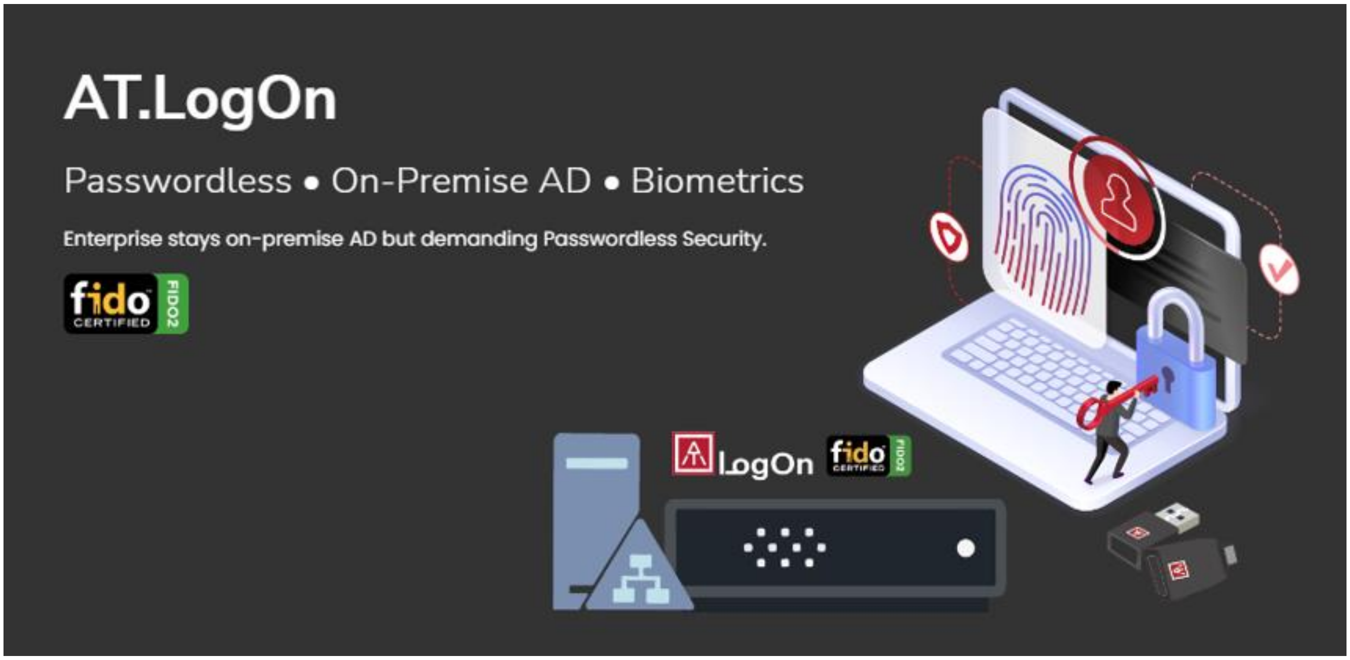
AUTHENTREND

LogOn

User Guide *(for Administrator)*


AT.LogOn
Passwordless • On-Premise AD • Biometrics
Enterprise stays on-premise AD but demanding Passwordless Security.
fido CERTIFIED FIDO2
LogOn
fido CERTIFIED FIDO2

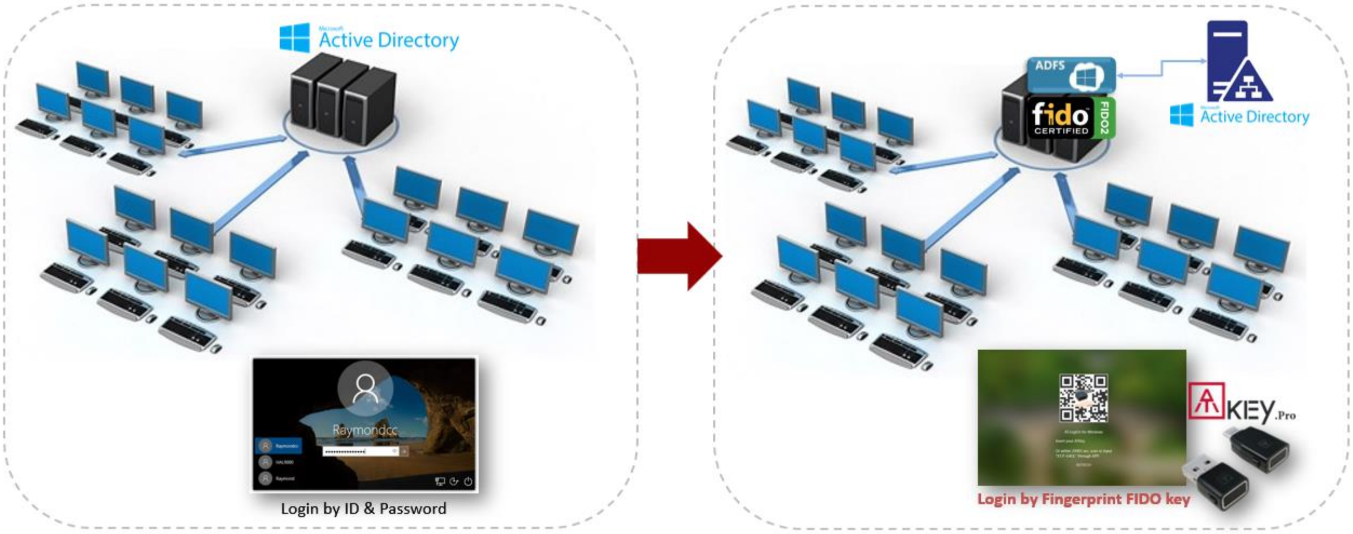
REVISION: 1.4
DATE: 2023 APR.

Table of Contents

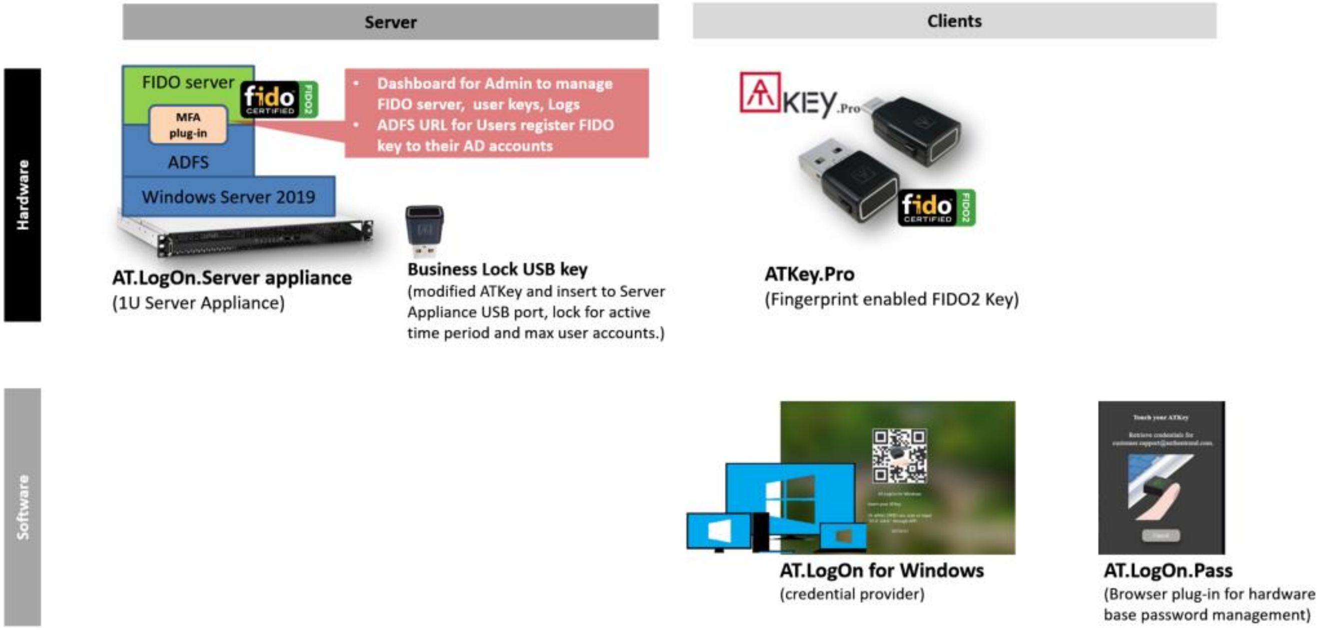
Table of Contents 1
1. About AT.LogOn 2
a) AT.LogOn includes below parts 2
b) AT.LogOn can achieve Passwordless login for below functionalities 3
c) AT.LogOn defined multiple roles and this user guide is targeting on "Customer IT Administrator" 3
2. IT Administrator – Initialization and Registration 4
a) URLs definitions and Highlights 4
b) AT.LogOn.Server initialization 4
c) Assign ATKey.Pro to employees 12
d) Deploy (install) "AT.LogOn for Windows" to employees PC 16
e) User cases for Admin 17
3. Employees Windows Logon 20
a) Enroll fingerprint 20
b) Register ATKe.Pro to AD account 20
c) 1st login vs. from 2nd login 23
d) Domain vs. outside domain 23
e) Online/offline 23
f) User cases from ATKey (for employees) 23
4. AT.LogOn Server management 26
a) Assign admin 26
b) Hotkey and Recovery code 27
c) Registered Users management 29
d) API Logs 30
5. RDP – Remote Desktop 32
a) Criteria of Host PC, Remote PC and AD settings 32
b) User cases for RDP 34
6. AT.LogOn.Pass 36
a) Chrome extension 36
b) Chrome whitelist 41
c) AT.LogOn.Pass via RDP 41
7. More from ATKey.Pro 45

1. About AT.LogOn

AT.LogOn is targeting on enterprise who stays in on-premise Active Directory environment (joined AD domain PCs), bringing FIDO2 Passwordless to secure AD credentials, simplify user experience and also reduce IT management efforts.



a) AT.LogOn includes below parts



Server

Clients

Hardware

FIDO server

MFA plug-in

ADFS

Windows Server 2019

- Dashboard for Admin to manage FIDO server, user keys, Logs
- ADFS URL for Users register FIDO key to their AD accounts

AT.LogOn.Server appliance
(1U Server Appliance)

Business Lock USB key
(modified ATKey and insert to Server Appliance USB port, lock for active time period and max user accounts.)

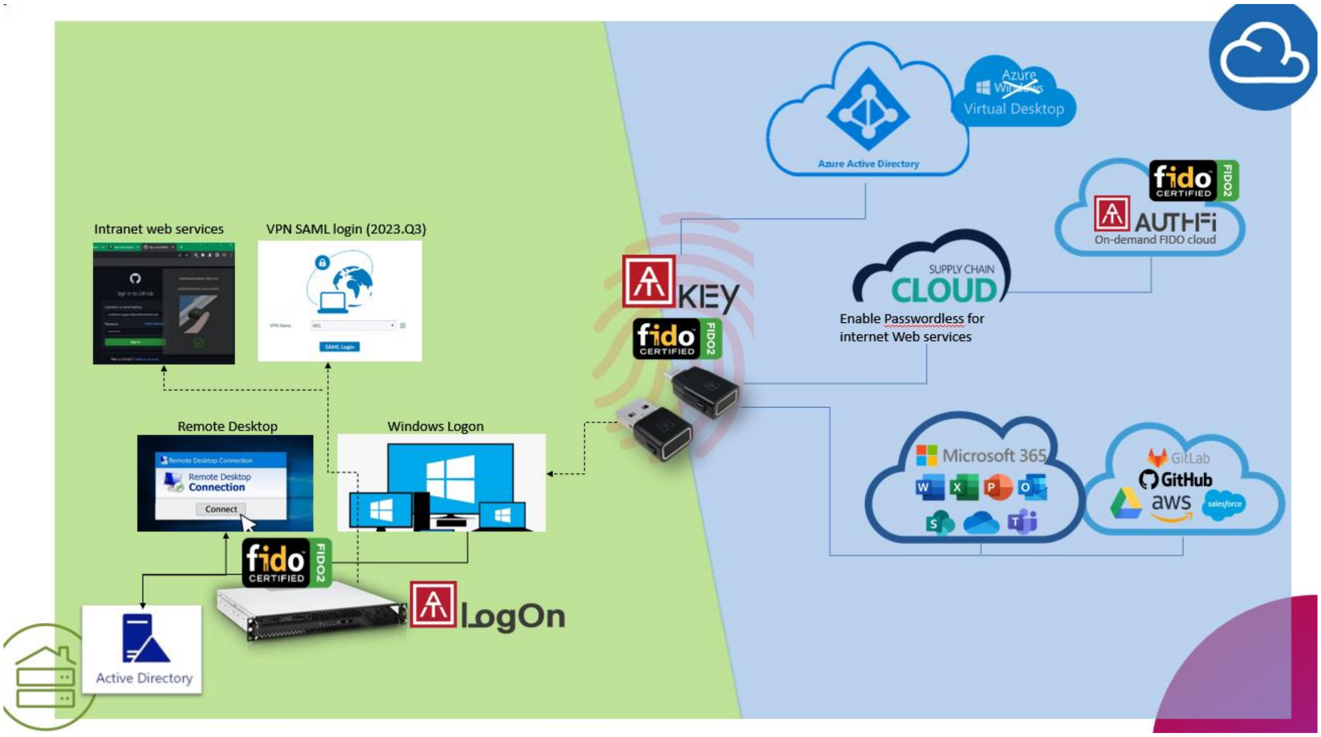
ATKey.Pro
(Fingerprint enabled FIDO2 Key)

Software

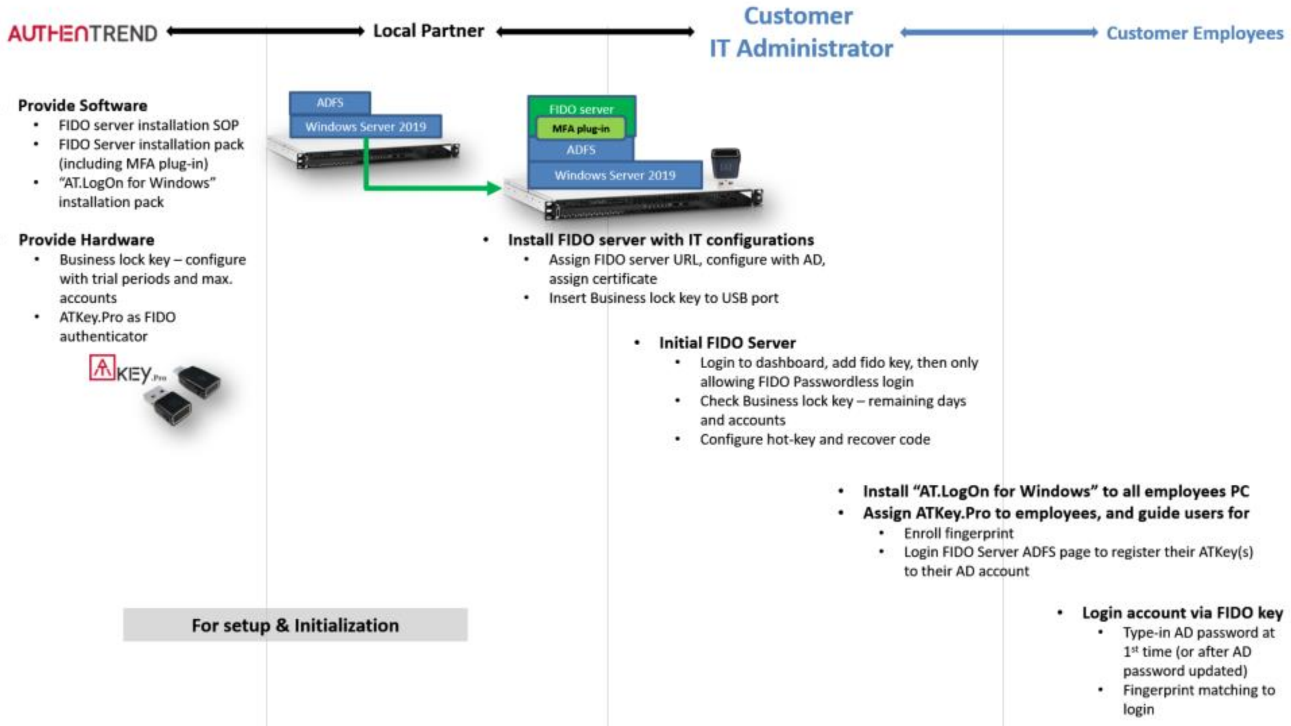
AT.LogOn for Windows
(credential provider)

AT.LogOn.Pass
(Browser plug-in for hardware base password management)

b) AT.LogOn can achieve Passwordless login for below functionalities



c) AT.LogOn defined multiple roles and this user guide is targeting on "Customer IT Administrator"



- **Provide Software**
  - FIDO server installation SOP
  - FIDO Server installation pack (including MFA plug-in)
  - "AT.LogOn for Windows" installation pack
- **Provide Hardware**
  - Business lock key – configure with trial periods and max. accounts
  - ATKey.Pro as FIDO authenticator

- **Install FIDO server with IT configurations**
  - Assign FIDO server URL, configure with AD, assign certificate
  - Insert Business lock key to USB port

- **Initial FIDO Server**
  - Login to dashboard, add fido key, then only allowing FIDO Passwordless login
  - Check Business lock key – remaining days and accounts
  - Configure hot-key and recover code

- **Install "AT.LogOn for Windows" to all employees PC**
- **Assign ATKey.Pro to employees, and guide users for**
  - Enroll fingerprint
  - Login FIDO Server ADFS page to register their ATKey(s) to their AD account

- **Login account via FIDO key**
  - Type-in AD password at 1st time (or after AD password updated)
  - Fingerprint matching to login

For setup & Initialization

2. IT Administrator – Initialization and Registration

a) URLs definitions and Highlights

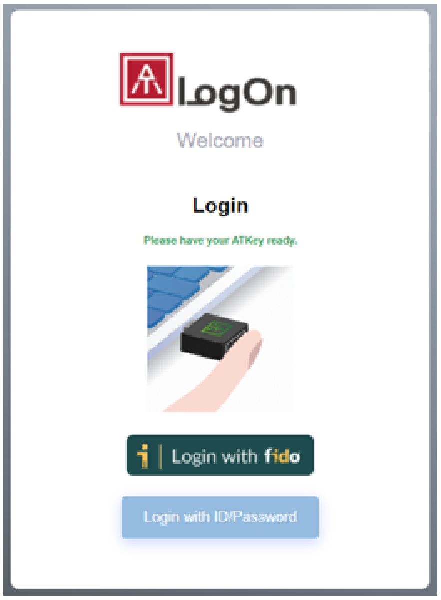
- Before start, please pay attention to below definitions:
  - ADFS URL
    - This URL also defined inside “AT FIDO server” pack (config.properity) for AT.LogOn.Server installation (by local partner)
    - This needs to be pre-defined during Server installation by local partner, normally it’s:
      - ✓ adfs01.domainname.com (for example “adfs01.atlogon.com”)
    - This URL also needs to define inside “AT.LogOn for Windows” batch file for silence installation to employees PCs
  - Register ATKey URL
    - register user’s ATKey.Pro to user AD account
    - URL assigned automatically by ADFS
      - ✓ If your ADFS URL is “adfs01.domainname.com”, then it will be “//adfs01.domainname.com/adfs/ls/idpinitiatedsignon”
  - AT.LogOn.Server Dashboard URL
    - This is for Administrator to login to manage AT.LogOn.Server
    - It will be “//adfs01.domainname.com/dashboard/”

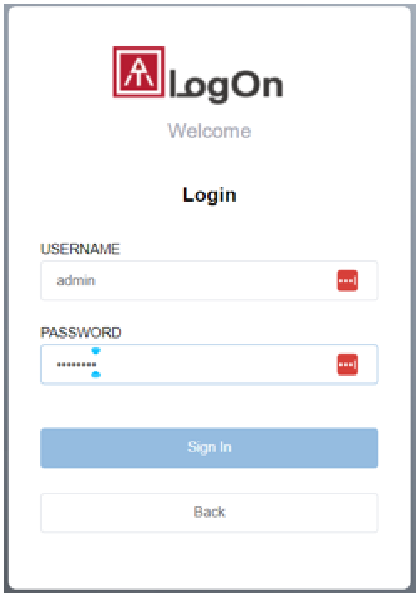
b) AT.LogOn.Server initialization

Flow:

(1) Login => (2) change ID/Password => (3) register ATKey.Pro => (4) check business lock status => (5) enable “Hot-key” & “Recovery code”

- 1st Login (“https://adfs01.domainname.com/dashboard/”) – Login with ID/Password



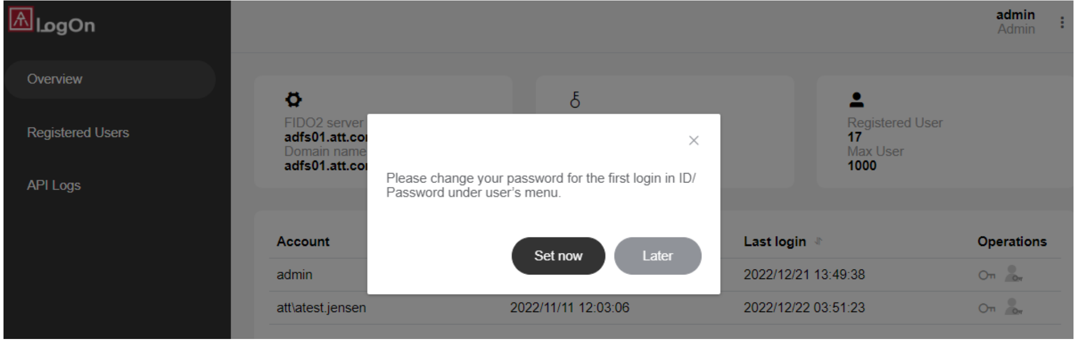


USERNAME: admin

PASSWORD: ••••••••

  - Default ID/password:
    - ID: admin
    - Password: password

    - Login-ed, it will ask you to change login ID and Password

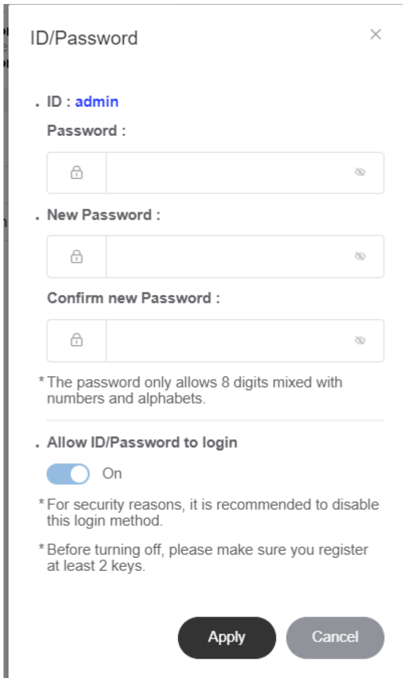


FIDO2 server
adfs01.att.co
Domain name
adfs01.att.co

Registered User
17
Max User
1000

Please change your password for the first login in ID/ Password under user's menu.

