urity info | | |
| These a | ire the methods you use | to sign into your acc | ount or rese |
| Defaul | t sign-in method: Authe | enticator app or hard | lware token |
| | dd sign-in method | | |
| \$ | Microsoft Authenticator Push multi-factor authentic | ation (MFA) | SM-S9080 |
| Add a | method | Fig. 3-2 | × |
| Which m | nethod would you like to add | ? | 1 |
| Choose | e a method | | \sim |
| Auther | nticator app | | |
| Phone | | | |
| App pa | assword | | |
| Securit | y key | h | |
| | | | |
| | | | |
| M | licrosoft | | |
| zake.h | uang@authentrend.com | | |
| Veri | fy your identity | | |
| ÿ¢ | Use Windows Hello or a se | curity key | |
| Ø | Approve a request on my N Authenticator app | Лicrosoft | |
| 123 | Use a verification code | If any auther method regis select it to lo | ntication stered, ogin acco |
| More in | nformation | | |
| Are you https:// | ur verification methods current? Cł 'aka.ms/mfasetup | ieck at | |
| | | Cancel | |
| | 1 | | |
| | | | |
| | | | |

AUTHENTREND

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.

| Sign in | |
|----------------------------|----------|
| userid@domain | name.com |
| Can't access your account? | 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.



AUTHENTREND

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 onpremises 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)





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

AUTHENTREND

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

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.



"gpedit.msc" > press "OK"

| 💷 Run | | × |
|-------|--|--------|
| | Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. | |
| Open: | gpedit.msc | \sim |
| | OK Cancel <u>B</u> rowse | |

- Administrative Templates > System > Logon

AUTHENTREND

1. Launch the "Run" command by pressing the "Windows+R" simultaneously > Type

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

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)

| Local Group Policy Editor | | | | | |
|------------------------------|--|---|----------------|---------|--|
| File Action View Help | | | | | |
| 🗢 🔿 🙍 🔂 🔂 🖬 🍸 | | | | | |
| I Local Computer Policy | Logon | | | | |
| Computer Configuration | Turn on security key sign-in | Setting | State | Comment | |
| Software Settings | | Allow users to select when a password is required when resu | Not configured | No | |
| Administrative Templates | Edit policy setting | Turn on convenience PIN sign-in | Not configured | No | |
| Control Panel | Requirements | Turn on security key sign-in | Enabled | No | |
| Conton uncl | At least Windows 10 | Turn off picture password sign-in | Not configured | No | |
| > Network | | Assign a default credential provider | Not configured | No | |
| Printers | Description: | Assign a default domain for logon | Not configured | No | |
| Server | This policy setting allows you to | Exclude credential providers | Not configured | No | |
| > 🧮 Start Menu and Taskbar | using external security keys. | Block user from showing account details on sign-in | Not configured | No | |
| ✓ | | E Show clear logon background | Not configured | No | |
| Access-Denied Assistan | If you enable this policy setting, users | Do not process the legacy run list | Not configured | No | |
| > 🧮 App-V | can sign in with external security keys. | Do not process the run once list | Not configured | No | |
| Audit Process Creation | If you disable or don't configure this | Turn off and potifications on the lock screen | Not configured | No | |
| Credentials Delegation | policy setting, users can't sign in with | Turn off Windows Startup sound | Not configured | No | |
| 📔 Device Guard | external security keys. | E Turn on windows startup sound | Not configured | No | |
| Device Health Attestatic | | Do not display network selection of | Not configured | No | |
| > 🧾 Device Installation | | Do not enumerate connected users on domain-joined comp | Not configured | No | |
| 🔛 Disk NV Cache | | Show first sign-in animation | Not configured | No | |
| Disk Quotas | | Enumerate local users on domain-joined computers | Not configured | No | |
| Display | | Hide entry points for Fast User Switching | Not configured | No | |
| Distributed COM | | Always use classic logon | Not configured | No | |
| Driver Installation | | Do not display the Getting Started welcome screen at logon | Not configured | No | |
| 📔 Early Launch Antimalwa | | E Run these programs at user logon | Not configured | No | |
| Enhanced Storage Acce: | | E Always wait for the network at computer startup and logon | Not configured | No | |
| 📔 File Classification Infras | | 📰 Always use custom logon background | Not configured | No | |
| 📔 File Share Shadow Copy | | | | | |
| > 🧾 Filesystem | | | | | |
| E Folder Redirection | | | | | |
| Group Policy | | | | | |
| Internet Communication | | | | | |
| > 🔛 iSCSI | | | | | |
| KDC | | | | | |
| Kerberos | | | | | |
| Kernel DMA Protection | | | | | |
| LAPS | | | | | |
| Local Security Authority | | | | | |
| Locale Services | | | | | |
| Logon | | | | | |
| Mitigation Options | | | | | |
| > Net Logon | | | | | |
| OS Policies | | | | | |
| PIN Complexity | | | | | |
| Bower Management | Extended Standard | | | | |

23 setting(s)

AUTHENTREND



LED of ATKey.Pro

What the LEDs mean



 \cap

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



AUTHENTREND



AUTHENTREND

Start passwordless with your company.







AuthenTrend



- www.AuthenTrend.com
- contact@authentrend.com
- AuthenTrend technology inc.