AUTHENTREND

AT LogOn

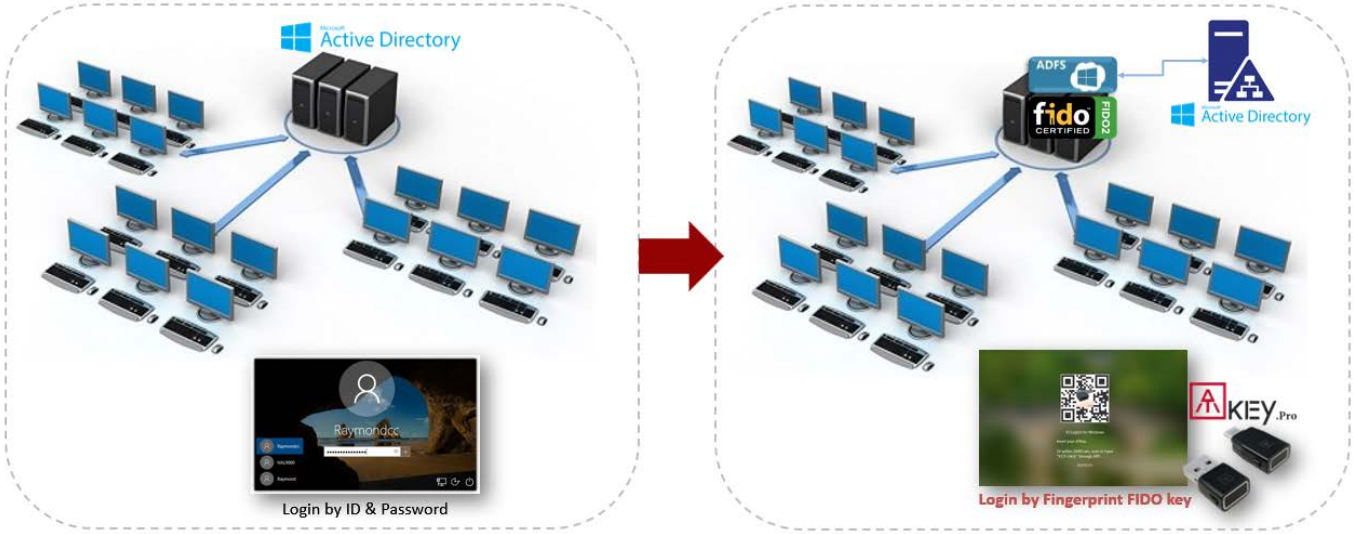
# ユーザーガイド *(管理者用)*


**REVISION: 1.0**
**DATE: 2022 DEC.**

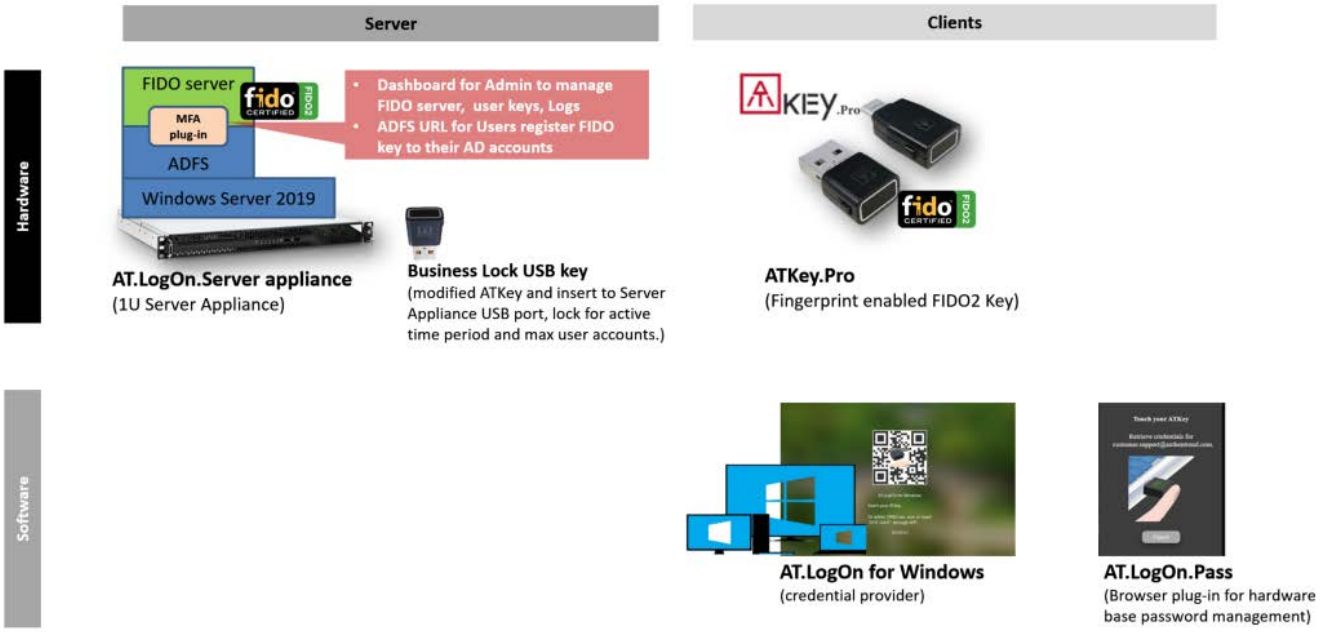
# Table of Contents

# 1. AT.LogOn について

AT.LogOn は、オンプレミスの Active Directory 環境（AD ドメイン PC）をご利用中の企業様をターゲットにしており、FIDO2 パスワードレスにより AD 認証情報を保護し、ユーザー体験を簡素化。IT 管理の労力を軽減します。