Account		Last login	Operations
admin		2022/12/21 13:49:38	
att\atest.jensen	2022/11/11 12:03:06	2022/12/22 03:51:23	


ID/Password

- ID : admin
  Password :
- New Password :
  Confirm new Password :

  * The password only allows 8 digits mixed with numbers and alphabets.
- Allow ID/Password to login

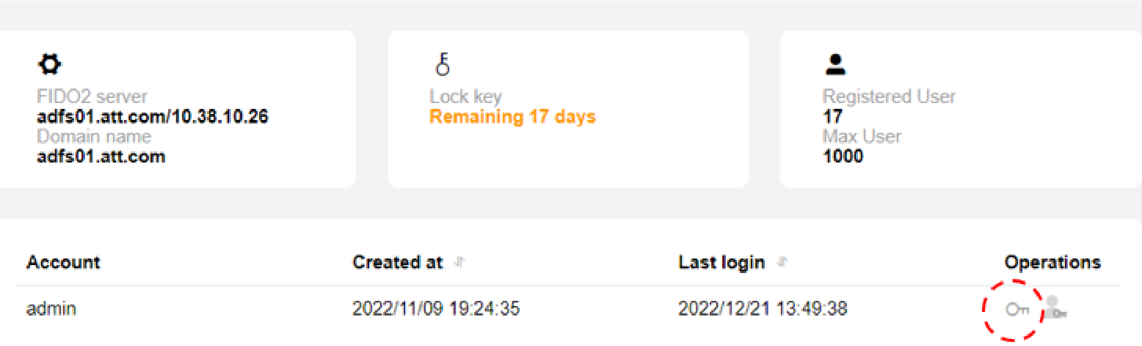
  On

  * For security reasons, it is recommended to disable this login method.

  * Before turning off, please make sure you register at least 2 keys.

- ✓ You can register ATKey.Pro as Passwordless login authenticator instead Password
  - ○ *Please enroll fingerprint to the specific ATKey.Pro before register to admin*
- ✓ “Allow IS/Password” still just an option in case you lost the ATKey.Pro and only you (one) administrator.

○ Register your ATKey.Pro for admin passwordless login

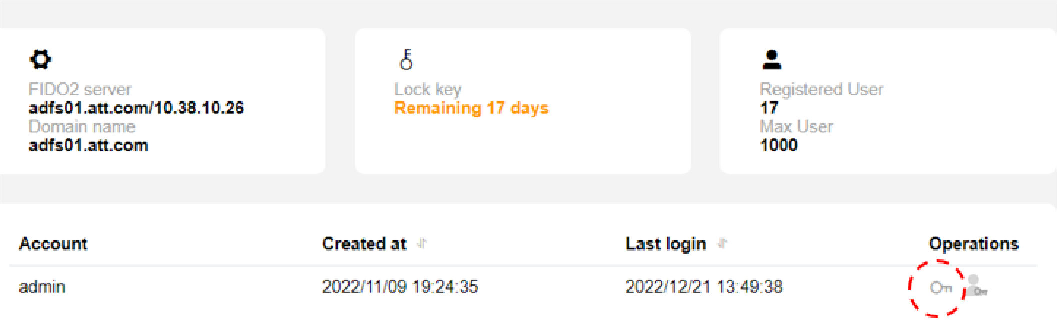

FIDO2 server
adfs01.att.com/10.38.10.26
Domain name
adfs01.att.com

Lock key
Remaining 17 days

Registered User
17
Max User
1000

Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/21 13:49:38	

- ▪ Click the “key” icon (above red circle highlighted one)



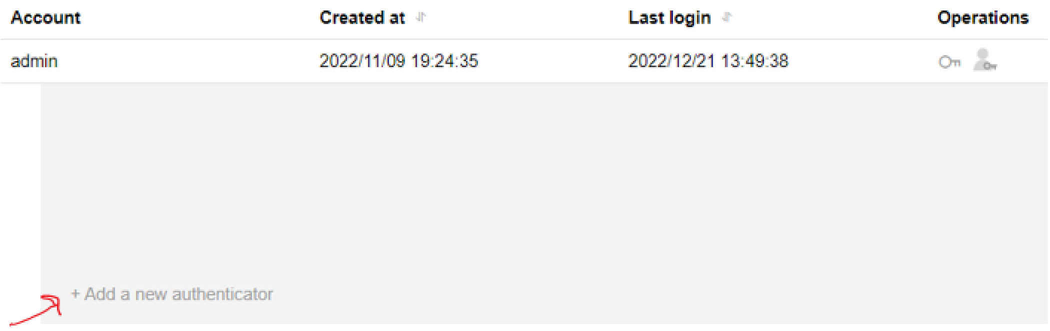
FIDO2 server
adfs01.att.com/10.38.10.26
Domain name
adfs01.att.com

Lock key
Remaining 17 days

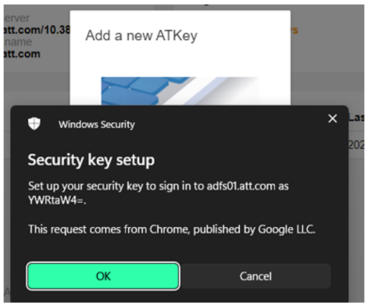
Registered User
17
Max User
1000

Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/21 13:49:38	

- Click “+ Add a new authenticator”



Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/21 13:49:38	



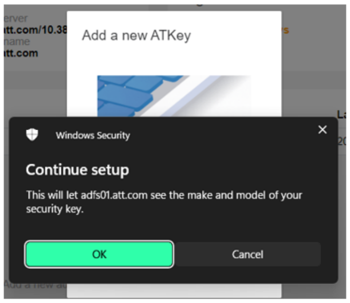
Add a new ATKey

Windows Security

Security key setup

Set up your security key to sign in to adfs01.att.com as YWRtaW4=.

This request comes from Chrome, published by Google LLC.

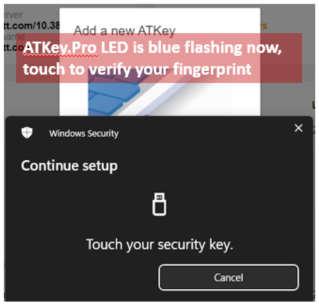


Add a new ATKey

Windows Security

Continue setup

This will let adfs01.att.com see the make and model of your security key.



Add a new ATKey

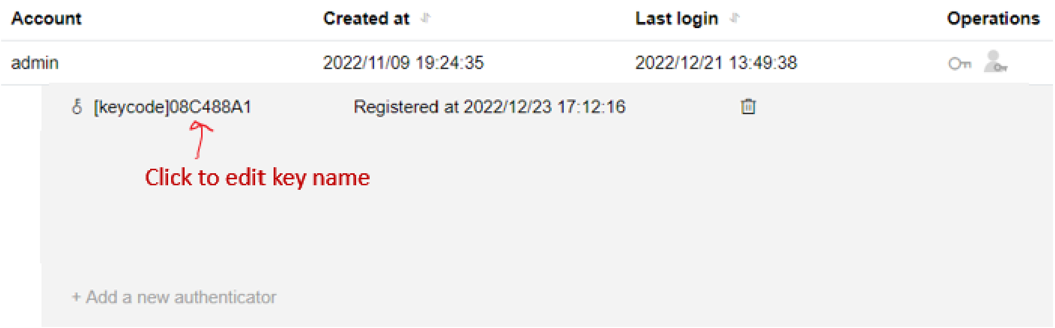
ATKey.Pro LED is blue flashing now, touch to verify your fingerprint

Windows Security

Continue setup

Touch your security key.

- If it’s success, new authenticator added and showed; click to rename – we will recommend using unique keycode inked on key



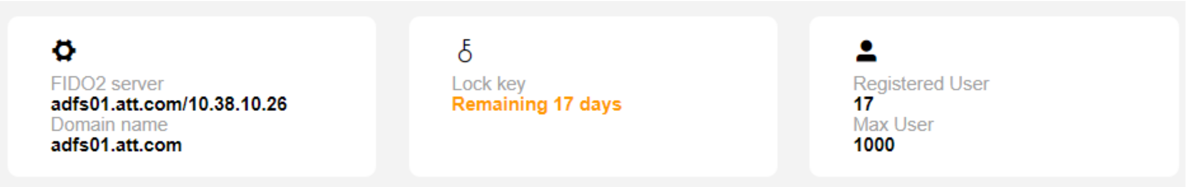
Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/21 13:49:38	

[keycode]08C488A1 Registered at 2022/12/23 17:12:16

Click to edit key name

✓ *If you prefer to disable ID/Password, we will recommend to register at least 2 keys (authenticators) to admin account to avoid key lost.*

- Check status of Business Lock Key



FIDO2 server
adfs01.att.com/10.38.10.26
Domain name
adfs01.att.com

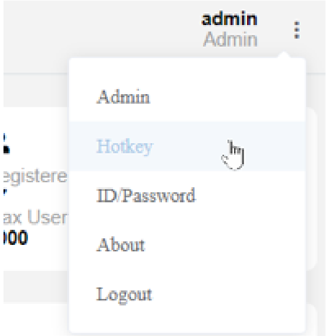
Lock key
Remaining 17 days

Registered User
17
Max User
1000

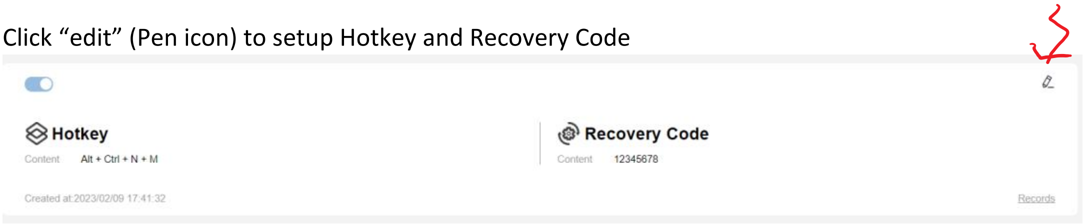
  - Here are Server and URL information at 1st block
  - 2nd block shows – remaining days of business lock key
    - ✓ Business lock key initial from 1st login (starting countdown for remaining days)
    - ✓ Less than 30 days, string is yellow, business lock key is Yellow flashing; contact server provider to renew business lock key (switch to new one)
    - ✓ Expired, string is RED, business lock key shows RED LED also and locked (authentication won't work); contact to renew business lock key (witch to new one)

- Setup "Hotkey" and "Recovery Code"
  - This is for users to login via their AD ID/Password from some urgent user cases

    Enter from admin list box



Click "edit" (Pen icon) to setup Hotkey and Recovery Code

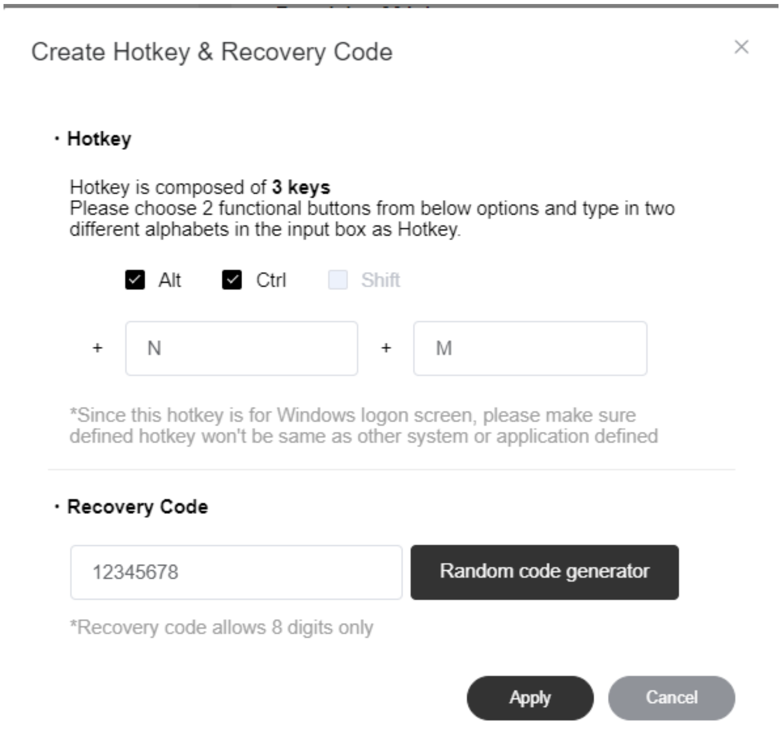


Hotkey
Content Alt + Ctrl + N + M

Recovery Code
Content 12345678

Created at 2023/02/09 17:41:32

Following Hotkey rule here to setup, and type in Recovery Code or random generate it



Create Hotkey & Recovery Code

· **Hotkey**

Hotkey is composed of **3 keys**
Please choose 2 functional buttons from below options and type in two different alphabets in the input box as Hotkey.

☑ Alt ☑ Ctrl □ Shift

+ N + M

*Since this hotkey is for Windows logon screen, please make sure defined hotkey won't be same as other system or application defined

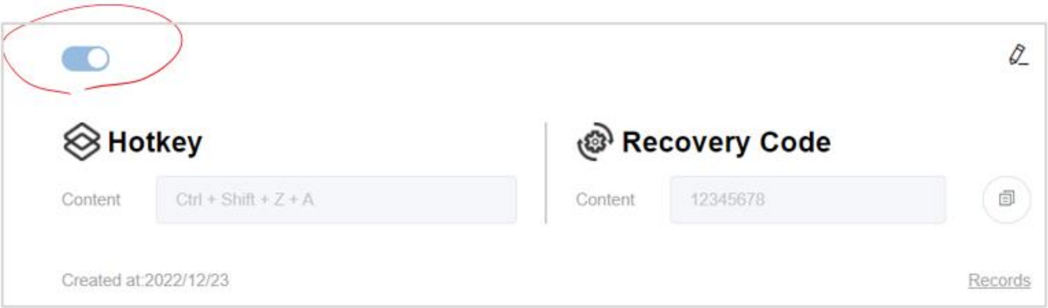
· **Recovery Code**

12345678

*Recovery code allows 8 digits only

**Note: we won't support "Windows key" for the combination from AT.FIDO.Server 2.00.08 to avoid any conflicts with other applications*

"Apply", remember to turn this function ON



Hotkey

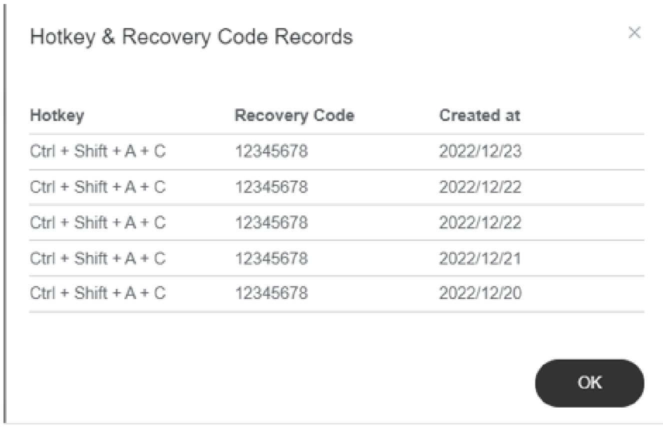
Content: Ctrl + Shift + Z + A

Recovery Code

Content: 12345678

Created at:2022/12/23

- ✓ At Windows login screen, if it's online and also joined domain, client ill sync "hotkey" and "Recovery Code" and encrypted locally
- ✓ For better security and management, we will recommend you to change Hotkey and Recovery code frequently, or change it when any user knows to login by it
- ✓ So if a PC needs historic Hotkey and Recovery code (always offline or outside the domain), you can check "Records" to see what's the Hotkey and Recover code to login

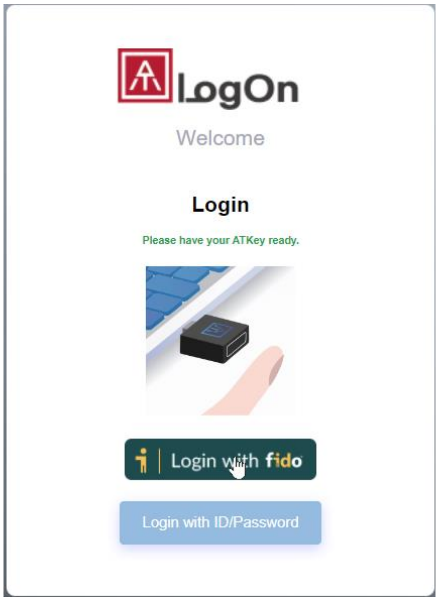


Hotkey & Recovery Code Records

Hotkey	Recovery Code	Created at
Ctrl + Shift + A + C	12345678	2022/12/23
Ctrl + Shift + A + C	12345678	2022/12/22
Ctrl + Shift + A + C	12345678	2022/12/22
Ctrl + Shift + A + C	12345678	2022/12/21
Ctrl + Shift + A + C	12345678	2022/12/20

  - Then, AT.LogOn.Server initialization and setup is done; please logout
    - Manually logout, or close browser to close the session;
    - If Admin did not logout or close Browser tab, we will logout it after 10 minutes; but during the period of time, same admin account can't login.

- From 2nd login
  - Login via registered ATKey.Pro

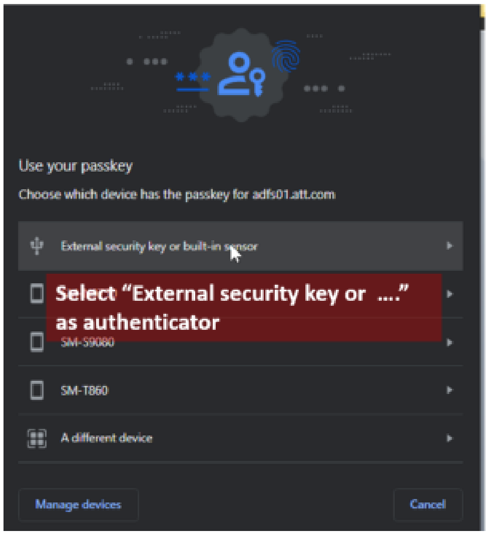


LogOn

Welcome

Login

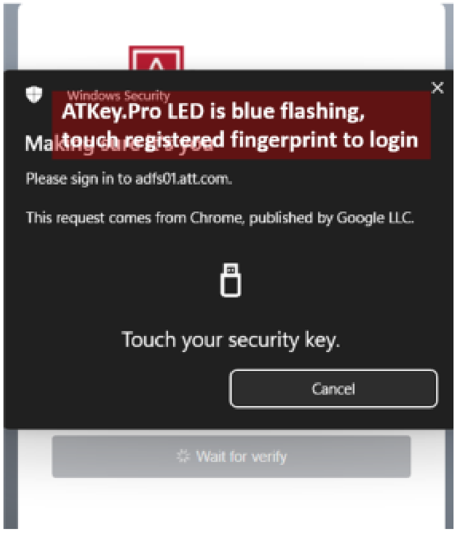
Please have your ATKey ready.



Use your passkey

Choose which device has the passkey for adfs01.att.com

Select "External security key or ...." as authenticator



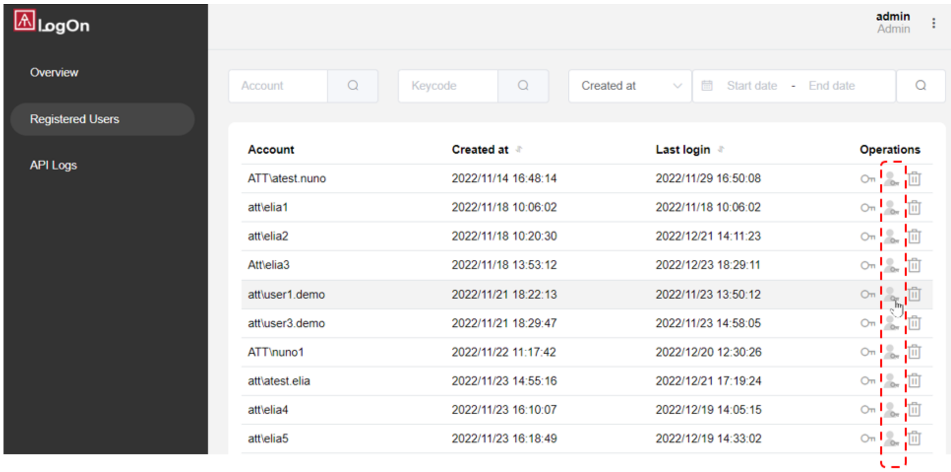
ATKey.Pro LED is blue flashing, touch registered fingerprint to login

Please sign in to adfs01.att.com.

This request comes from Chrome, published by Google LLC.

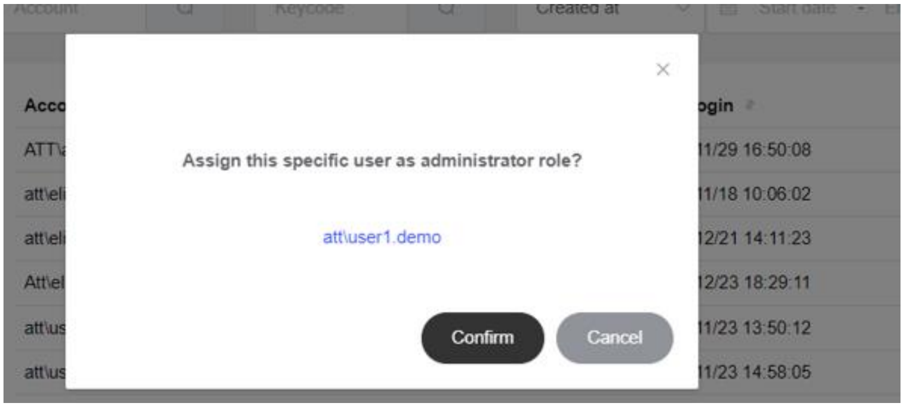
Touch your security key.