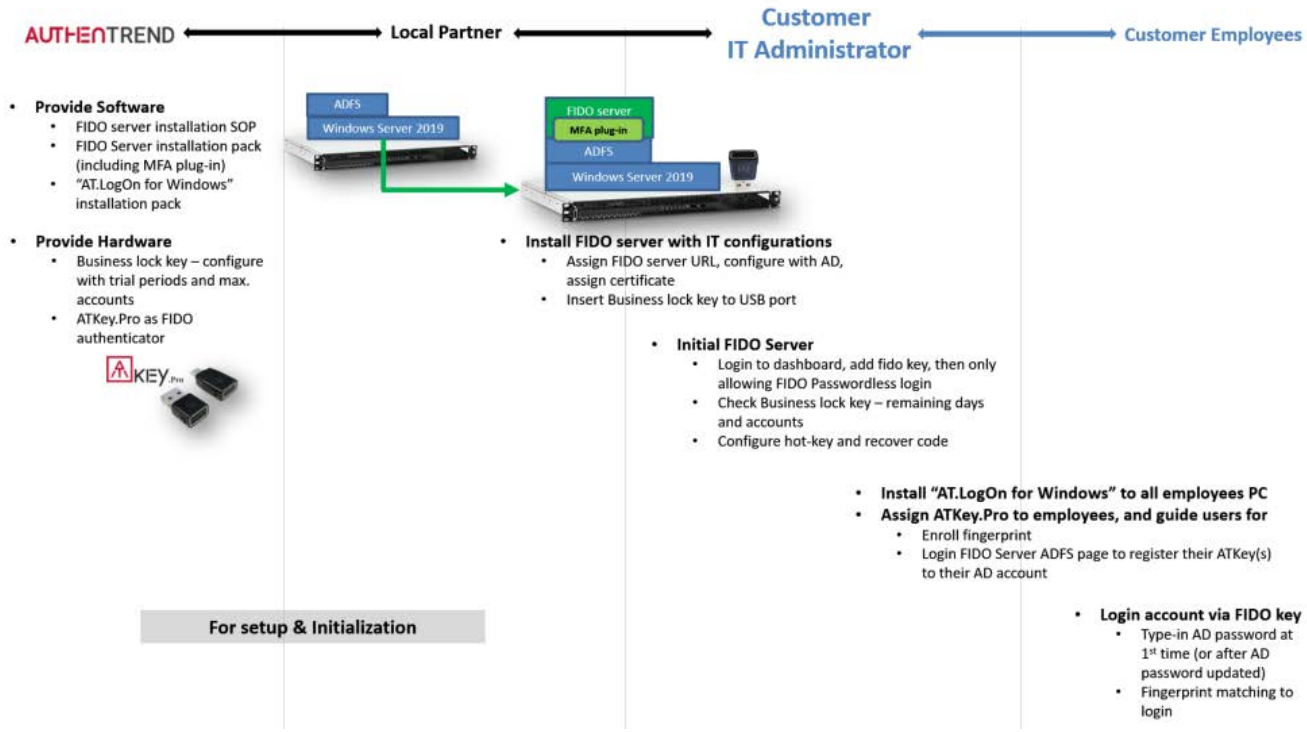



## a) AT.LogOn には以下の利用/環境が含まれます



b) AT.LogOn は以下のシナリオでパスワードレスログインを実現できます。


c) AT.LogOn は複数の利用シーンを定義しており、このユーザーガイドは“お客様の IT 管理者様”を対象にご説明いたします。



# 2. IT 管理者 – 初期化と登録

## a) URLs の定義と注目点

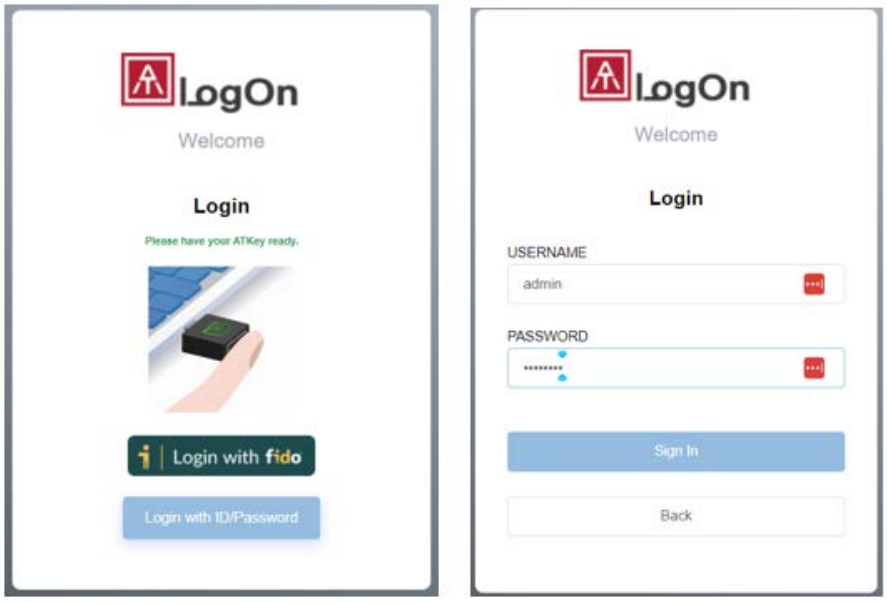
- 事前に以下の定義についてご注意ください：
  - ADFS URL
    - この URL はローカルパートナーから提供される AT.LogOn.Server のインストレーションの AT FIDO server パック(プロパティの設定)の中に定義されています。
    - これはサーバーのインストール時にローカルパートナーによって事前に定義する必要があります。通常では：
      - ✓ adfs01.domainname,com（例 “adfs01.atlogon.com”）
    - この URL もまた、社員用 PC にサイレントインストールするために AT.LogOn for Windows 内のバッチファイルを定義する必要があります。
  - ATKey URL の登録
    - ユーザーの ATKey.Pro をユーザーの AD アカウントに登録します。