- Assign more administrators
  - Admin can select "Registered Users" to assign the administrator authority
    - ✓ Find the specific user, click "admin icon" as below



Account	Created at	Last login	Operations
ATT\atest.nuno	2022/11/14 16:48:14	2022/11/29 16:50:08	
att\elia1	2022/11/18 10:06:02	2022/11/18 10:06:02	
att\elia2	2022/11/18 10:20:30	2022/12/21 14:11:23	
Att\elia3	2022/11/18 13:53:12	2022/12/23 18:29:11	
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	
att\user3.demo	2022/11/21 18:29:47	2022/11/23 14:58:05	
ATT\nuno1	2022/11/22 11:17:42	2022/12/20 12:30:26	
att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	
att\elia4	2022/11/23 16:10:07	2022/12/19 14:05:15	
att\elia5	2022/11/23 16:18:49	2022/12/19 14:33:02	

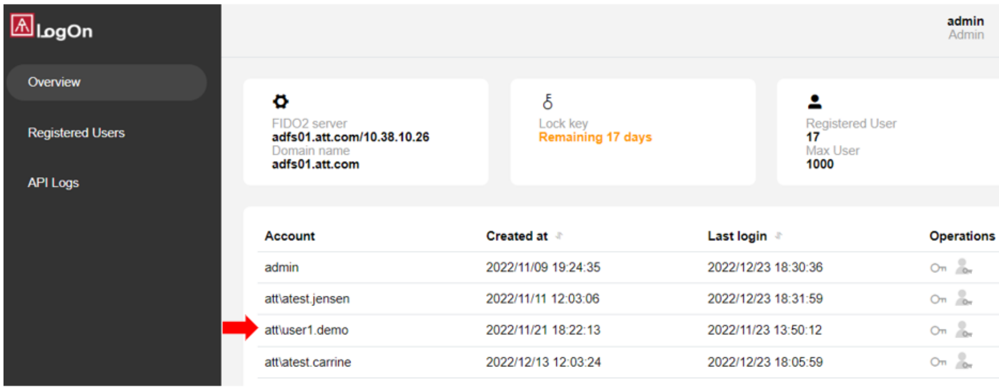
    - ✓ Confirm the user
    - ✓ Then it will show on "Overview" as one of the admin, then the specific user can login



Assign this specific user as administrator role?

att\user1.demo

    - ✓ AT.LogOn.Server dashboard via his/her ATKey.Pro as admin



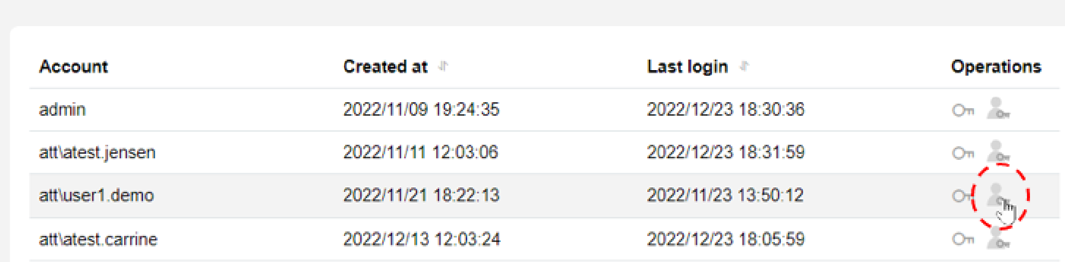
FIDO2 server
adfs01.att.com/10.38.10.26
Domain name
adfs01.att.com

Lock key
Remaining 17 days

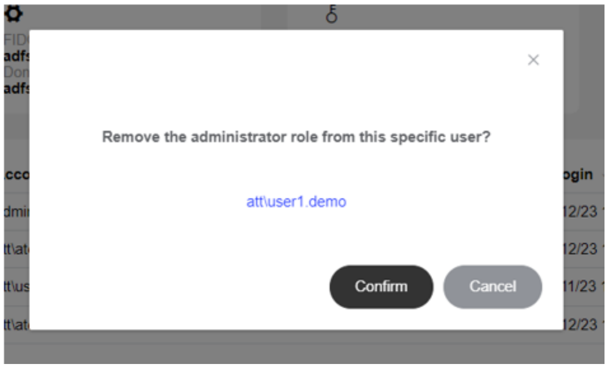
Registered User
17
Max User
1000

Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/23 18:30:36	
att\atest.jensen	2022/11/11 12:03:06	2022/12/23 18:31:59	
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	
att\atest.carrine	2022/12/13 12:03:24	2022/12/23 18:05:59	

- Login-ed Admin can remove another assigned administrator from the list



Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/23 18:30:36	
att\atest.jensen	2022/11/11 12:03:06	2022/12/23 18:31:59	
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	
att\atest.carrine	2022/12/13 12:03:24	2022/12/23 18:05:59	

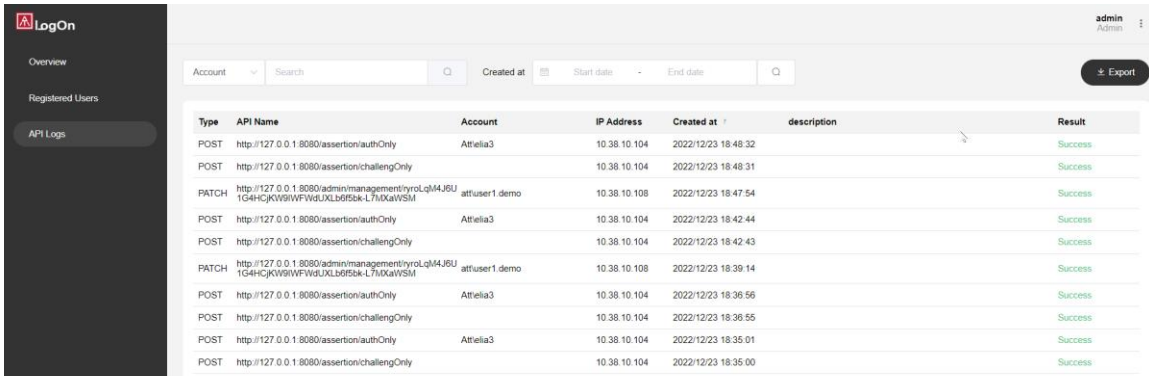


Remove the administrator role from this specific user?

att\user1.demo

- Some highlights for multiple administrators or one admin with multiple keys
  - ✓ We can allow multiple admin logins for management, but it must be different account (same account can't login in parallel via ID/Password or different registered ATKey.Pro)
  - ✓ Please "Logout" if you finish all settings or management.

- API Logs
  - ○ Check or search demanding logs (from every API)



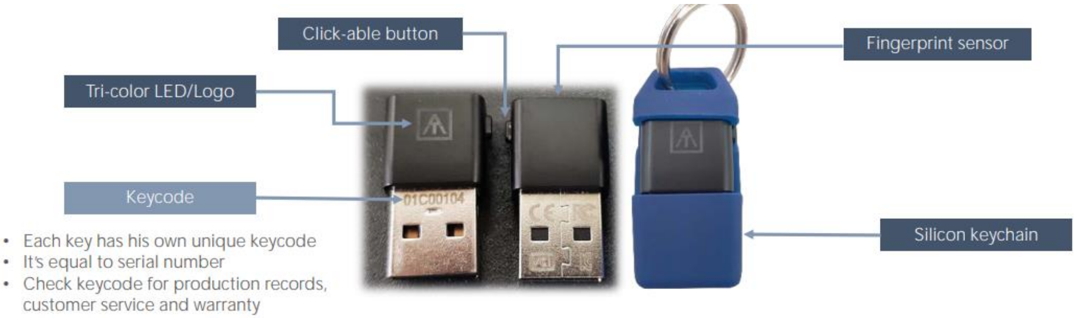
Type	API Name	Account	IP Address	Created at	description	Result
POST	http://127.0.0.1:8080/assertion/authOnly	Att\elia3	10.38.10.104	2022/12/23 18:48:32		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.104	2022/12/23 18:48:31		Success
PATCH	http://127.0.0.1:8080/admin/management/ryroLqM4J6U 1G4HCjKW9IWFWdUXLb6f5bk-L7MXaWSM	att\user1.demo	10.38.10.108	2022/12/23 18:47:54		Success
POST	http://127.0.0.1:8080/assertion/authOnly	Att\elia3	10.38.10.104	2022/12/23 18:42:44		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.104	2022/12/23 18:42:43		Success
PATCH	http://127.0.0.1:8080/admin/management/ryroLqM4J6U 1G4HCjKW9IWFWdUXLb6f5bk-L7MXaWSM	att\user1.demo	10.38.10.108	2022/12/23 18:39:14		Success
POST	http://127.0.0.1:8080/assertion/authOnly	Att\elia3	10.38.10.104	2022/12/23 18:36:56		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.104	2022/12/23 18:36:55		Success
POST	http://127.0.0.1:8080/assertion/authOnly	Att\elia3	10.38.10.104	2022/12/23 18:35:01		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.104	2022/12/23 18:35:00		Success

  - ○ Export necessary logs (dates, type, …) to send out for debug

        - Since API logs might be huge records (all API record), if you want to export as a file and send out for debug, please limit the time period for 3 days as an export file.
        - The export file will be downloaded by browser (default download folder of your browser), the file name is always “ExportLog.csv”.

c) Assign ATKey.Pro to employees

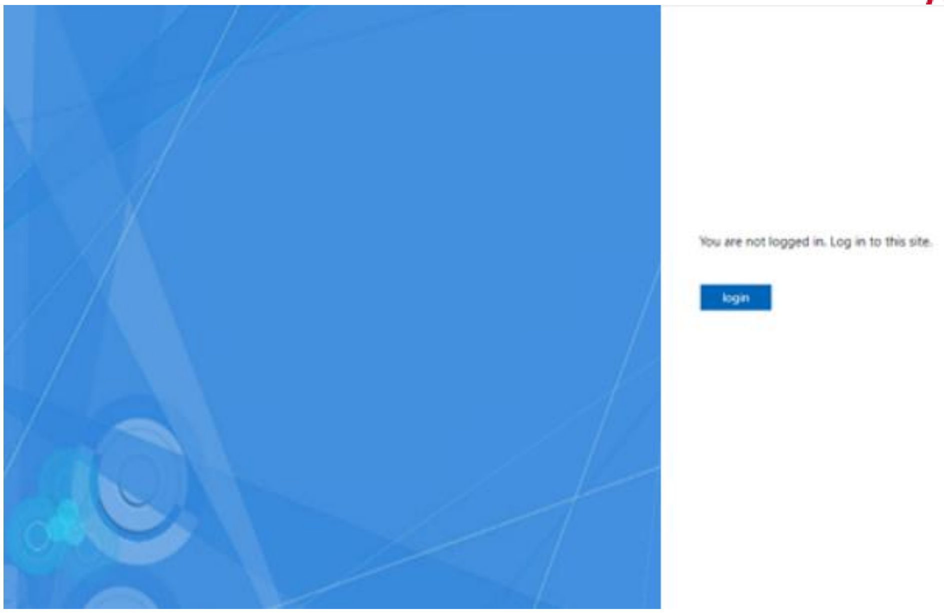
- ATKey.Pro vs. Employees (keycode)
    - Ideally, one key for one employee; each key has an unique keycode both laser ink on key and also stored inside the key (hardware chip).
        - If one ATKey.Pro registered to multiple users, we are doing the same user scenario as Azure AD, it will just login to last login account since ATKey.Pro (FIDO2 key) is a roaming key per user, not a key for multiple users design.
    - During ATKey.Pro registration (to AD account), user needs to type in their keycode, so it’s easier for management (user vs. key).
        - Keycode (8 digits) is the unique code inside Hardware chip, it’s also as serial number of each key


Click-able button
Fingerprint sensor
Tri-color LED/Logo
Keycode
01C00104
Silicon keychain
Each key has his own unique keycode
It's equal to serial number
Check keycode for production records, customer service and warranty

    - One user can have multiple keys (at most 10 keys), one key allows max 10 fingerprints
        - We will recommend to register at least 2 keys for admin; or assign multiple administrators to avoid if key lost
        - We will always recommend to register at least 2 fingers per key, to avoid if one registered finger got something wrong.

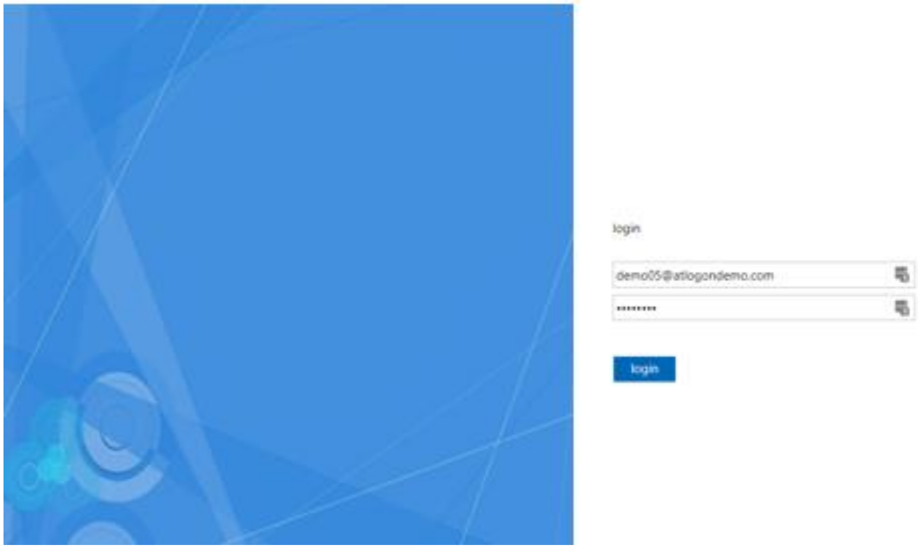
- Guide employees to enroll fingerprint
    - Fingerprint can enroll to ATKey.Pro via
        - Windows Settings (Windows 10 build 1903 and later versions)
        - Chrome browser (Security and privacy) on non-Windows platform
        - Standalone enrollment: https://youtu.be/NnNqXbrf7vA
    - Check the video to understand how to enroll fingerprint well: https://youtu.be/bCLPMtZJhkM
    - We will always recommend to register at least 2 fingers per key.

- register to AD account (Register ATKey URL)
    - Open chrome browser and type in assigned register ATKey URL, (for example): https//adfs01.domainname.com/adfs/ls/idpinitiatedsignon,
        - Please make sure this registration is doing inside domain trust environment, since starting from Chrome 110, webauthn can’t be userd on sites with TLS certification errors



You are not logged in. Log in to this site.

- ○ Sign in by user's AD ID/PWD

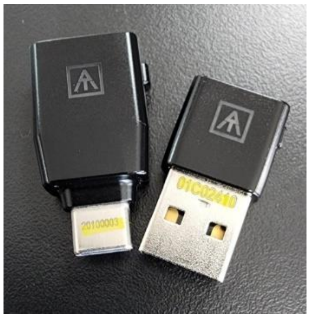


login

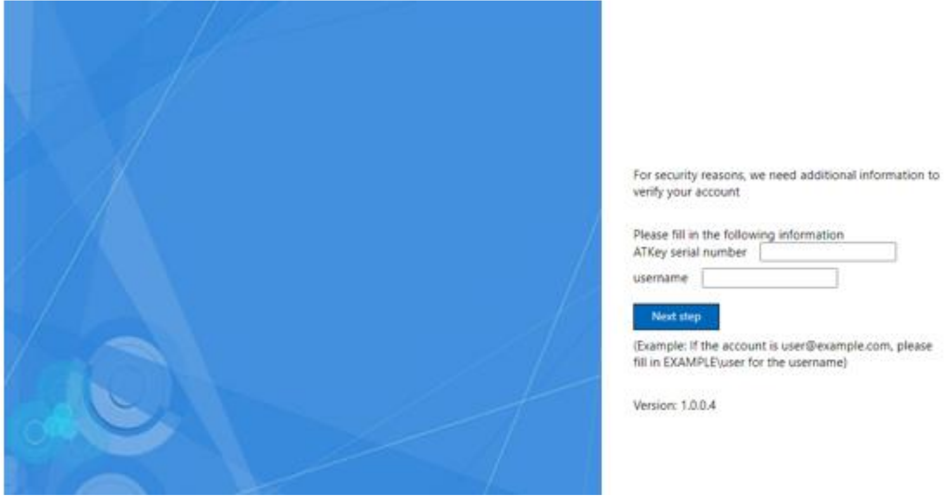
demo05@atlogondemo.com

••••••••

- ○ If it's 1st time to register FIDO authenticator - Enter ATKey.Pro <u>Keycode</u> and <u>User name</u>
  - ▪ Keycode - where is the "keycode of "ATKey.Pro"? check below image, keycode is unique code (8 digits) inside the key and laser inked on surface of the key.



  - ▪ Please be noted – "username" must be totally correct input since it's not changeable.
    - Format: domainname\username



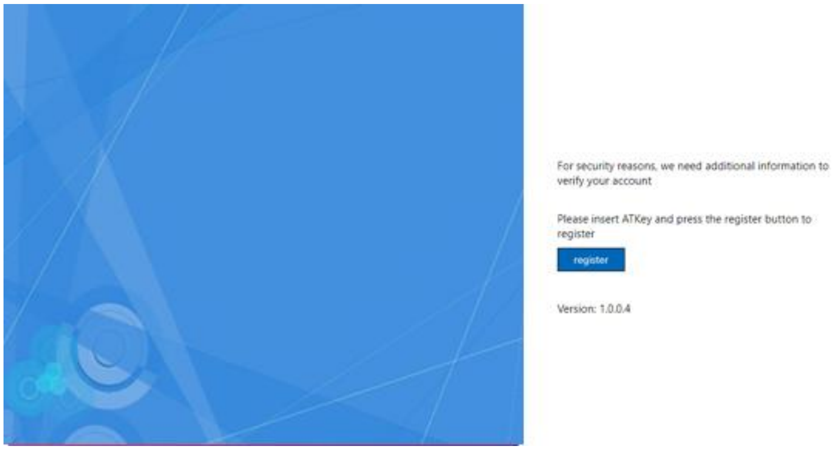
For security reasons, we need additional information to verify your account

Please fill in the following information
ATKey serial number
username

(Example: If the account is user@example.com, please fill in EXAMPLE\user for the username)

Version: 1.0.0.4

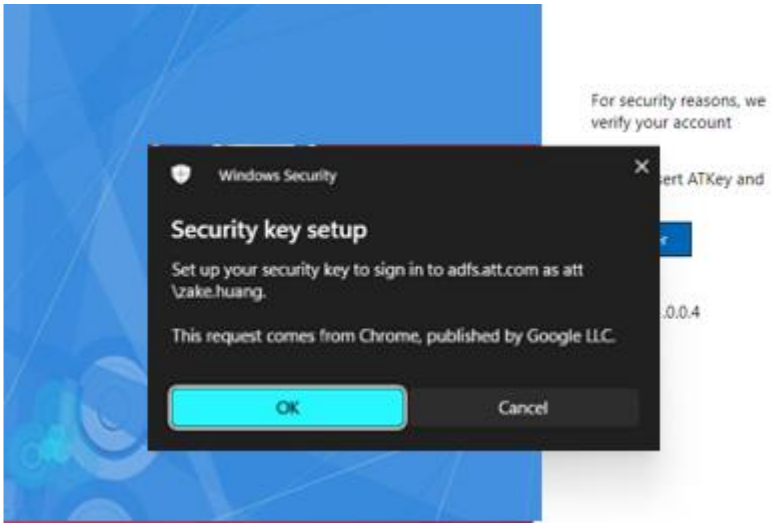
- Press Register to verify fingerprint on ATKey.Pro, then it's done.



For security reasons, we need additional information to verify your account

Please insert ATKey and press the register button to register

Version: 1.0.0.4



For security reasons, we
verify your account

ert ATKey and

.0.0.4

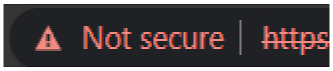
Windows Security

Security key setup

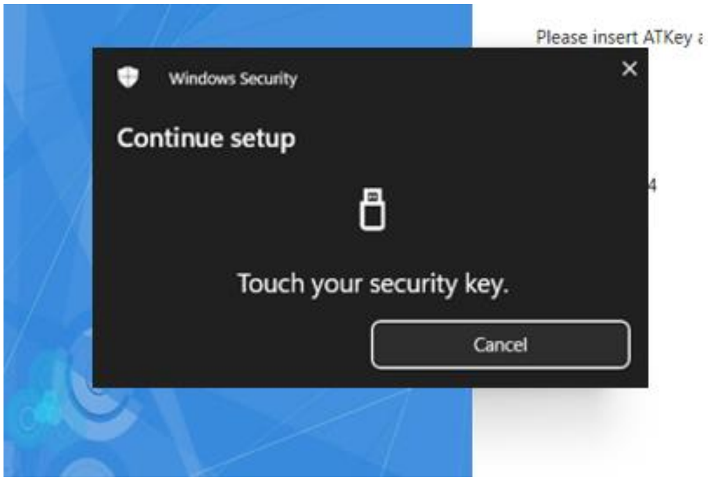
Set up your security key to sign in to adfs.att.com as att \zake.huang.

This request comes from Chrome, published by Google LLC.

*If this Browser dialog can't pop-up (webauthn), please make sure your URL has no "Not sure" hint as below:



Not secure | ~~https~~



Please insert ATKey a

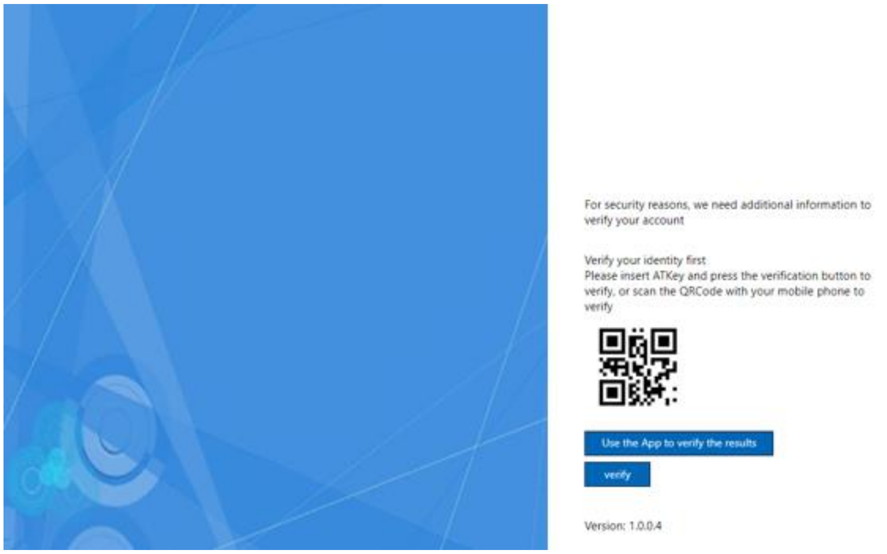
Windows Security

Continue setup

Touch your security key.

- ○ Then, Admin should find the record (User name and registered time stamp) from Dashboard – Registered Users

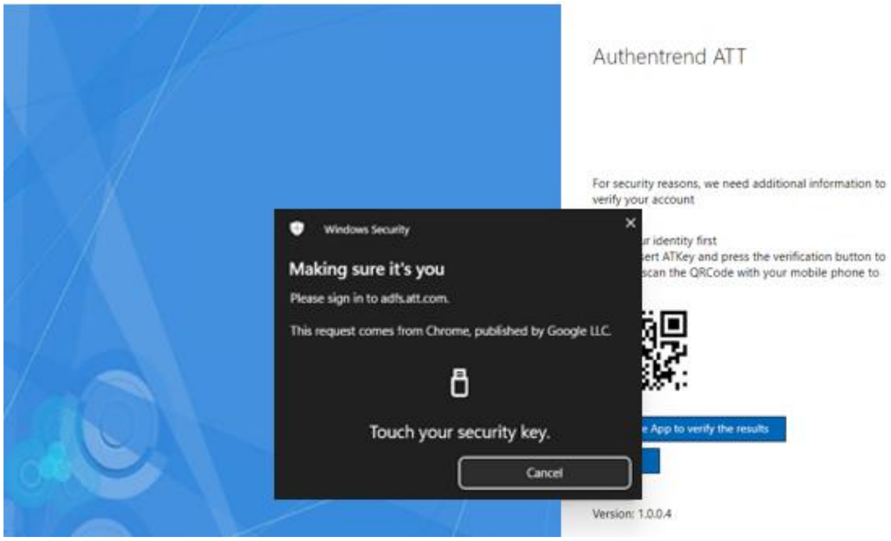
- ○ If the user account ever registered another ATKey.Pro, it needs to verify by registered one first for security reason – click "Verify" button



For security reasons, we need additional information to verify your account

Verify your identity first
Please insert ATKey and press the verification button to verify, or scan the QRCode with your mobile phone to verify

Version: 1.0.0.4



Authentrend ATT

For security reasons, we need additional information to verify your account

r identity first
ert ATKey and press the verification button to
scan the QRCode with your mobile phone to

Windows Security

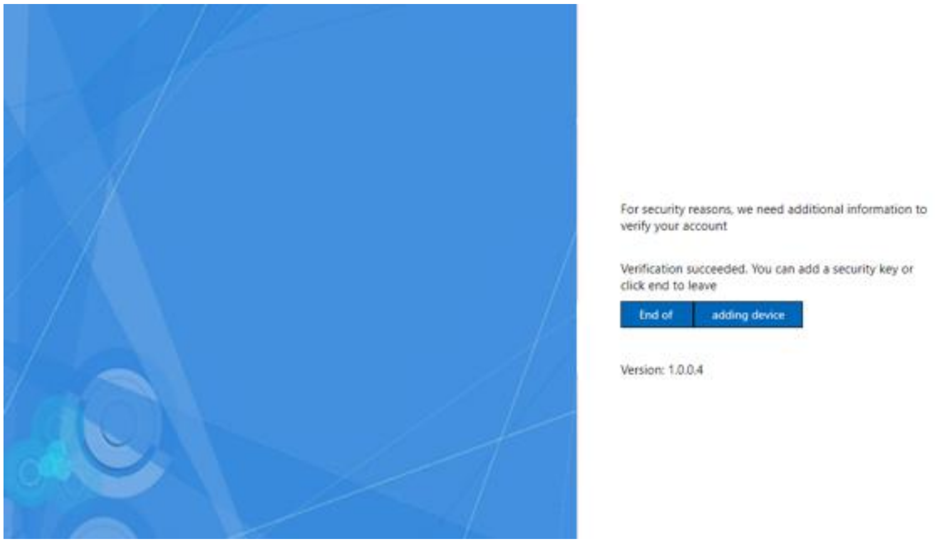
Making sure it's you

Please sign in to adfs.att.com.

This request comes from Chrome, published by Google LLC.

Touch your security key.

Version: 1.0.0.4



For security reasons, we need additional information to verify your account

Verification succeeded. You can add a security key or click end to leave

Version: 1.0.0.4

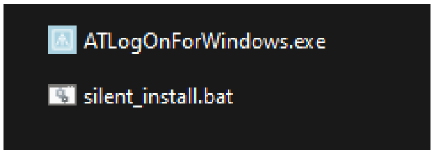
Click "Adding device", back to above "Add new key" – keycode, username, register

- But, If the original registered ATKey.Pro lost, Admin can remove that ATKey.Pro from Dashboard – Registered Users, then user can register new ATKey.Pro

d) Deploy (install) "AT.LogOn for Windows" to employees PC

- Please make sure VC distribution existing in the PC, or you can download and install it: https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170, https://learn.microsoft.com/ja-JP/cpp/windows/latest-supported-vc-redist?view=msvc-170

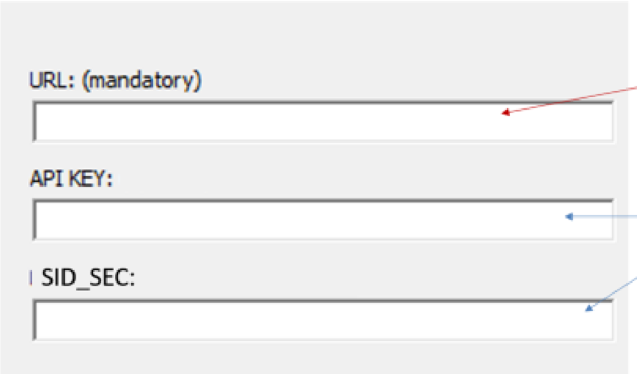
- There are 2 files for the installation



ATLogOnForWindows.exe

silent_install.bat

  - We will prepare customized batch file for silent installation, or Admin can modify batch file for these 3 items:



URL: (mandatory)

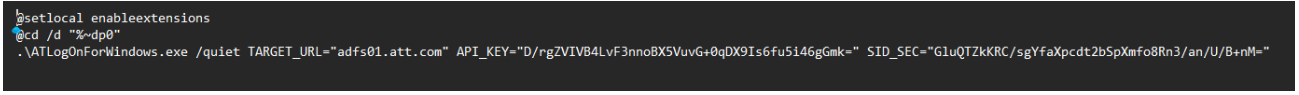
API KEY:

SID_SEC:

ADFS URL (pre-defined by customer admin with Local partner)

Defined and assigned by AuthenTrend to Local Partner, to Administrator (each AT.LogOn.Server has unique key)

    - TARGET_URL="adfs01.domainname.com"
    - API_KEY= "D/rgZVIVB4LvF3nnoBX5VuvG+0qDX9Is6fu5i46gGmk="
    - SID_SEC= "GluQTZkKRC/sgYfaXpcdt2bSpXmfo8Rn3/an/U/B+nM="



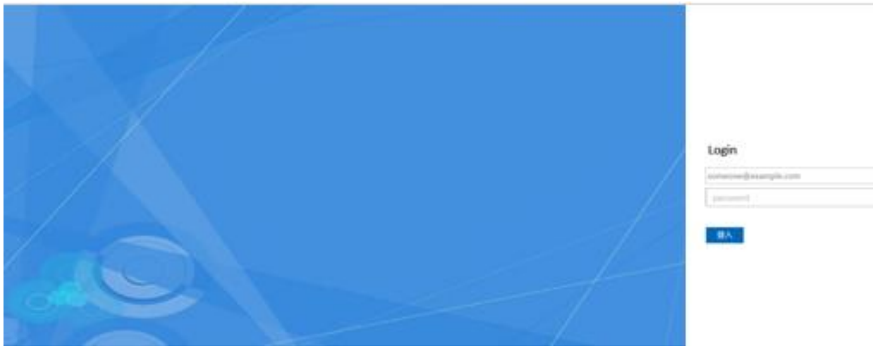
```
@setlocal enableextensions
@cd /d "%~dp0"
.\ATLogOnForWindows.exe /quiet TARGET_URL="adfs01.att.com" API_KEY="D/rgZVIVB4LvF3nnoBX5VuvG+0qDX9Is6fu5i46gGmk=" SID_SEC="GluQTZkKRC/sgYfaXpcdt2bSpXmfo8Rn3/an/U/B+nM="
```

- Install by “Silent_install.bat”
  - “silent_install.bat” is created by AuthenTrend and assign to customer, each customer/server may have different bat file.

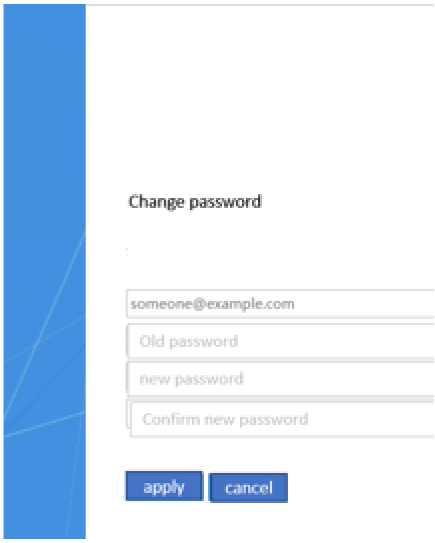
e) User cases for Admin

- (User case d.1) Existing employees, existing PCs
  - Assign ATKey.Pro to user
  - User enrolls fingerprints to ATKey.Pro (recommend at least 2 fingers)
  - Register ATKey.Pro user’s AD account
  - Install “AT.LogOn for Windows” to user’s PC
  - Logon Windows by registered ATKey.Pro (fingerprint matching)
    - 1st time: user needs to type in and confirm AD password – it must online and inside domain due to AD connection
    - From 2nd time: user just touch fingerprint to login
    - But if AD password changed (regular, or manually), after fingerprint matching, system will request to type in and confirm new password again to login (after it, all login by fingerprint)

- (User case d.2) New on-board employees (1st change password)
  - If IT assigned default AD account and password, and user needs to change at 1st login
    - 1st login may happen in ADFS page (register ATKey to AD account)
      - User needs to login and change password from ADFS page
        - Login by assigned ID and password

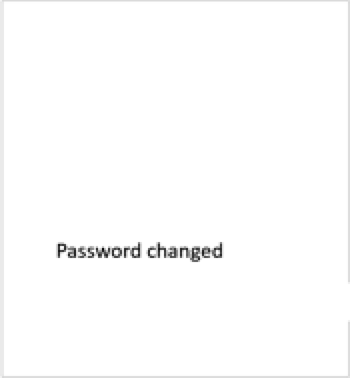


        - Type in ID: account@domain.com or domain\account, then type in assigned password and type in new password; Apply to confirm



Change password

- Done, and please go back to ADFS page manually



Password changed

- (User case d.3) User account is disabled or deleted from AD
    - The user can still do ATKey.Pro login (fingerprint matching) but it will pop up "password change dialog" instead of reject with message (but message is not totally right – deleted account shows ""The password seems to have been changed")
    - After type-in password, then it will show error message and reject login
    - So, if the users are disabled or deleted from AD, please remove them from AT.LogOn server dashboard also ask ATKey.Pro back (to reset for new user), so the user even can't try to login for both online and offline.

- (User case d.4) User AD password changed or expired
    - User verify fingerprint via ATKey.Pro to logon, then it will pop up dialog to ask typing new password.

- (User case d.5) One key vs. multiple accounts
    - If one specific ATKey.Pro registered to multiple accounts, that means the ATKey.Pro store multiple "fido credentials"; since it's Passswordless login, following FIDO spec., it will use "most recent" credential to login; for example:
        - ATKey.Pro#1 registered to user#A1, user#B2 and user#C3, and last login in user#C3; so login via ATKey.Pro#1, it will do Passwordless login to user#C3 account.
        - User can delete specific credentials (for example, delete #B2 and #C3, only reserve for #A1) from Chrome browser (non-Windows platform), or through AuthenTrend admin tool "SecurityKeyVault"

        - Or User can find Admin to remove ATKey.Pro#1 from user#B2 account (from AT.LogOn server dashboard)

- (User case d.6) Multiple keys vs. one account
    - User can login his/her account by any registered ATKey.Pro
    - But register new ATkey.Pro on ADFS page – it needs authentication by existing ATKey.Pro first, then register new key.

- (User case d.7) AD login failed counter
    - If AD policy allows "N" times password failure for user login, but for AT.LogOn, the actual count will be "N-1" at password changed or expired, due to AT.LogOn needs to login (by ATKey.Pro) first then we find wrong password, so user may not know this failure happened once since they did not type in password.
        - For example: account#A failure counter max. is 3, but through AT.LogOn, user password failed twice, it will lock since 1st failure happened at ATKey.Pro login.

- (User case d.8) Safe mode
    - If user boots their Windows PC and gets into "Safe mode", it will be back to original Windows logon screen to type in ID/Password to login Safe mode.

3. Employees Windows Logon

a) Enroll fingerprint

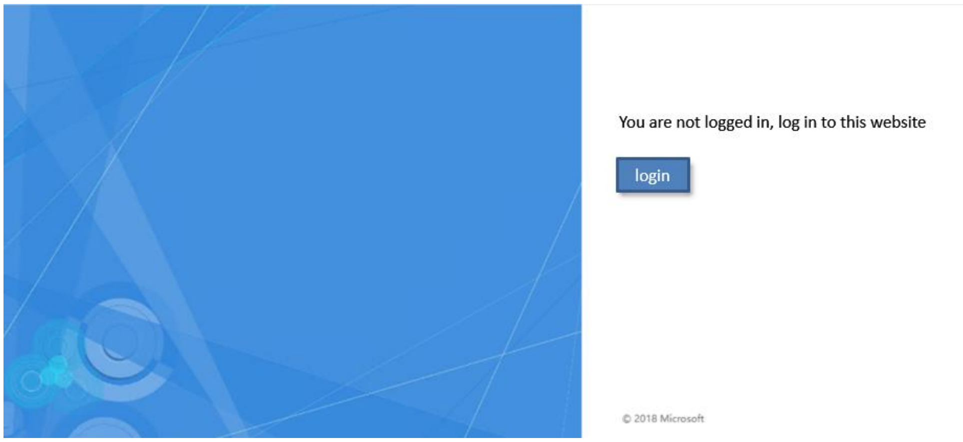
a. Fingerprint can enroll to ATKey.Pro via
   i. Windows Settings (Windows 10 build 1903 and later versions)
   ii. Chrome browser (Security and privacy) on non-Windows platform
   iii. Standalone enrollment: https://youtu.be/NnNqXbrf7vA

b. Check the video to understand how to enroll fingerprint well: https://youtu.be/bCLPMtZJhkM

c. We will always recommend to register at least 2 fingers per key.

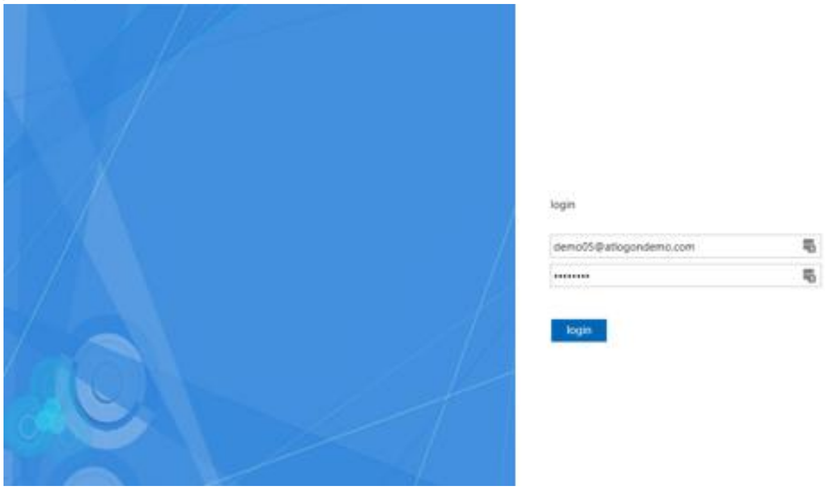
b) Register ATKe.Pro to AD account

a. Open chrome browser and type in assigned ADFS URL, for example: https://fs.domainname.com/adfs/ls/idpinitiatedsignon



You are not logged in, log in to this website

b. Sign in by user's AD ID/PWD

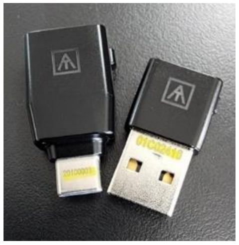


demo05@atlogondemo.com

••••••••

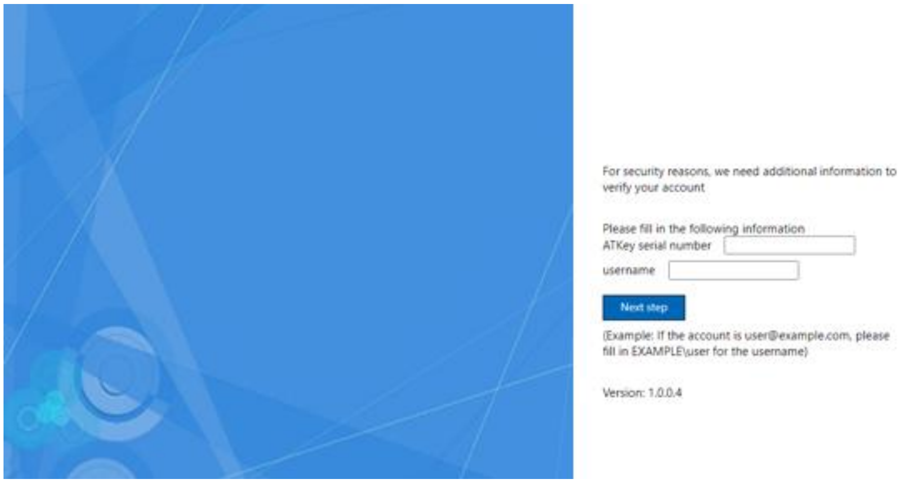
c. If it's 1st time to register FIDO authenticator - Enter ATKey.Pro Keycode and User name

   i. Keycode - where is the "keycode of "ATKey.Pro"? check below image, keycode is unique code (8 digits) inside the key and laser inked on surface of the key.



ii. Please be noted – “username” must be totally correct input since it’s not changeable.

1. Format: domainname\username



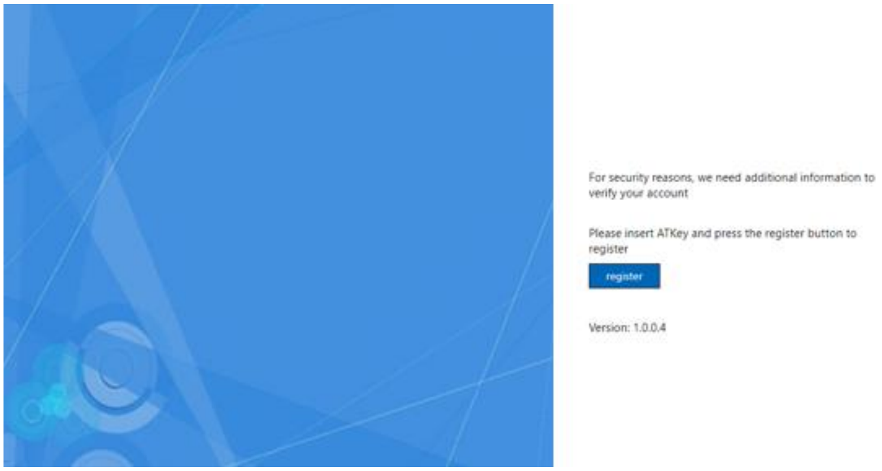
For security reasons, we need additional information to verify your account

Please fill in the following information
ATKey serial number
username

(Example: If the account is user@example.com, please fill in EXAMPLE\user for the username)

Version: 1.0.0.4

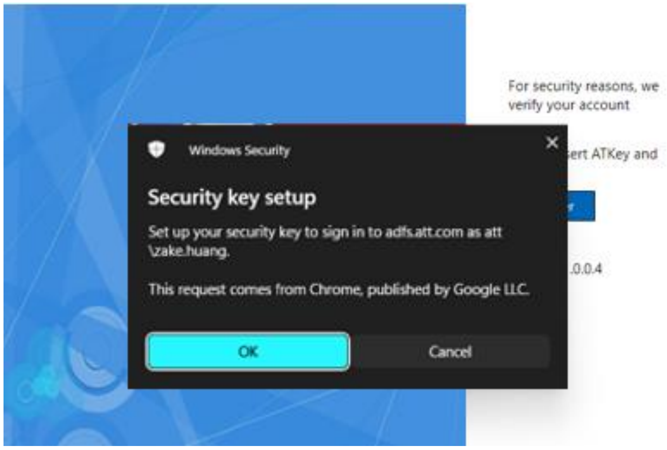
d. Press Register to verify fingerprint on ATKey.Pro, then it’s done.



For security reasons, we need additional information to verify your account

Please insert ATKey and press the register button to register

Version: 1.0.0.4



For security reasons, we
verify your account

ert ATKey and

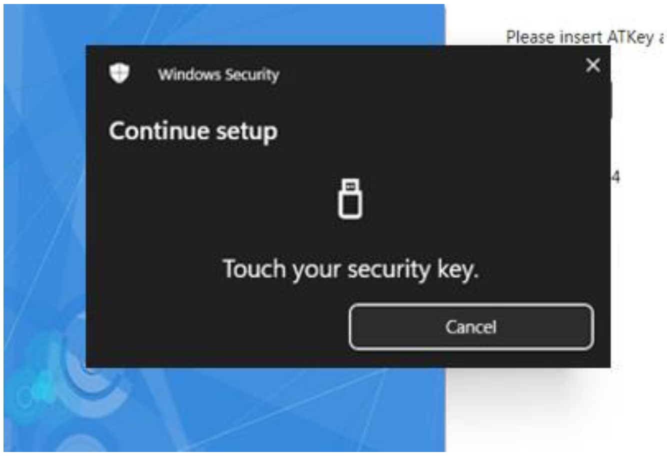
.0.0.4

Windows Security

Security key setup

Set up your security key to sign in to adfs.att.com as att\zake.huang.

This request comes from Chrome, published by Google LLC.



Please insert ATKey a

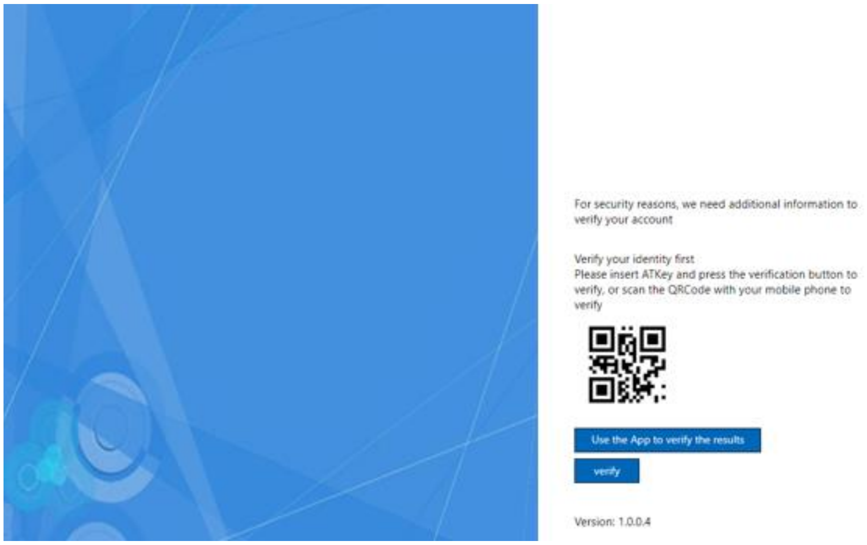
Windows Security

Continue setup

Touch your security key.

e. Then, Admin should find the record (User name and registered time stamp) from Dashboard - Users

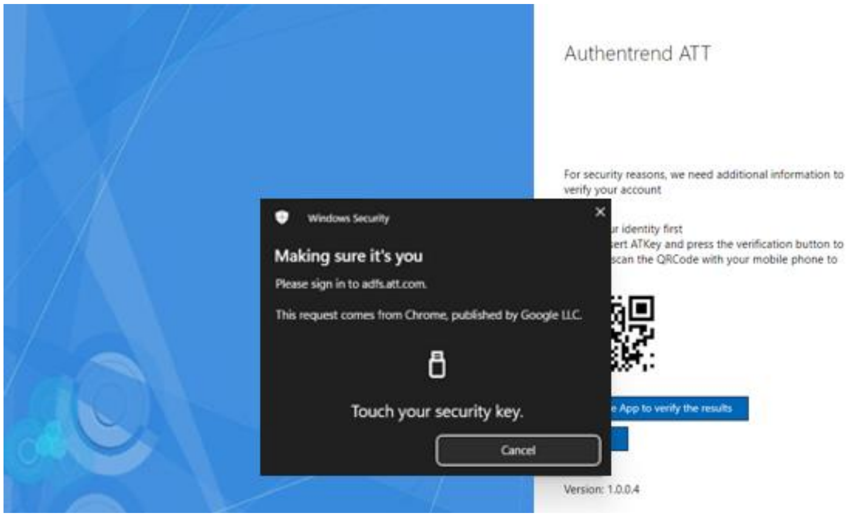
f. If the user account ever registered another ATKey.Pro, it needs to verify by registered one first for security reason – click “Verify” button



For security reasons, we need additional information to verify your account

Verify your identity first
Please insert ATKey and press the verification button to verify, or scan the QRCode with your mobile phone to verify

Version: 1.0.0.4



Authentrend ATT

For security reasons, we need additional information to verify your account

r identity first
ert ATKey and press the verification button to
scan the QRCode with your mobile phone to

Windows Security

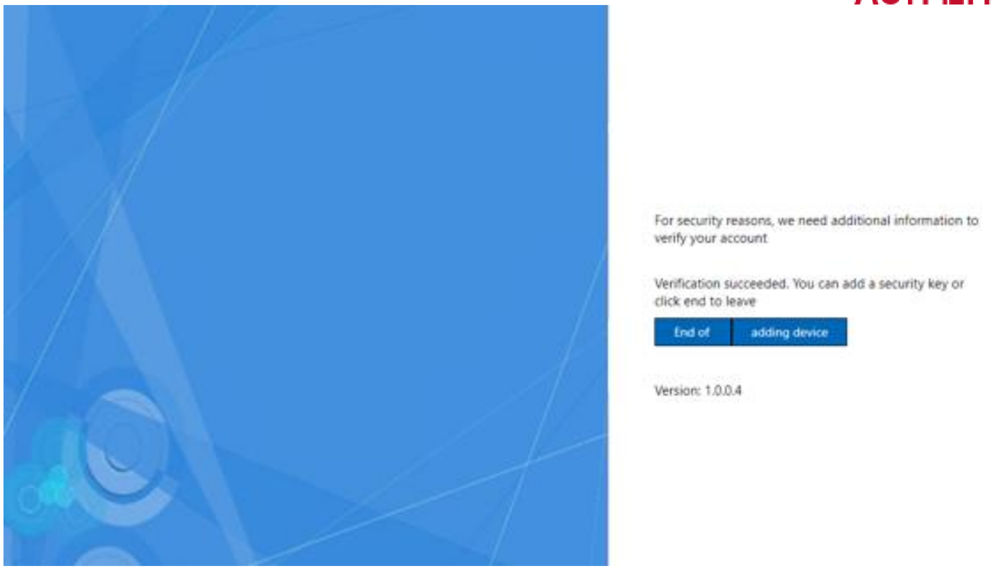
Making sure it's you

Please sign in to adfs.att.com.

This request comes from Chrome, published by Google LLC.

Touch your security key.

Version: 1.0.0.4



For security reasons, we need additional information to verify your account

Verification succeeded. You can add a security key or click end to leave

Version: 1.0.0.4

Click “Adding device”, back to above “Add new key” – keycode, username, register

g. But, If the original registered ATKey.Pro lost, Admin can remove that ATKey.Pro from Dashboard – Registered Users, then user can register new ATKey.Pro

c) 1st login vs. from 2nd login

a. Logon Windows by registered ATKey.Pro (fingerprint matching)
   i. 1st time: user needs to type in and confirm AD password – it must be online and inside domain, since it needs AD
   ii. From 2nd time: user just touch fingerprint to login
   iii. But if AD password changed (regular, or manually), after fingerprint matching, system will request to type in and confirm new password again to login (after it, all login by fingerprint)

d) Domain vs. outside domain

a. Inside domain (inside company or through VPN)
   i. Login via ATKey.Pro for both online and offline

b. Outside domain
   i. Login via ATKey.Pro for both online and offline

c. Please be noted – register ATKey.Pro to AD account, at 1st time login, it must be online and inside the domain since it needs AD authority

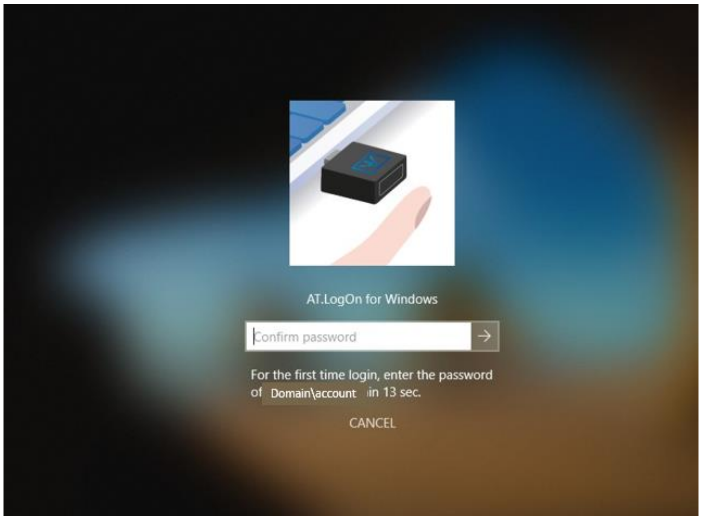
e) Online/offline

a. No matter PC is online or offline, ATKey.Pro can login to PC; this is also the benefit from FIDO hardware authenticator.

f) User cases from ATKey (for employees)

- (User case f.1) AD Password changed
  - at Windows logon screen, ATKey.Pro verified, it will ask type-in “password” to confirm to login

- (User case f.2) AD Password expired
  - at Windows logon screen, ATKey.Pro verified, then it will ask:
    - confirm password – original password

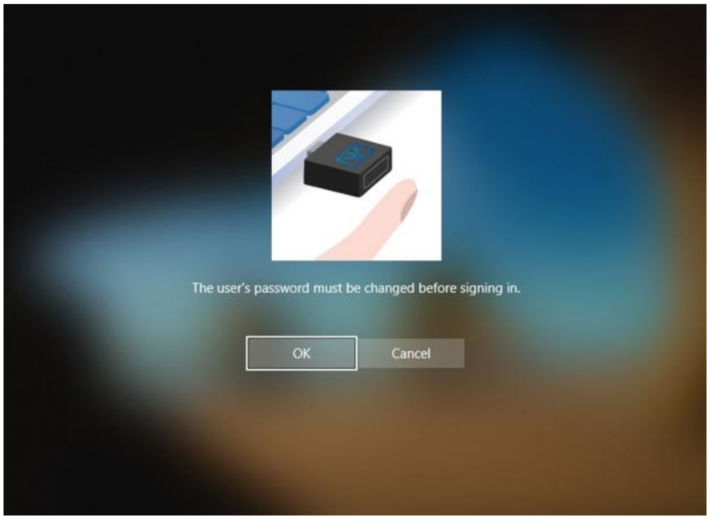


AT.LogOn for Windows

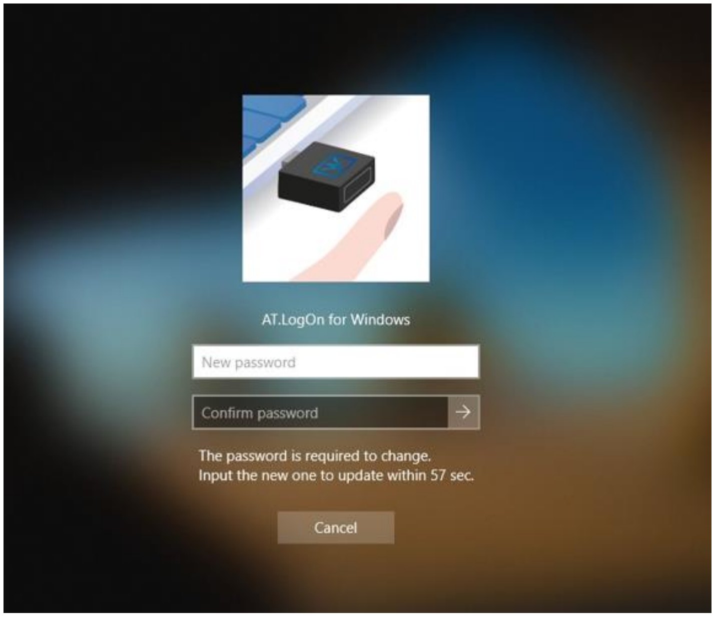
Confirm password

For the first time login, enter the password of Domain\account in 13 sec.

  - then, ask for new password, confirm it to login



The user's password must be changed before signing in.



AT.LogOn for Windows

New password

Confirm password

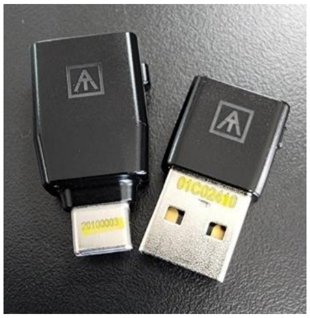
The password is required to change.
Input the new one to update within 57 sec.

- (User case f.3) Forget bringing key

  - User can login following admin's instructions:
    - Press defined hotkeys (4 keys together, and it's defined inside AT.LogOn Server dashboard by admin)
    - Type in "Recovery code" – it's defined inside AT.LogOn Server dashboard by admin
    - User can login via his/her ID and Password, but type in format must be:
      - Domainname\accountID+password
  - Admin can change "Hot-key" and "Recovery Code" on AT.LogOn Server Dashboard any time, and it keeps all records in case some users may need previous hot-key and code (never online to sync).

- (User case f.4) Lost key
  - Register a new ATKey.Pro
    - Admin can remove User's ATKey from AT.LogOn Server Dashboard
    - Then user can register new ATKey.Pro through ADFS page
  - If user is out of company and he/her can't get a new ATKey.Pro
    - Press defined hotkeys (4 keys together, and it's defined inside AT.LogOn Server dashboard by admin)
    - Type in "Recovery code" – it's defined inside AT.LogOn Server dashboard by admin
    - User can login via his/her ID and Password, but type in format must be:
      - Domainname\accountID+password
  - Admin can change "Hot-key" and "Recovery Code" on AT.LogOn Server Dashboard any time, and it keeps all records in case some users may need previous hot-key and code (never online to sync).

- (User case f.5) Not sure which key is …
  - Since all ATKey.Pro are in same outlook, user can judge if it's his/her key via keycode



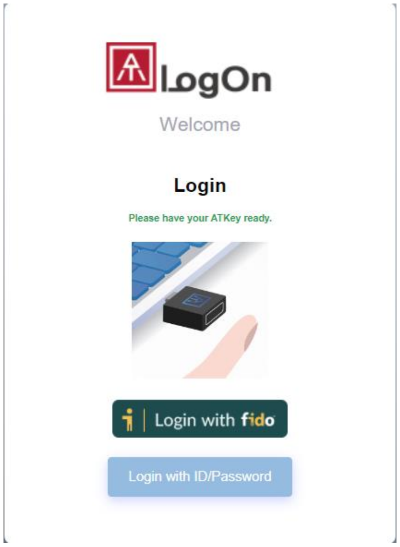
  - or Admin can search keycode from AT.LogOn Server dashboard to see who registered this key.

- (User case f.6) Shared PC or workstations
  - User can login to his/her account via registered ATKey.Pro on any Shared PC; but it will request typing and confirming Password again at 1st login.

4. AT.LogOn Server management

a) Assign admin

- Admin login via registered ATKey.Pro or assigned ID/Password (ex. https://adfs01.domainname.com/dashboard/)

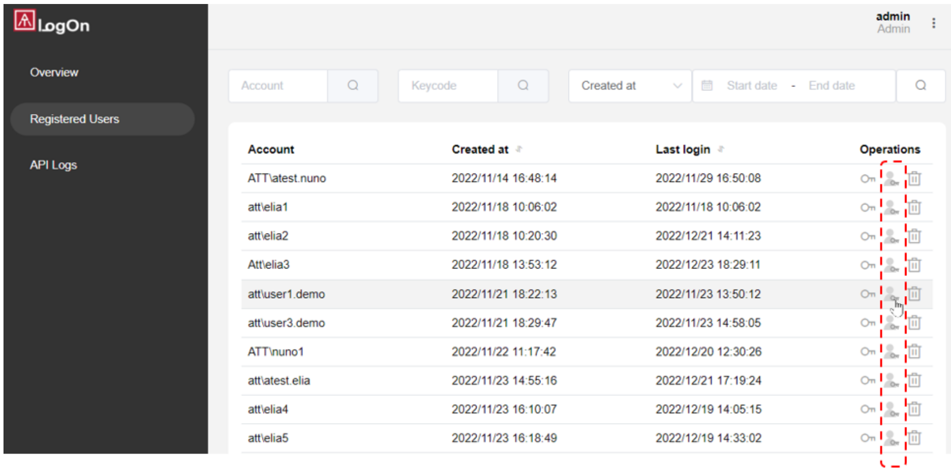


Welcome

Login

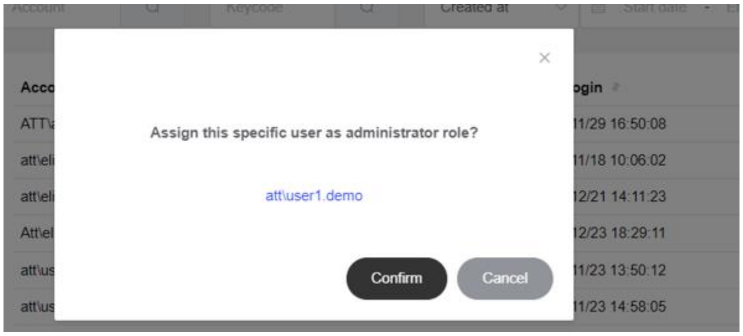
Please have your ATKey ready.

- From "Registered Users"
  - Admin can select "Registered Users" to assign the administrator authority
    - Find the specific user, click "admin icon" as below



Account	Created at	Last login	Operations
ATT\atest.nuno	2022/11/14 16:48:14	2022/11/29 16:50:08	
att\elia1	2022/11/18 10:06:02	2022/11/18 10:06:02	
att\elia2	2022/11/18 10:20:30	2022/12/21 14:11:23	
Att\elia3	2022/11/18 13:53:12	2022/12/23 18:29:11	
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	
att\user3.demo	2022/11/21 18:29:47	2022/11/23 14:58:05	
ATT\nuno1	2022/11/22 11:17:42	2022/12/20 12:30:26	
att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	
att\elia4	2022/11/23 16:10:07	2022/12/19 14:05:15	
att\elia5	2022/11/23 16:18:49	2022/12/19 14:33:02	

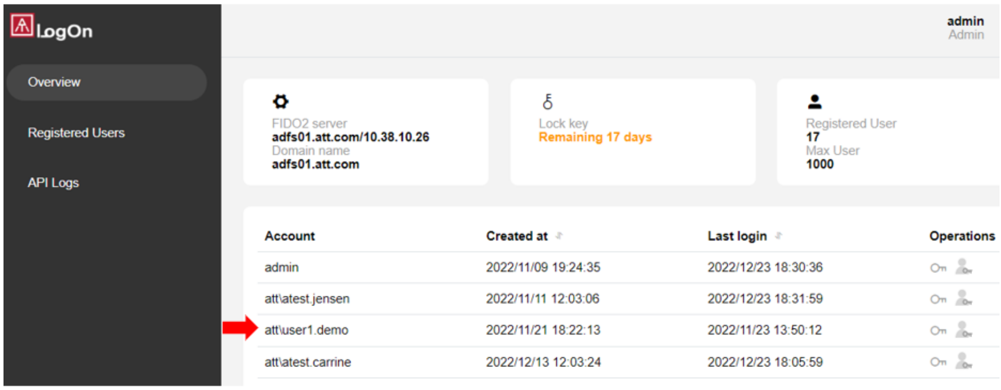
    - Confirm the user
    - Then it will show on "Overview" as one of the admin, then the specific user can login



Assign this specific user as administrator role?

att\user1.demo

    - AT.LogOn.Server dashboard via his/her ATKey.Pro as admin



FIDO2 server
adfs01.att.com/10.38.10.26
Domain name
adfs01.att.com

Lock key
Remaining 17 days

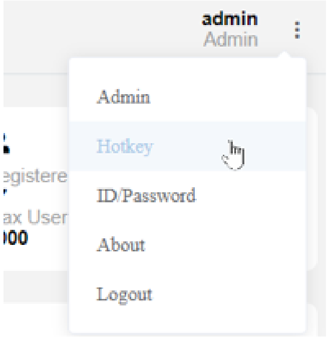
Registered User
17
Max User
1000

Account	Created at	Last login	Operations
admin	2022/11/09 19:24:35	2022/12/23 18:30:36	
att\atest.jensen	2022/11/11 12:03:06	2022/12/23 18:31:59	
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	
att\atest.carrine	2022/12/13 12:03:24	2022/12/23 18:05:59	

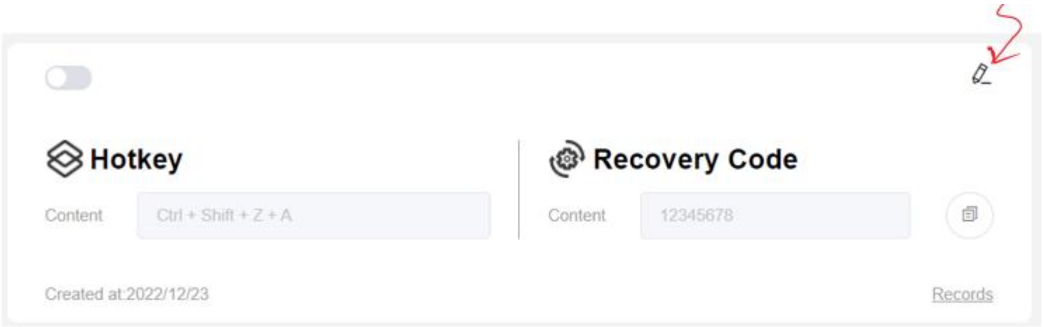
- Login-ed administrator can add/remove other administrators.

b) Hotkey and Recovery code

- Setup "Hotkey" and "Recovery Code"
  - This is for users to login via their AD ID/Password from some urgent user cases (key is not with user, lost key, key damaged, outside of office, …..)
    - Enter from admin list box



- Click "edit" (Pen icon) to setup Hotkey and Recovery Code

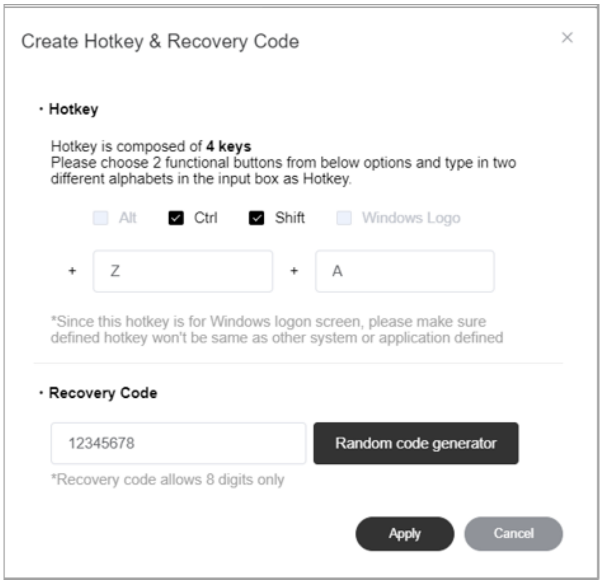


Content: Ctrl + Shift + Z + A

Content: 12345678

Created at:2022/12/23

- Following Hotkey rule here to setup, and type in Recovery Code or random generate it



Create Hotkey & Recovery Code

- **Hotkey**

Hotkey is composed of **4 keys**
Please choose 2 functional buttons from below options and type in two different alphabets in the input box as Hotkey.

□ Alt ☑ Ctrl ☑ Shift □ Windows Logo

+ Z + A

*Since this hotkey is for Windows logon screen, please make sure defined hotkey won't be same as other system or application defined

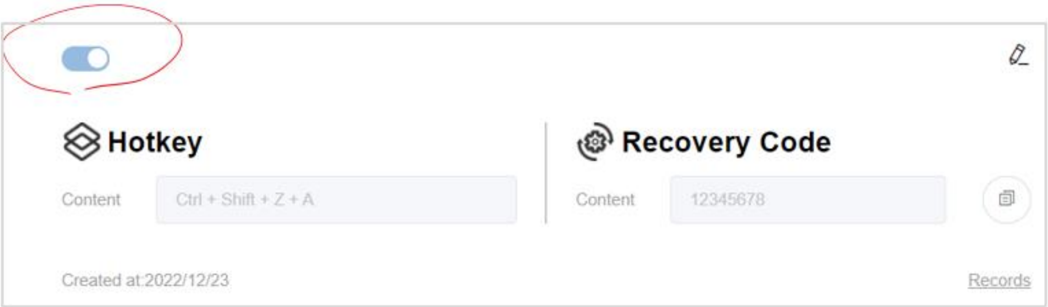
- **Recovery Code**

12345678

*Recovery code allows 8 digits only

**Note: we won't support "Windows key" for the combination from AT.FIDO.Server 2.00.08 to avoid any conflicts with other applications*

- "Apply", remember to turn this function ON



Hotkey

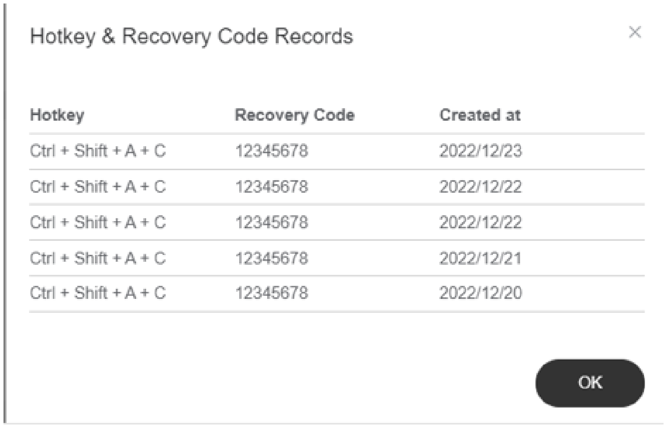
Content: Ctrl + Shift + Z + A

Recovery Code

Content: 12345678

Created at:2022/12/23

  - At Windows login screen, if it's online and also joined domain, client ill sync "hotkey" and "Recovery Code" and encrypted locally
  - For better security and management, we will recommend you to change Hotkey and Recovery code frequently, or change it when any user knows to login by it
  - So if a PC needs historic Hotkey and Recovery code (always offline or outside the domain), you can check "Records" to see what's the Hotkey and Recover code to login

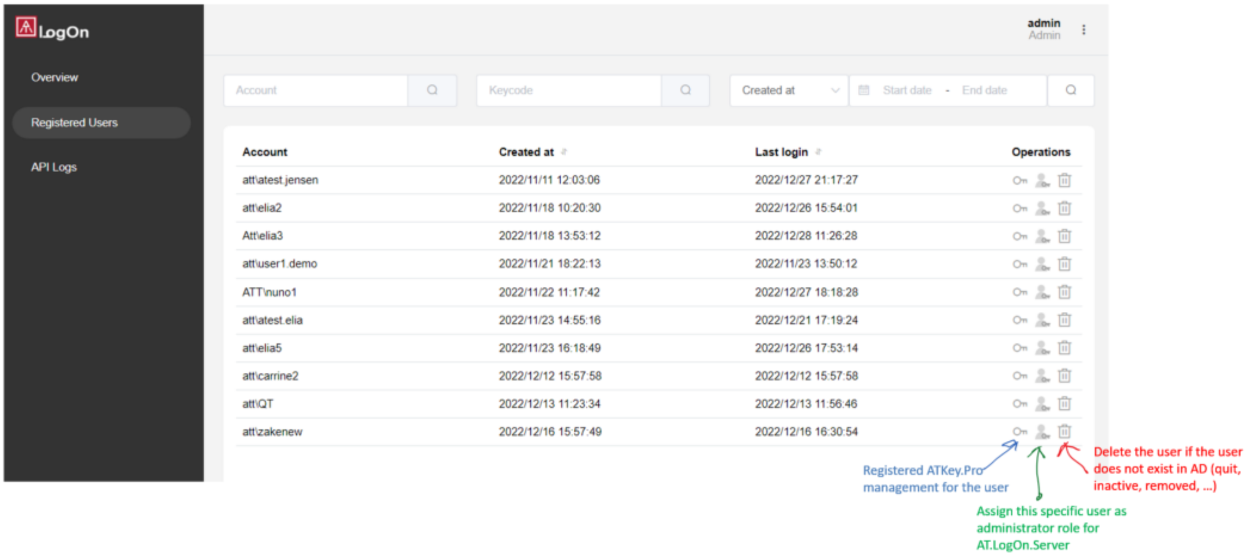


Hotkey & Recovery Code Records

Hotkey	Recovery Code	Created at
Ctrl + Shift + A + C	12345678	2022/12/23
Ctrl + Shift + A + C	12345678	2022/12/22
Ctrl + Shift + A + C	12345678	2022/12/22
Ctrl + Shift + A + C	12345678	2022/12/21
Ctrl + Shift + A + C	12345678	2022/12/20

c) Registered Users management

- Login Dashboard to "Registered Users" , it will show the user lists (sorting by last login time), you can see every user
    - ♦ "Created time": from ADFS web page (https://fs.domainname.com/adfs/ls/idpinitiatedsignon) to registered ATKey.Pro; a click-able sorting button beside to sorting by most recently "Created users" or most old "Create Users".
    - ♦ "Last login time": last login to his/her account (PC login); a click-able sorting button beside to sorting by most recently "Login users" or most old "Login Users".



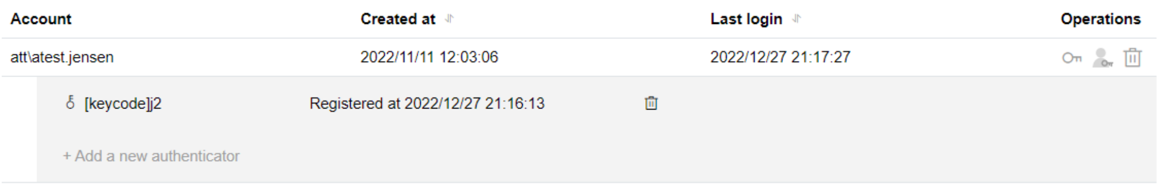
Account	Created at	Last login	Operations
att\atest.jensen	2022/11/11 12:03:06	2022/12/27 21:17:27	🔑 👤 🗑
att\elia2	2022/11/18 10:20:30	2022/12/26 15:54:01	🔑 👤 🗑
Att\elia3	2022/11/18 13:53:12	2022/12/28 11:26:28	🔑 👤 🗑
att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	🔑 👤 🗑
ATT\nuno1	2022/11/22 11:17:42	2022/12/27 18:18:28	🔑 👤 🗑
att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	🔑 👤 🗑
att\elia5	2022/11/23 16:18:49	2022/12/26 17:53:14	🔑 👤 🗑
att\carrine2	2022/12/12 15:57:58	2022/12/12 15:57:58	🔑 👤 🗑
att\QT	2022/12/13 11:23:34	2022/12/13 11:56:46	🔑 👤 🗑
att\zakenew	2022/12/16 15:57:49	2022/12/16 16:30:54	🔑 👤 🗑

Registered ATKey.Pro management for the user

Assign this specific user as administrator role for AT.LogOn.Server

Delete the user if the user does not exist in AD (quit, inactive, removed, …)

- ♦ Check or delete registered ATKey.Pro from the specific user
    - ➢ Click "key" icon to show up drop down list

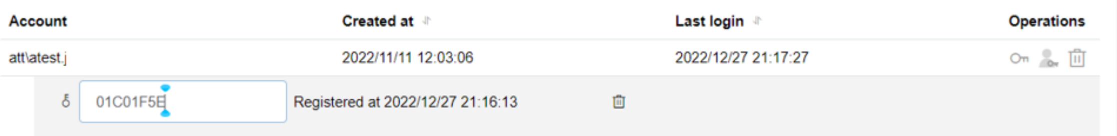


Account	Created at	Last login	Operations
att\atest.jensen	2022/11/11 12:03:06	2022/12/27 21:17:27	🔑 👤 🗑

[keycode]j2 Registered at 2022/12/27 21:16:13 🗑

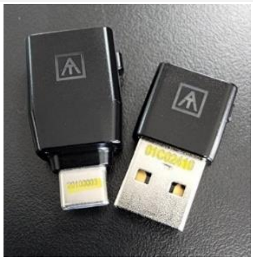
+ Add a new authenticator

- ▪ Double click [keycode] area to come out text box to edit correct key code (in case, user typo the keycode when registered his/her ATKey.Pro on ADFS web page)

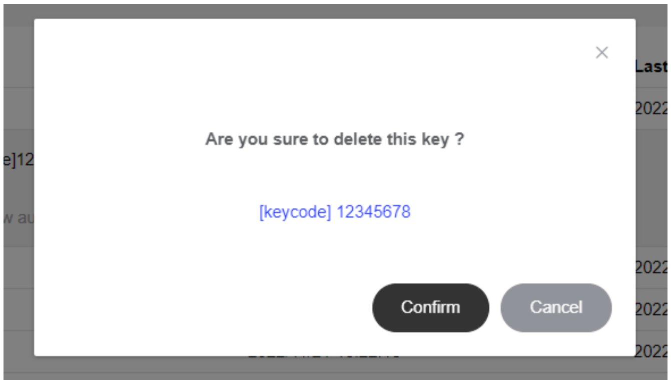


Account	Created at	Last login	Operations
att\atest.j	2022/11/11 12:03:06	2022/12/27 21:17:27	🔑 👤 🗑

01C01F5E Registered at 2022/12/27 21:16:13 🗑


<= here is the keycode inked on each key

- ▪ If user registered multiple keys, it will all listing here with registered time
- ▪ Admin can delete the registered ATKey.Pro as key revoke from AT.LogOn.Server
    - User lost the key
    - User switch to another key and original key get reset or damaged
- ▪ Click "+ Add a new authenticator", it will jump to ADFS web page for user to login and registered new key

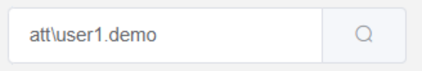


Are you sure to delete this key ?

[keycode] 12345678

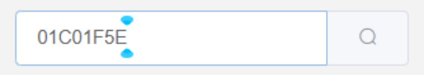
- Double click [keycode] area to come out text box to edit correct key code (in case, user typo the keycode when registered his/her ATKey.Pro on ADFS web page)

- Assign the specific user as Administrator role for AT.LogOn.Server
- Delete the specific user from AT.LogOn.Server FIDO database
- Search by
  - User name: the format is same as what you type-in when you are doing ATKey.Pro registration on ADFS web page, it should be “domainname\accoutname”



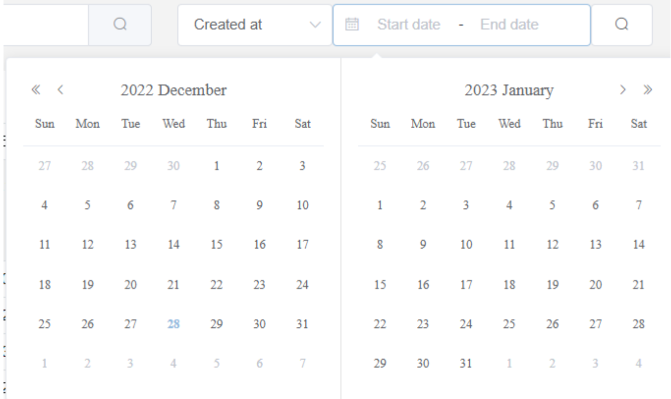
att\user1.demo

  - Keycode: in case, if there are ATKey.Pro somewhere, it’s difficult to judge who owns this key, admin can search keycode to figure the owner.



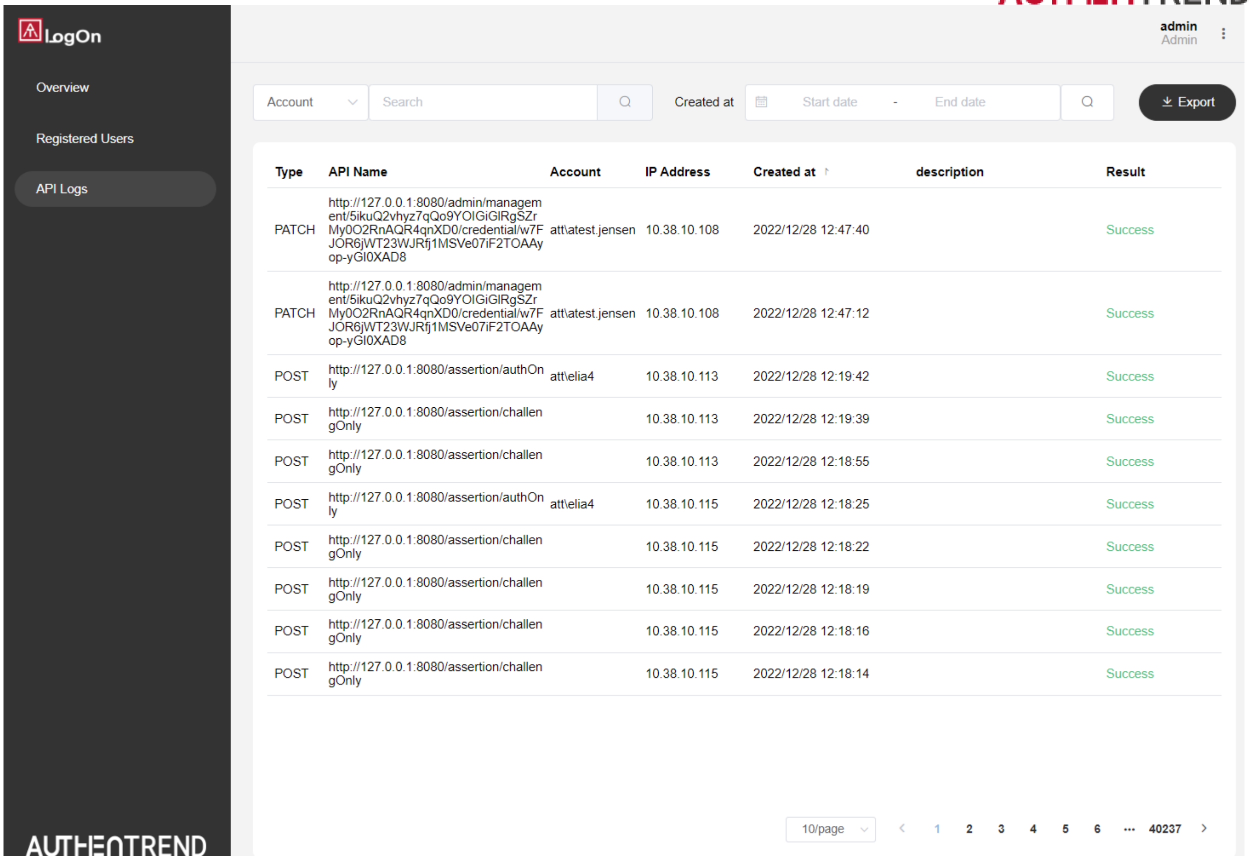
01C01F5E

  - Created date-time: Admin can search certain period of time to know the user login records



d) API Logs

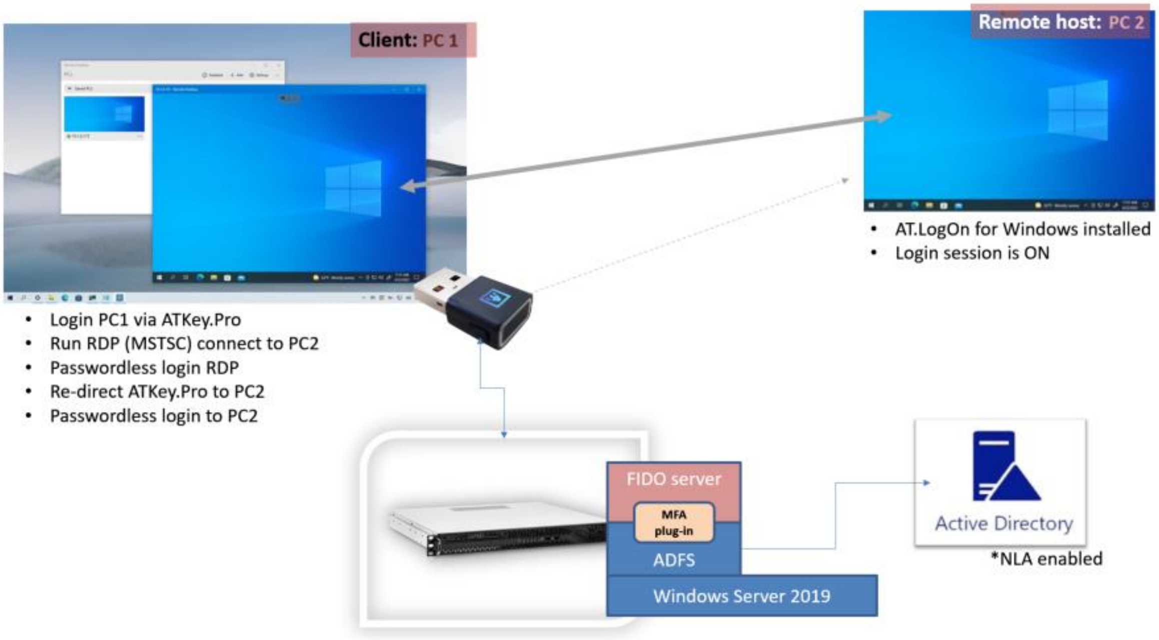
- We recorded every API logs (every action to AT.LogOn.Server) for



Type	API Name	Account	IP Address	Created at ↑	description	Result
PATCH	http://127.0.0.1:8080/admin/management/5ikuQ2vhyz7qQo9YOIGiGlRgSZrMy0O2RnAQR4qnXD0/credential/w7FJOR6jWT23WJRfj1MSVe07iF2TOAAyop-yGl0XAD8	att\atest.jensen	10.38.10.108	2022/12/28 12:47:40		Success
PATCH	http://127.0.0.1:8080/admin/management/5ikuQ2vhyz7qQo9YOIGiGlRgSZrMy0O2RnAQR4qnXD0/credential/w7FJOR6jWT23WJRfj1MSVe07iF2TOAAyop-yGl0XAD8	att\atest.jensen	10.38.10.108	2022/12/28 12:47:12		Success
POST	http://127.0.0.1:8080/assertion/authOnly	att\elia4	10.38.10.113	2022/12/28 12:19:42		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.113	2022/12/28 12:19:39		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.113	2022/12/28 12:18:55		Success
POST	http://127.0.0.1:8080/assertion/authOnly	att\elia4	10.38.10.115	2022/12/28 12:18:25		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.115	2022/12/28 12:18:22		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.115	2022/12/28 12:18:19		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.115	2022/12/28 12:18:16		Success
POST	http://127.0.0.1:8080/assertion/challengOnly		10.38.10.115	2022/12/28 12:18:14		Success

- Debug
  - If it’s necessary, export logs (limited period) to file to send back for debug
- User actions
  - Check the specific users all actions
- API logs only reserved for 12 months to avoid huge and heavy logs

5. RDP – Remote Desktop



- AT.LogOn for Windows installed
- Login session is ON

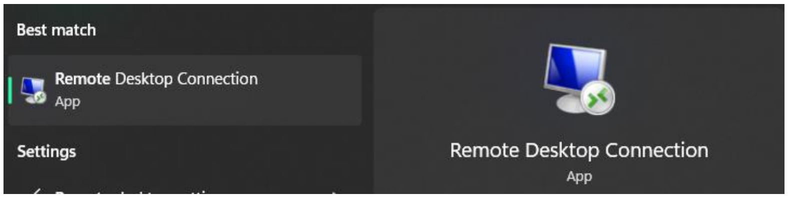
- Login PC1 via ATKey.Pro
- Run RDP (MSTSC) connect to PC2
- Passwordless login RDP
- Re-direct ATKey.Pro to PC2
- Passwordless login to PC2

*NLA enabled

Demo video: https://www.youtube.com/watch?v=Jrj7ec-BD1M

a) Criteria of Host PC, Remote PC and AD settings

- Support Remote Desktop Connection (mstsc)


Best match

Remote Desktop Connection
App

Settings

Remote Desktop Connection
App

- Here are criteria of each role

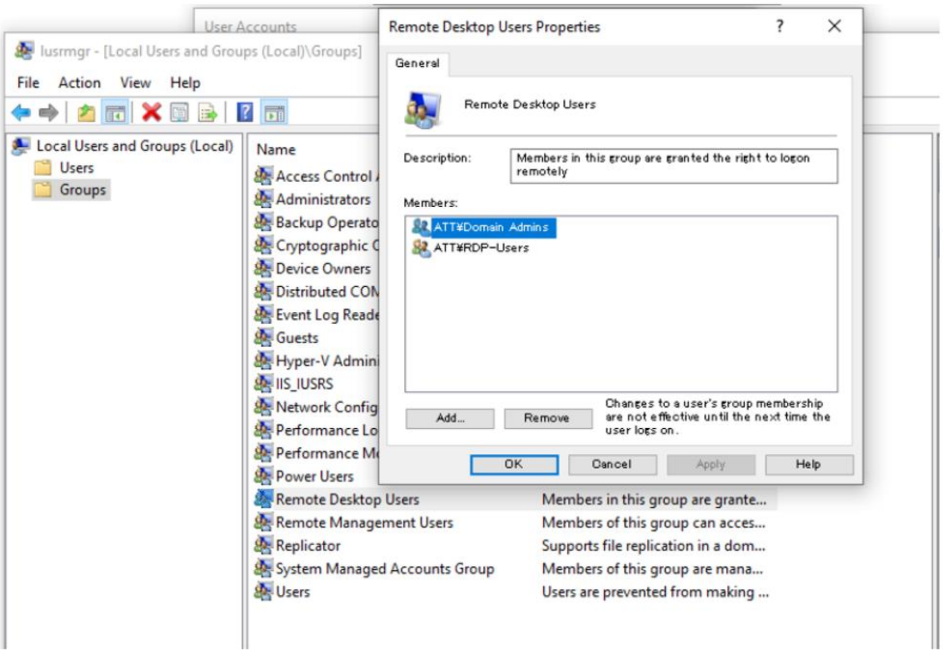
Joined AD domain account	AT.LogOn for Windows installed	Account with admin authority	Run as admin (Remote Desktop Client – mstsc)	Other items
Ok for joined-AD or non-joined-AD account.	Installed for joined-AD client. Not installed for non-joinedAD client.	Must.	Ok for both – run as admin (recommend) or run it directly.	The ATKey.Pro needs to register to the remote host account.

Joined AD domain account	AT.LogOn for Windows installed	RDP permitted account by AD	Other items
Must. (AT.LogOn won't install to non-joined AD PC)	Installed. 1st login needs typing Password	Must. AD admin account is also ok.	The ATKey.pRO needs to register to this remote host account, and re-directly ATKey.Pro to the remote host. But Remote PC needs "login session" ready; so if the remote PC is after cool-boot or warm-boot, it can just login via "Hotkey + Recovery Code", then ID/PWD; but after it, re-direct ATKey.Pro can work since login session is ready

NLA enabled AD

Must.

- In addition, the account must be assigned logon remote right by AD



Remote Desktop Users Properties

Remote Desktop Users

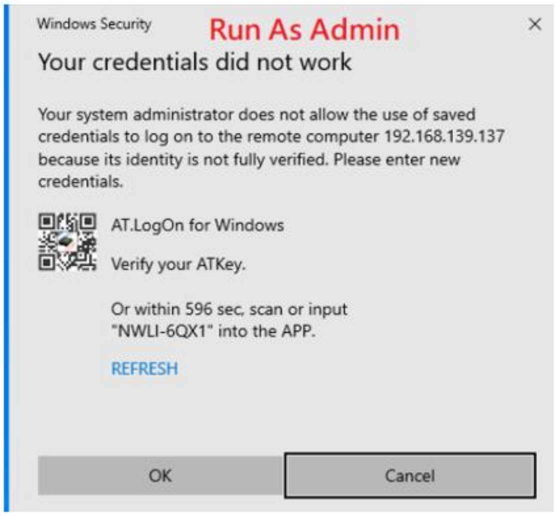
Description: Members in this group are granted the right to logon remotely

Members:
ATT¥Domain Admins
ATT¥RDP-Users

Changes to a user's group membership are not effective until the next time the user logs on.

Name	
Access Control /	
Administrators	
Backup Operato	
Cryptographic (	
Device Owners	
Distributed COM	
Event Log Reade	
Guests	
Hyper-V Admini	
IIS_IUSRS	
Network Config	
Performance Lo	
Performance Mo	
Power Users	
Remote Desktop Users	Members in this group are grante...
Remote Management Users	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Accounts Group	Members of this group are mana...
Users	Users are prevented from making ...

- Remote Desktop Connection (mstsc) “Run as admin (by ATKey.Pro)” vs. “Not run as admin (by Password)”



Your credentials did not work

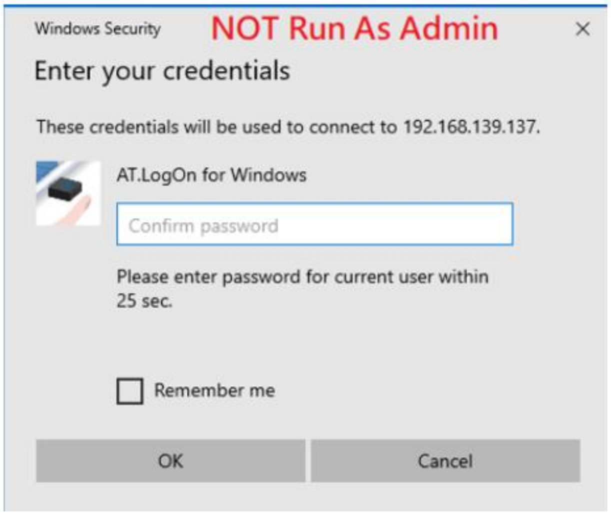
Your system administrator does not allow the use of saved credentials to log on to the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.

AT.LogOn for Windows

Verify your ATKey.

Or within 596 sec, scan or input "NWLI-6QX1" into the APP.

REFRESH



Enter your credentials

These credentials will be used to connect to 192.168.139.137.

AT.LogOn for Windows

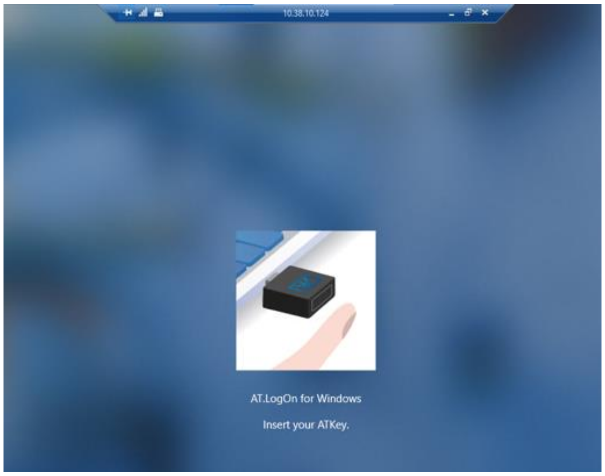
Confirm password

Please enter password for current user within 25 sec.

□ Remember me

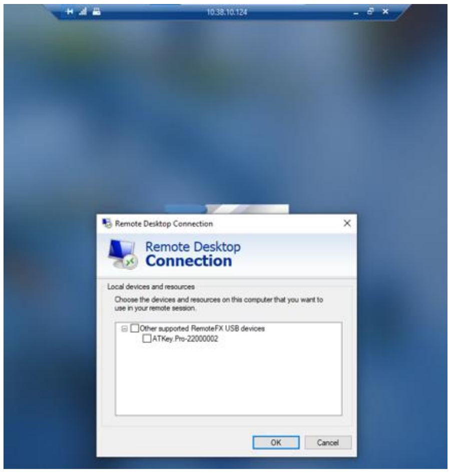
Touch fingerprint on ATKey.Pro, then go for remote host screen

- Remote Desktop Connection (mstsc) re-direct ATKey.Pro
At full screen, you can see the caption bar there:



AT.LogOn for Windows

Insert your ATKey.

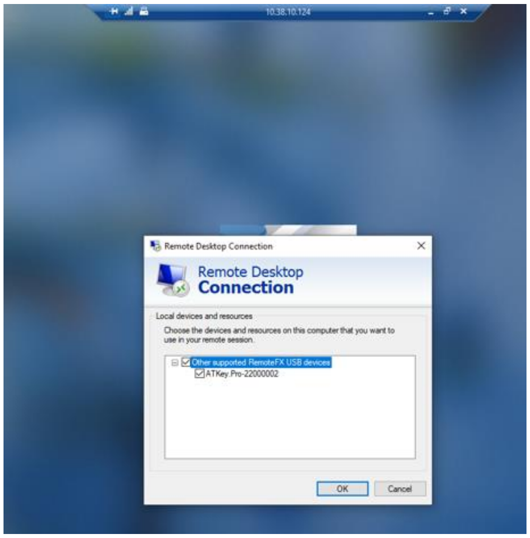


Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

- □ Other supported RemoteFX USB devices
  - □ ATKey.Pro-22000002

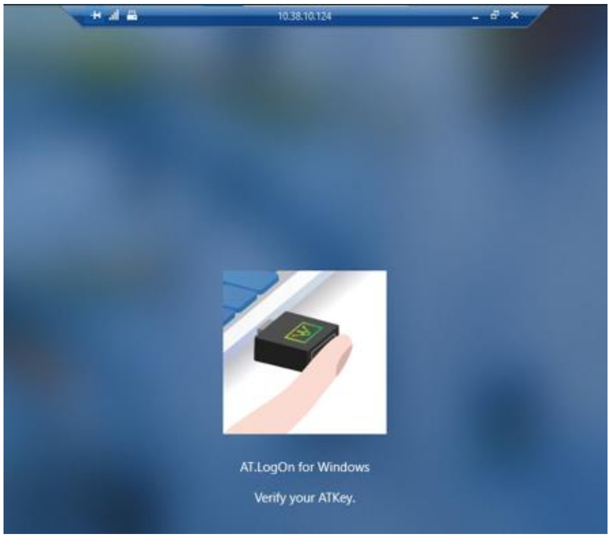


Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

- ☑ Other supported RemoteFX USB devices
  - ☑ ATKey.Pro-22000002



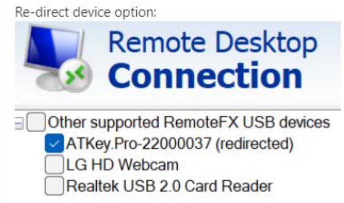
AT.LogOn for Windows

Verify your ATKey.

b) User cases for RDP

- (User case b.1) re-direct ATKey.Pro key must be registered to the same user account with remote host
  - Account#A is client, Account#B is remote host
  - ATKey#2 registered to Account#B
  - ATKey#2 stays with client and re-direct to remote host Account#B, ok to login
  - ATKey#1 registered to Account#A and re-direct to remote host Account#B, it won’t work, and it may just freeze and waiting long time to response, or not response.

- (User case b.2) ATKey.Pro re-direct to Remote PC (#258) for remote login and remote web services
  - There are 2 kinds of purposes using ATKey.Pro for RDP
    - Passwordless Login Remote PC via ATKey.Pro
      - This is no issues, just re-direct for login



Re-direct device option:

Remote Desktop Connection

- □ Other supported RemoteFX USB devices
  - ☑ ATKey.Pro-22000037 (redirected)
  - □ LG HD Webcam
  - □ Realtek USB 2.0 Card Reader

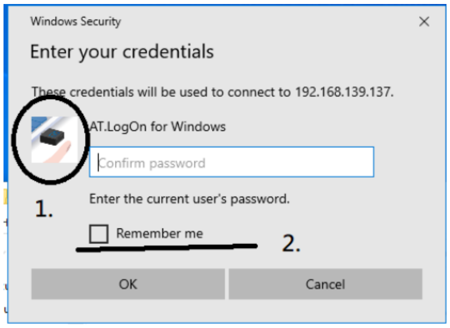
      - So ATKey.Pro belongs “host machine” fido key

- ATKey.Pro for FIDO2 enabled web services or AT.LogOn.Pass
  - ➢ ATKey.Pro (FIDO2 authenticator) work with browser through WebAUTHN (W3C), from Microsoft, starting from Windows 10 21H2 and Windows 11 22H2, then it can allow fido2 authenticator re-direct to remote PC; before the version, it will just reject re-direct ATKey.pro.
  - ➢ So on Remote PC, if user wants to leverage ATKey.Pro for fido2 web service, how to do it?
    1. It must be Windows 10 21H2 build or Windows 11 22H2 build or later versions
    2. Uncheck re-direct ATKey.Pro from toolbar, then the ATKey.Pro can be re-direct for WebAUTHN as browser FIDO2 authenticator

- (User case b.3) ATKey.Pro re-direct to Remote PC (#249), but client PC goes to lock screen (logon screen)
  - Since ATKey.Pro already re-direct to remote PC, so client one can't login via the key at the moment
    - Disconnect wi-fi or network or logout

- (User case b.4) the password failure counter is "N-1" (deduct once)
  - For example, if AD assigned the account password failure counter is 3, but AD password expired (must change password at next login)
  - Since we are using ATKey.Pro login with original password, so it failed once, then ask type in new password, so failure account is deducted; in this case, if user types in password wrong 2 times, account locked since AD counter is 3 times already.

- (User case b.5) Not "run as admin", user can login by typing password, but the check box "Remember me" is useless.



Windows Security

Enter your credentials

These credentials will be used to connect to 192.168.139.137.

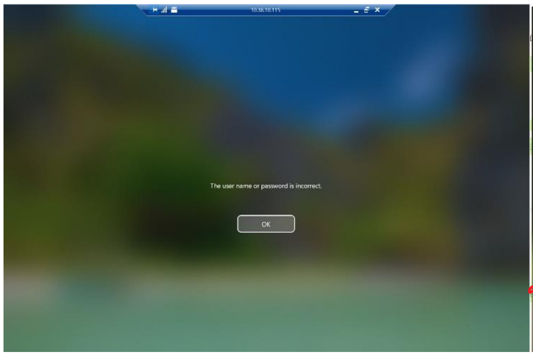
AT.LogOn for Windows

Confirm password

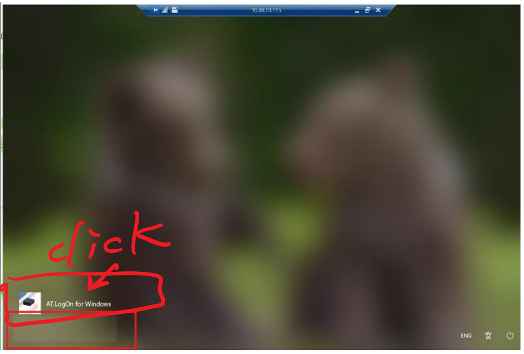
Enter the current user's password.

□ Remember me

- (User case b.6) in some case, remote to remote host, it may show "The user name or password is incorrect", click "OK" to continue, it shows empty option in left-bottom corner, user needs to click "AT.LogOn for Windows" to the Passwordless login screen – fixed on "AT.LogOn for Windows" v0.0.1.8



The user name or password is incorrect.



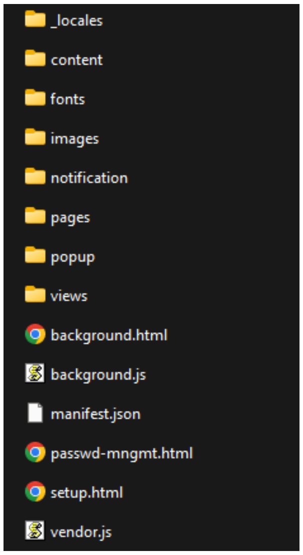
6. AT.LogOn.Pass

To support all “Intranet web services” including legacy one, we developed AT.LogOn.Pass as hardware password manager with fingerprint with Chrome whitelist control, it’s **AT.LogOn.Pass**.

AT.LogOn.Pass is a hardware-based password manager, unlike most existing password management solutions where user credentials such as username and password are stored either in the web browser cache or on a remote server, AT.LogOn.Pass securely stores credentials within the chipset encrypted and accessible only after a user successfully verifies their fingerprint through the authentication process.

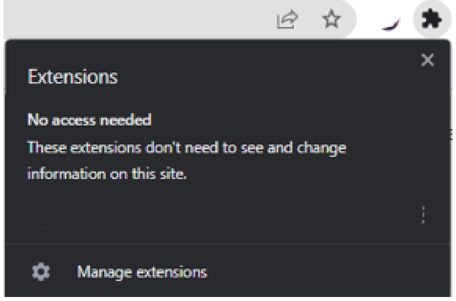
a) Chrome extension

- Here are source files for installation



```
_locales
content
fonts
images
notification
pages
popup
views
background.html
background.js
manifest.json
passwd-mngmt.html
setup.html
vendor.js
```

- From Chrome “Extensions” icon => Manage extensions

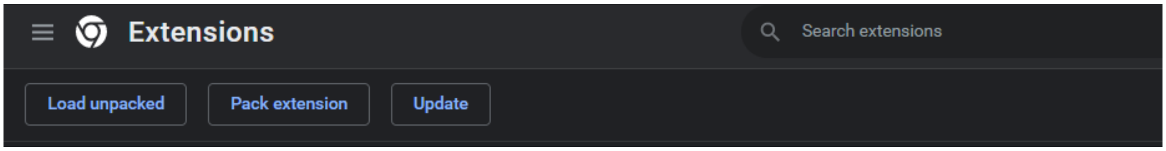


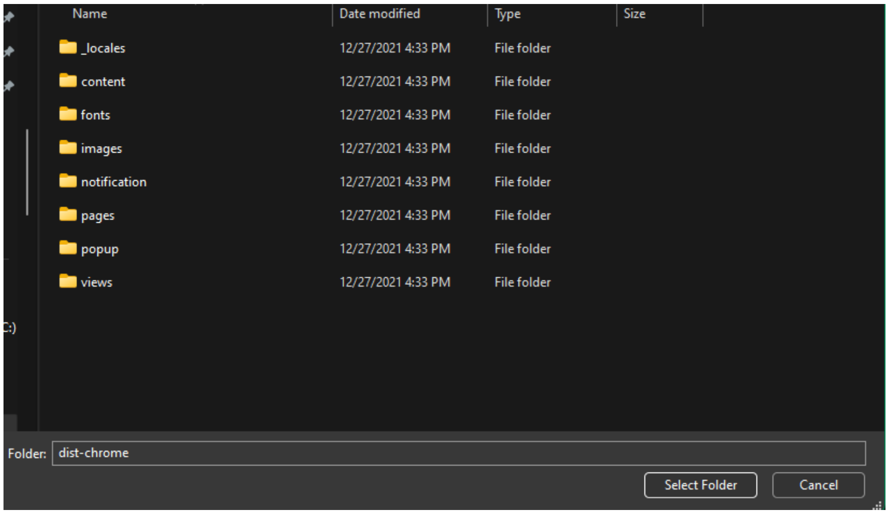
Extensions

No access needed

These extensions don't need to see and change information on this site.

  - Select “Load unpacked”, point to above file folder to “Select Folder”

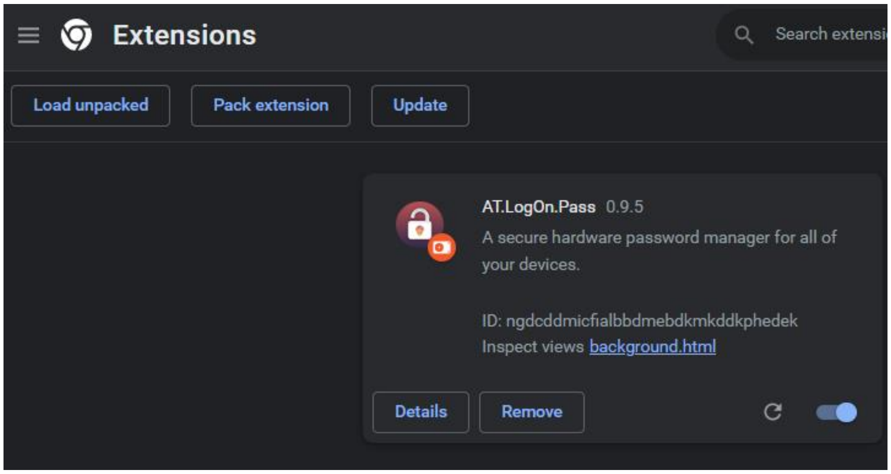




Name	Date modified	Type	Size
_locales	12/27/2021 4:33 PM	File folder	
content	12/27/2021 4:33 PM	File folder	
fonts	12/27/2021 4:33 PM	File folder	
images	12/27/2021 4:33 PM	File folder	
notification	12/27/2021 4:33 PM	File folder	
pages	12/27/2021 4:33 PM	File folder	
popup	12/27/2021 4:33 PM	File folder	
views	12/27/2021 4:33 PM	File folder	

Folder: dist-chrome

- ○ Then AT.LogOn.Pass installed as below and it will jump to initial page directly



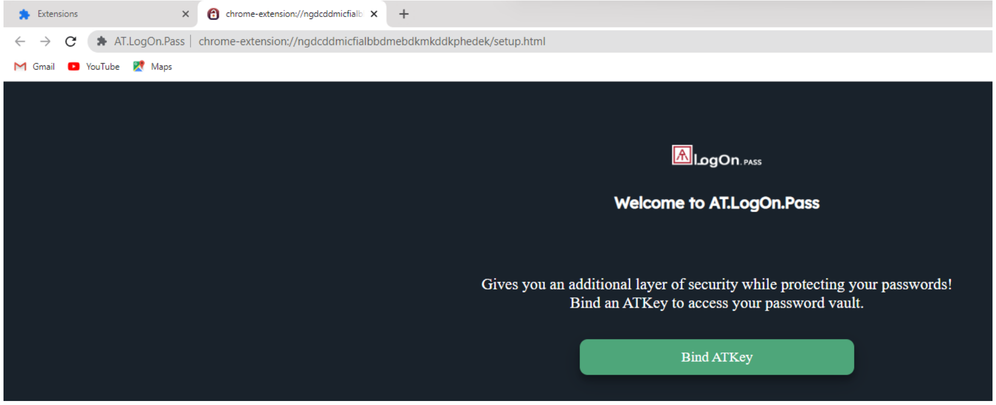
AT.LogOn.Pass 0.9.5

A secure hardware password manager for all of your devices.

ID: ngdcddmicfialbbdmebdkmkddkphedek

Inspect views background.html

- Start binding your ATKey.Pro

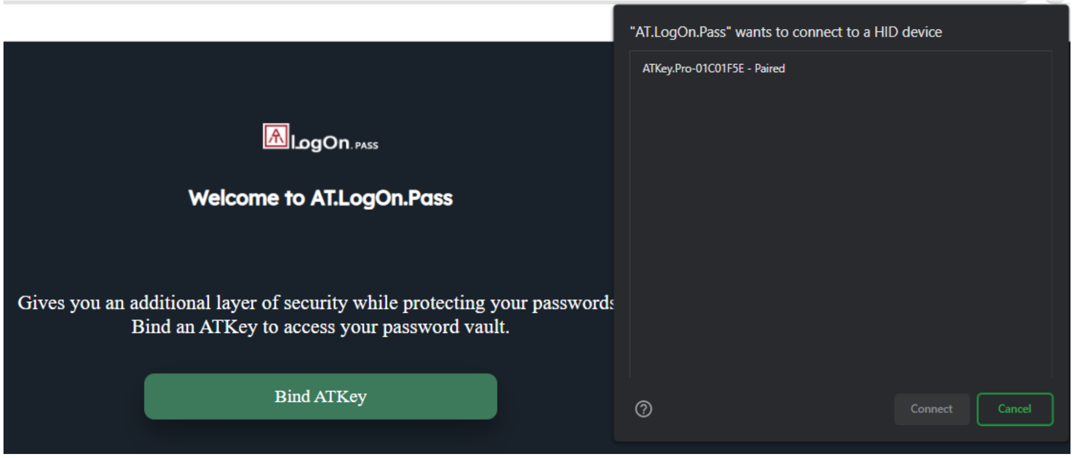


chrome-extension://ngdcddmicfialbbdmebdkmkddkphedek/setup.html

Welcome to AT.LogOn.Pass

Gives you an additional layer of security while protecting your passwords!
Bind an ATKey to access your password vault.

- ○ Please insert your ATKey.Pro to USB port, and click “Bind ATKey”, it will pop up the ATKey on the list including keycode



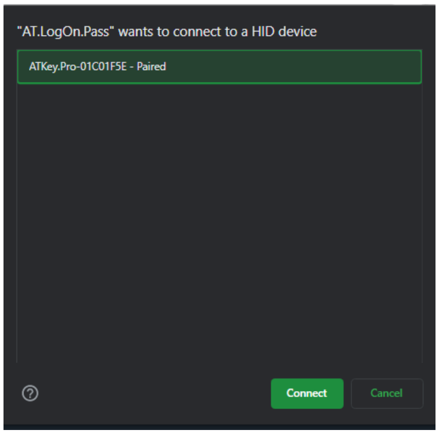
Welcome to AT.LogOn.Pass

Gives you an additional layer of security while protecting your passwords
Bind an ATKey to access your password vault.

"AT.LogOn.Pass" wants to connect to a HID device

ATKey.Pro-01C01F5E - Paired

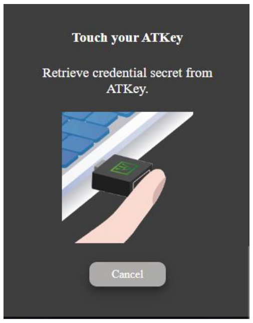
Click the listing ATKey to "Connect"



"AT.LogOn.Pass" wants to connect to a HID device

ATKey.Pro-01C01F5E - Paired

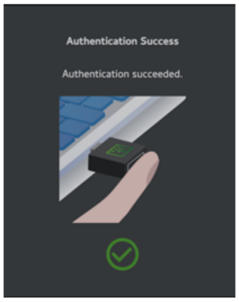
Then ATKey.Pro LED is blue flashing, please verify your fingerprint



Touch your ATKey

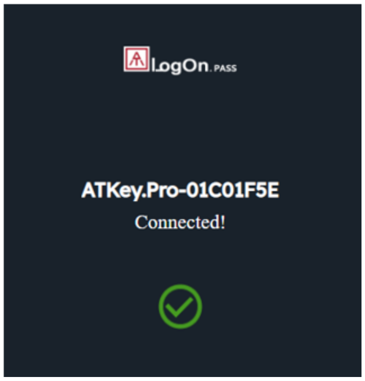
Retrieve credential secret from ATKey.

Fingerprint is matched, binding is done.



Authentication Success

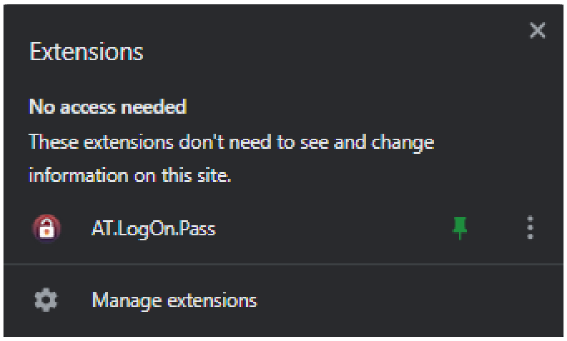
Authentication succeeded.



ATKey.Pro-01C01F5E

Connected!

Then AT.LogOn.Pass installed and show icon on extension bar (pin to extension bar)



Extensions

No access needed

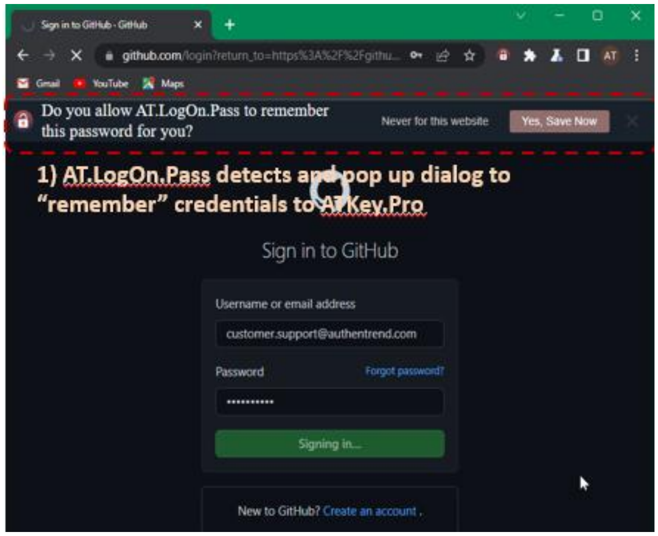
These extensions don't need to see and change information on this site.

AT.LogOn.Pass

Manage extensions

- encrypted Credentials to store inside ATKey.Pro
  - if you enabled Chrome whitelist, only those URLs will be detected and request to save to ATKey.Pro

    To the URL, login by ID/password, login to the URL; you can see a pop up message as below, click "Yes, Store now", so the credential is encrypted and stored to ATKey



Sign in to GitHub · GitHub
github.com/login?return_to=https%3A%2F%2Fgithu...
Gmail
YouTube
Maps

Do you allow AT.LogOn.Pass to remember this password for you?

Never for this website

Yes, Save Now

1) AT.LogOn.Pass detects and pop up dialog to "remember" credentials to ATKey.Pro

Sign in to GitHub

Username or email address: customer.support@authentrend.com

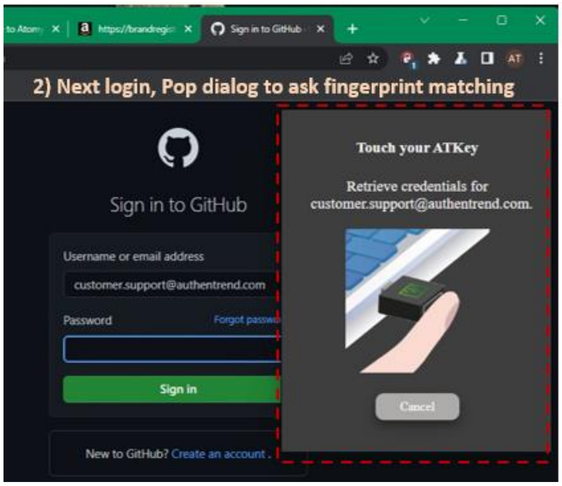
Password: ••••••••••

Forgot password?

Signing in...

New to GitHub? Create an account.

Next time, go to the "saved" URL, AT.LogOn.Pass will detect pop up "Touch your ATKey" dialog (LED is blue flashing), please verify your fingerprint, if matched, auto-fill the ID/Password that we stored inside ATKey.Pro, then click "Sing in" to login



2) Next login, Pop dialog to ask fingerprint matching

Sign in to GitHub

Username or email address: customer.support@authentrend.com

Password

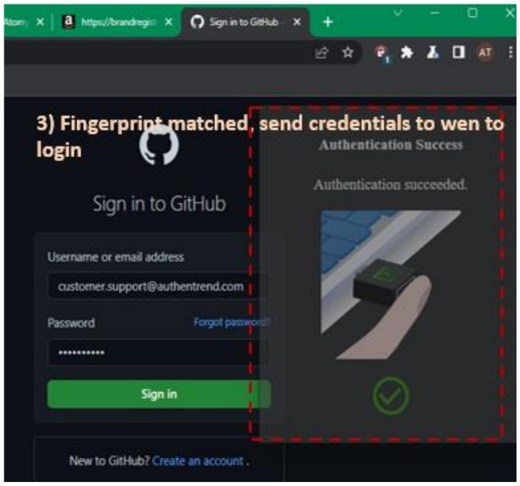
Sign in

New to GitHub? Create an account.

Touch your ATKey

Retrieve credentials for customer.support@authentrend.com.

Cancel



3) Fingerprint matched, send credentials to wen to login

Authentication Success

Authentication succeeded.

Sign in to GitHub

Username or email address: customer.support@authentrend.com

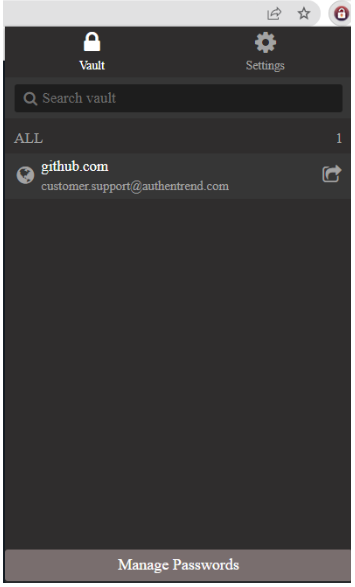
Password: ••••••••••

Sign in

New to GitHub? Create an account.

Please check Video here: https://www.youtube.com/watch?v=7g3gjnb5mPA for the user operations, we take Github as example here.

- AT.LogOn.Pass management
  - Click icon for the dialog, it will show all "stored" URLs

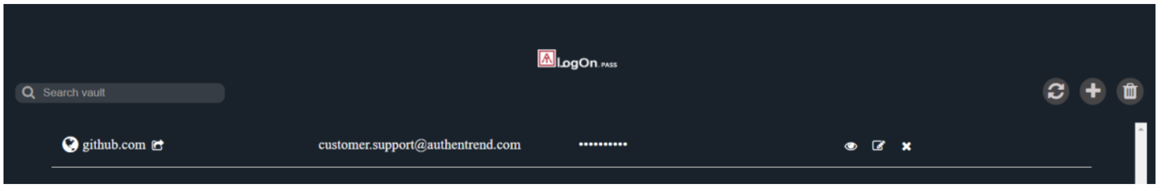


ALL 1

github.com
customer.support@authentrend.com

  - You can click the URL as bookmark to the web site

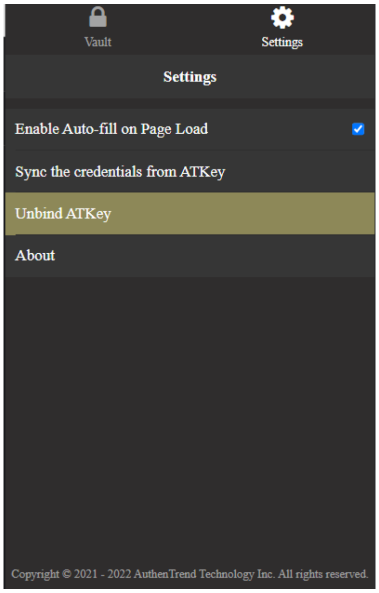
  - "Manage Passwords"



github.com customer.support@authentrend.com ••••••••••

You can view/edit the password (after fingerprint verified)
You can delete the saved URL (fingerprint verified)
You can add new one manually

  - Settings



Enable Auto-fill on Page Load ☑

Sync the credentials from ATKey

Unbind ATKey

About

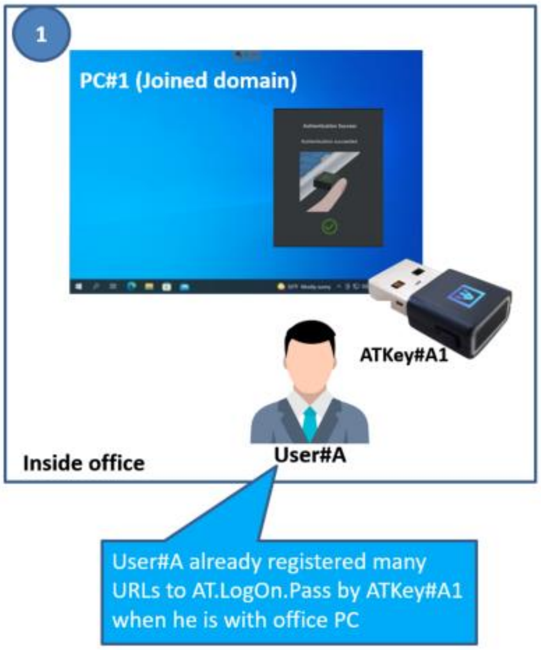
Copyright © 2021 - 2022 AuthenTrend Technology Inc. All rights reserved.

b) Chrome whitelist

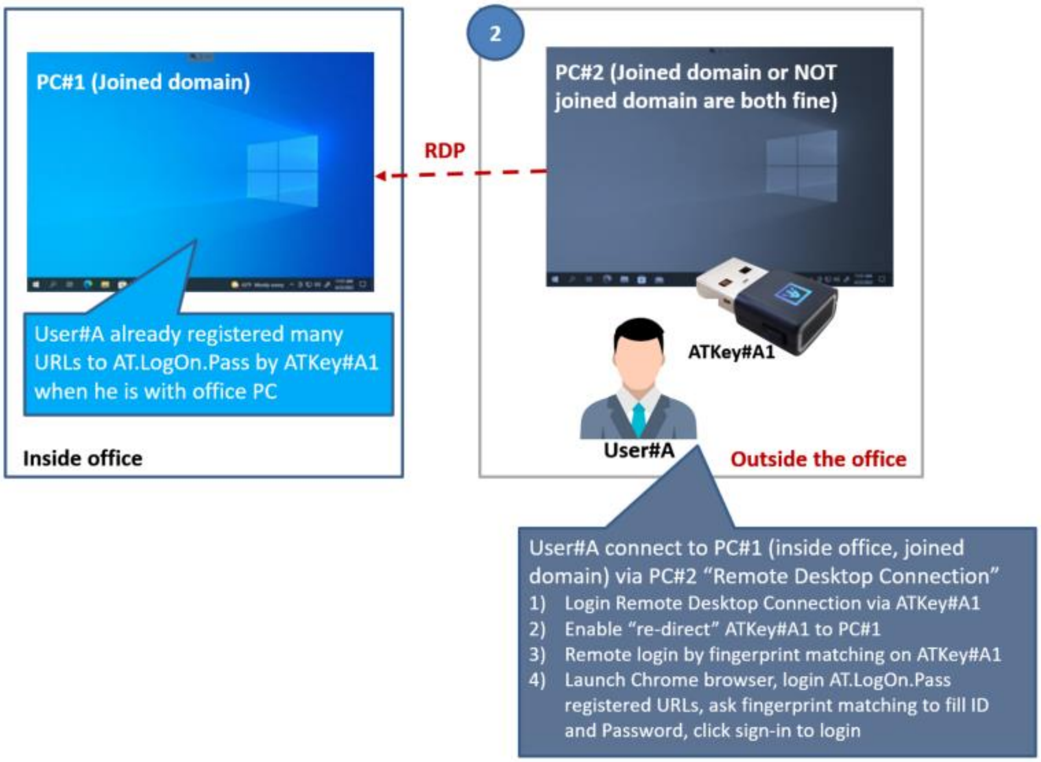
- It's better to enable Chrome whitelist for organization allowed intranet or internet URLs only, to avoid users leverage this feature for all internet URLs, it will be out of control for admin and also for our product response since too many different kinds of URLs WW, we won't deal one by one if user meets issues, we can only guarantee Admin allowed intranet or internet URL works.

c) AT.LogOn.Pass via RDP

- [User case c.1]
  i. User#A with ATKey#A1 works on joined-domain PC#1


1
PC#1 (Joined domain)
ATKey#A1
Inside office
User#A
User#A already registered many URLs to AT.LogOn.Pass by ATKey#A1 when he is with office PC

  ii. User#A is outside the office with home PC#2 or shared office PC#2 but not joined domain (Or joined domain), but User#A still wants to login intranet URL (on PC#1) via ATKey#A1



User#A already registered many URLs to AT.LogOn.Pass by ATKey#A1 when he is with office PC

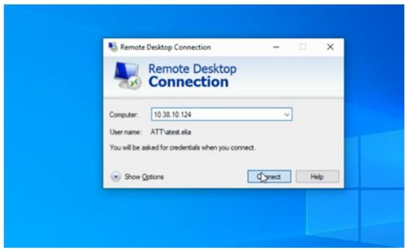
User#A connect to PC#1 (inside office, joined domain) via PC#2 "Remote Desktop Connection"

1) Login Remote Desktop Connection via ATKey#A1
2) Enable "re-direct" ATKey#A1 to PC#1
3) Remote login by fingerprint matching on ATKey#A1
4) Launch Chrome browser, login AT.LogOn.Pass registered URLs, ask fingerprint matching to fill ID and Password, click sign-in to login

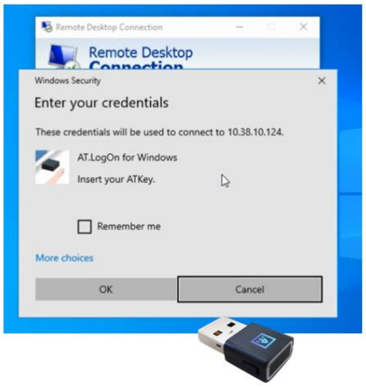
iii. User flow:

- Remote Desktop Connection

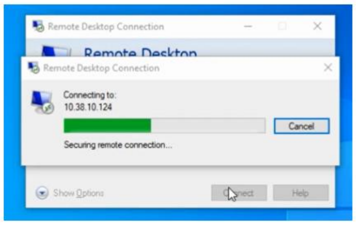
  Computer IP address, Connect, fingerprint matching on ATKey to connect.



Computer: 10.38.10.124
User name: ATT\atest.ella
You will be asked for credentials when you connect.



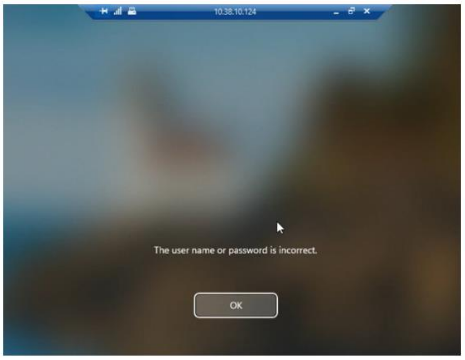
Enter your credentials
These credentials will be used to connect to 10.38.10.124.
AT.LogOn for Windows
Insert your ATKey.
□ Remember me



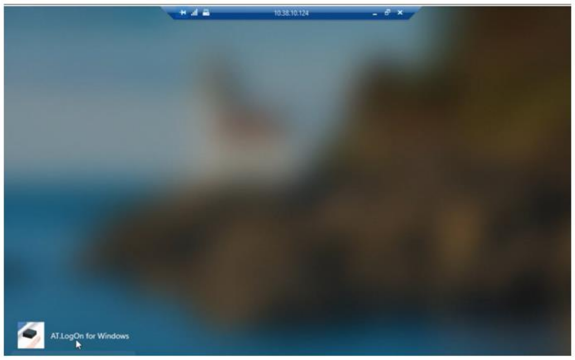
Connecting to:
10.38.10.124
Securing remote connection...

- Remote Windows lock screen

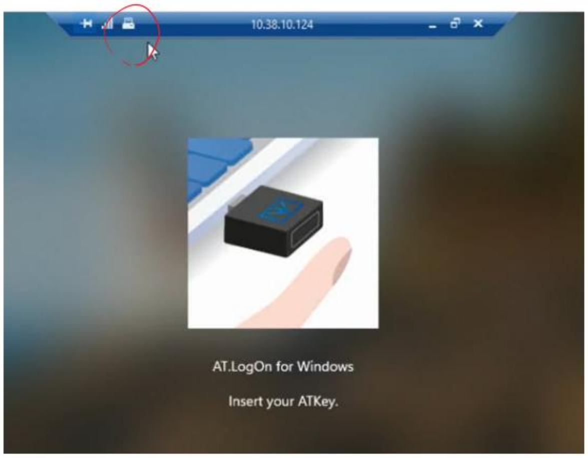
  In some cases, it may show "The user name or password is incorrect", click "ok" and select "AT.LogOn for Windows" to continue



The user name or password is incorrect.

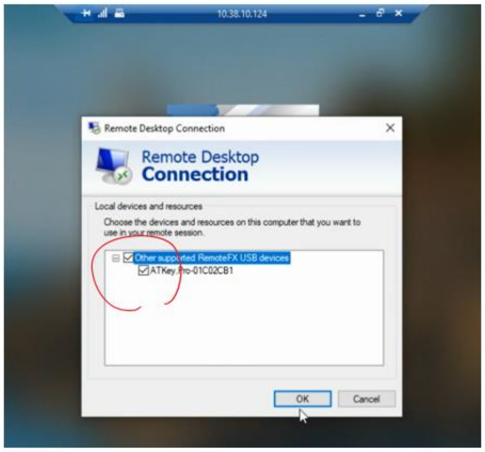


Re-direct the “ATKey.Pro”, then fingerprint matching on ATKey.Pro to remote login



AT.LogOn for Windows

Insert your ATKey.



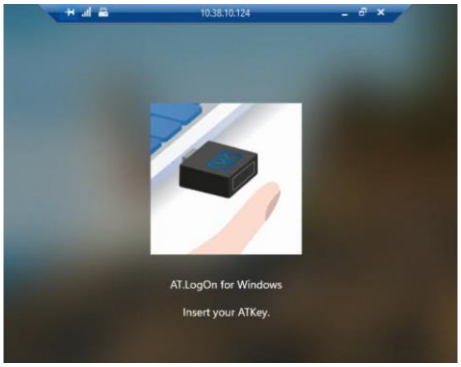
Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

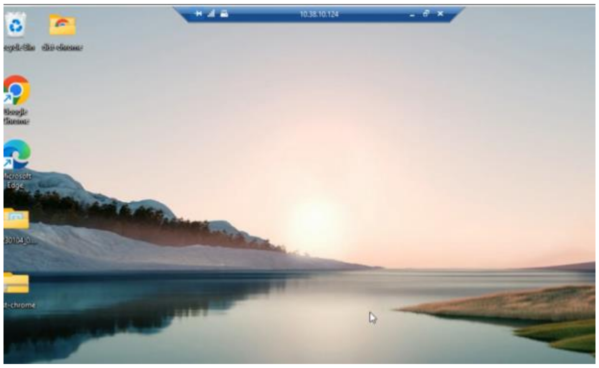
☑ Other supported RemoteFX USB devices

☑ ATKey.Pro-01C02CB1

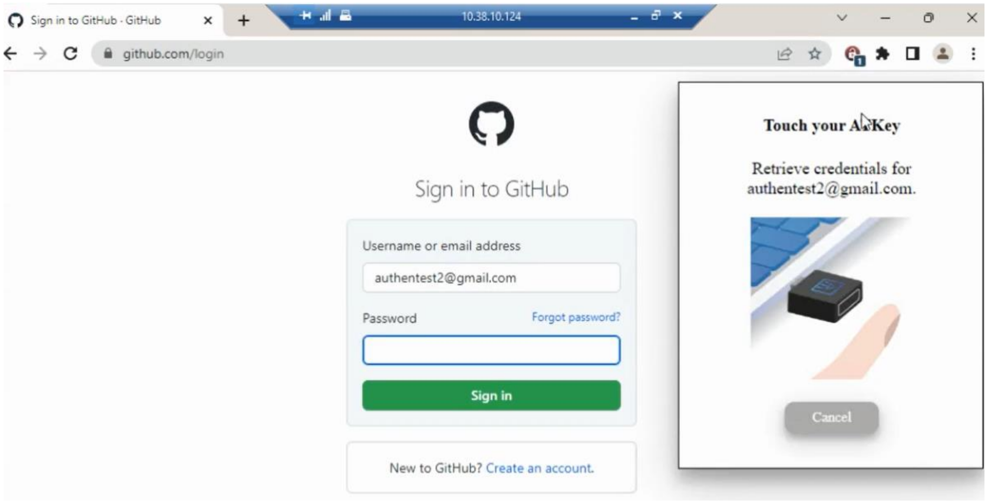


AT.LogOn for Windows

Insert your ATKey.



- Launch Chrome browser, go to the registered URL to login, fingerprint matching to auto-fill the ID/password to login



Sign in to GitHub

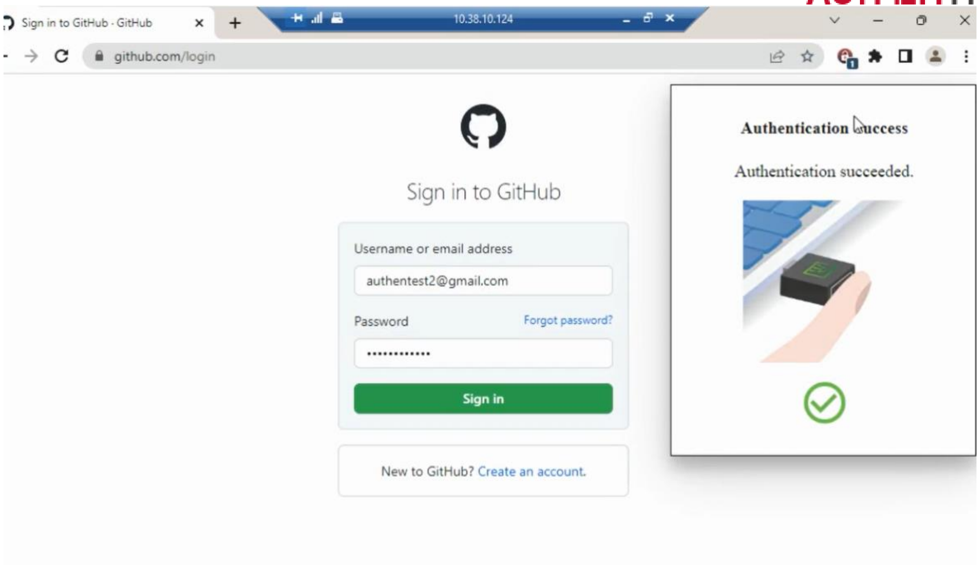
Username or email address: authentest2@gmail.com

Password

New to GitHub? Create an account.

Touch your ATKey

Retrieve credentials for authentest2@gmail.com.



Sign in to GitHub · GitHub

10.38.10.124

github.com/login

Sign in to GitHub

Username or email address

authentest2@gmail.com

Password

Forgot password?

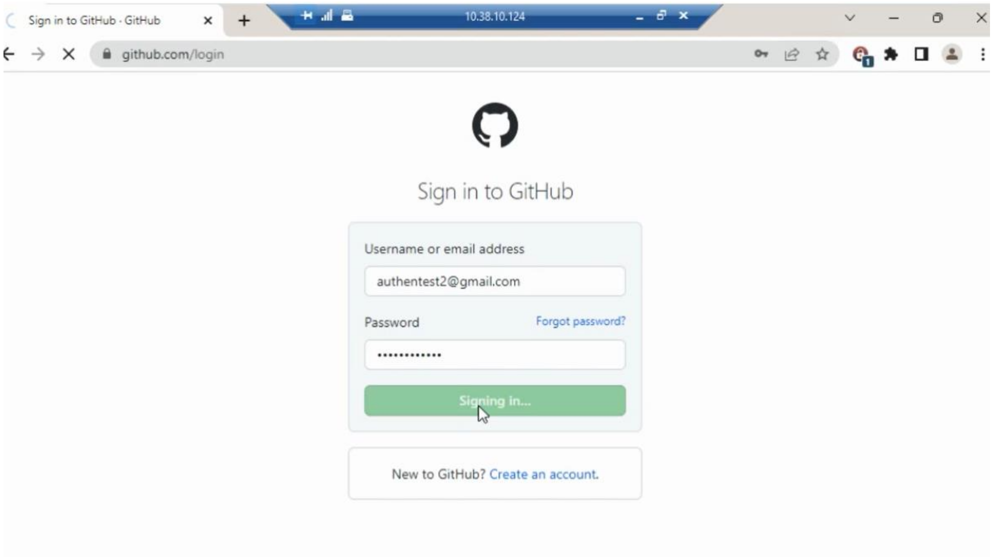
••••••••••••

Sign in

New to GitHub? Create an account.

Authentication success

Authentication succeeded.



Sign in to GitHub · GitHub

10.38.10.124

github.com/login

Sign in to GitHub

Username or email address

authentest2@gmail.com

Password

Forgot password?

••••••••••••

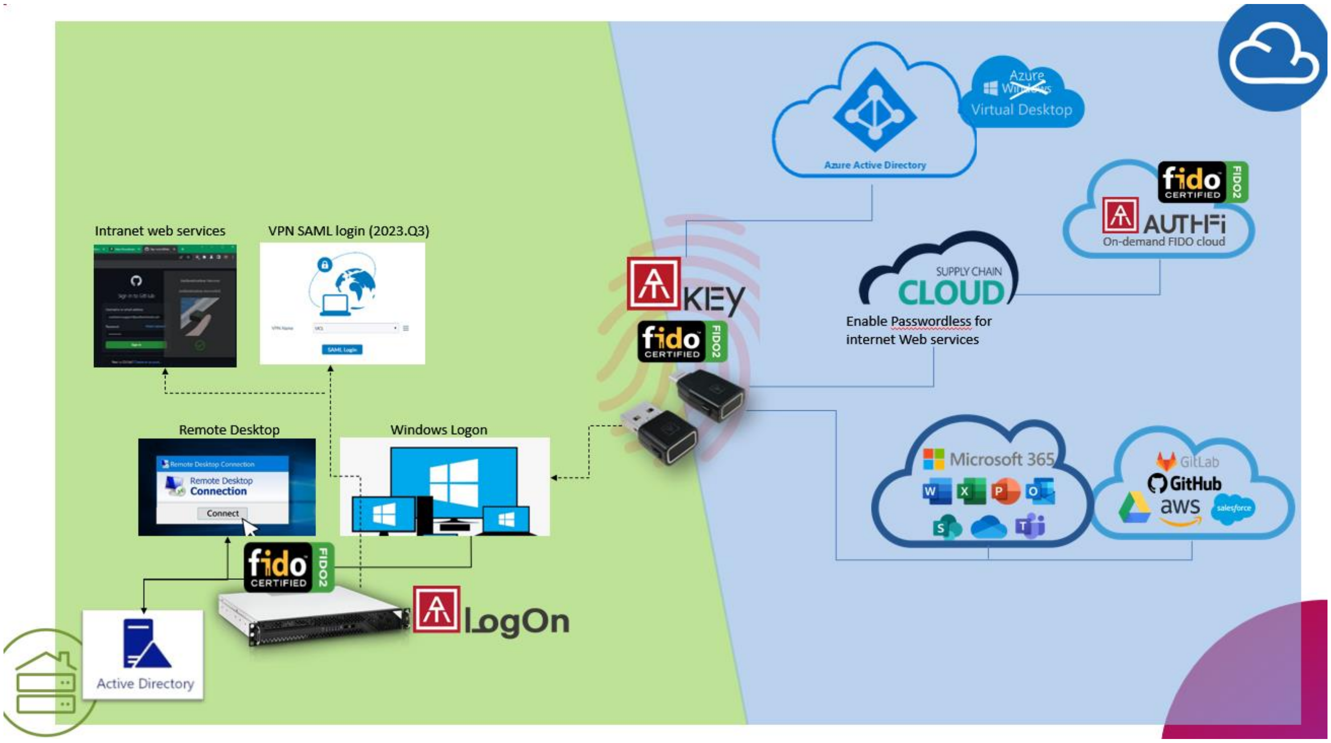
Signing in...

New to GitHub? Create an account.

- In some cases (registered URL login), if LED of ATKey.Pro is not flashing, please close your browser and re-launch it again to make sure it can really talk to ATKey.Pro remotely well; or disable then re-enable “redirect” from RDP caption bar to let AT.LogOn.Pass can find ATKey.Pro remotely well.

7. More from ATKey.Pro

Since ATKey.Pro is fido2 certified authenticator, it can also work with any FIDO2/U2F enabled web services, not limited for AT.LogOn only.



- Only when the LED of ATKey.Pro is blue flashing, it's time to touch the sensor for fingerprint matching
- if the ATKey.Pro LED is not blue flashing as you expect, you can try to remove the key (from USB) and re-insert to USB port to see if the LED from static BLUE to flashing BLUE.
- For RDP, since it needs to re-direct ATKey to remote, it may needs longer response time, so even screen shows "touch fingerprint sensor on key", but please still wait till LED blue flashing
- If the LED is static RED, it means you may fail on fingerprint matching 3 times continuously, please remove it and insert to USB port again to try; ideally, it's only allowed 5 cycles (3 times continuous failure, 5 cycles) failure, and it will be locked (only reset key can unlock it, but everything will be gone from the key).
- If LED has no color, please remove and try again; if LED is static white, please remove it and try again; if LED is cyan color, please remove and try again;

Please find more detail information from: https://authentrend.com/atkey-pro/