    - URL は ADFS が自動的に割り当てします。
      - ✓ 例えばあなたの ADFS URL が“adfs01.domainname.com”の場合, “//adfs01.domainname.com/adfs/ls/idpinitiatedsignon”となります。
  - AT.LogOn.Server のダッシュボード URL
    - AT.LogOn.Server を管理するために管理者がログインする為のものです。
    - “//adfs01.domainname.com/dashboard/” のようになります。

## b) AT.LogOn.Server の初期設定

**流れ:**

**(1) ログイン => (2) ID/Password の変更 => (3) ATKey.Pro の登録 => (4) ビジネスロックキーの状態確認 => (5) “ホットキー” と “リカバリコード”を有効にする**

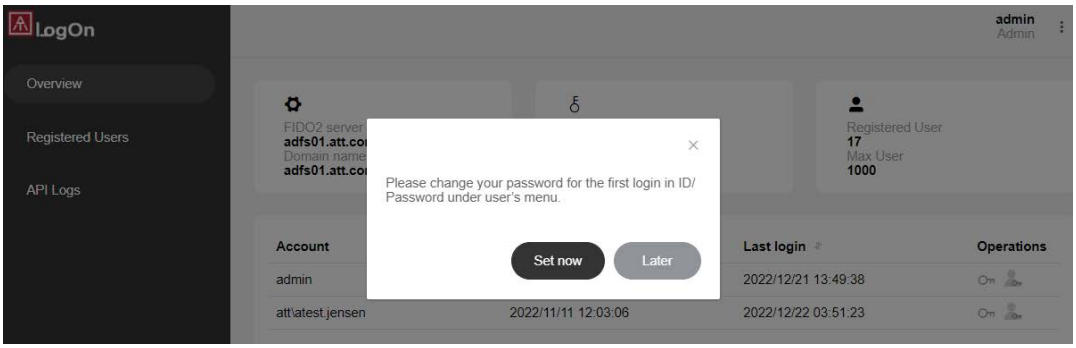
- 初回ログイン(“https://adfs01.domainname.com/dashboard/”) – ID/Password でログインします。

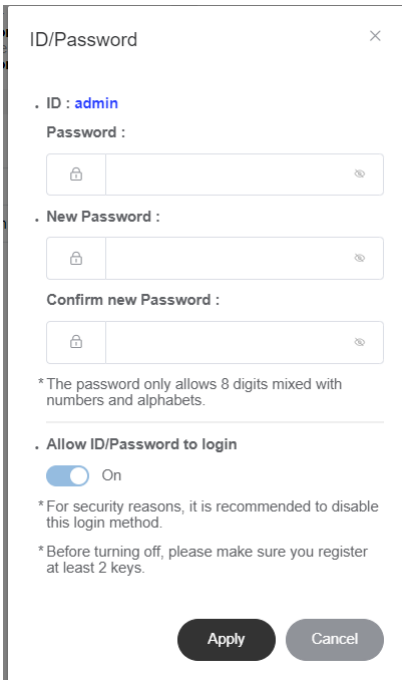



  - デフォルト ID/password は下記となります:

- ID: admin
- Password: password

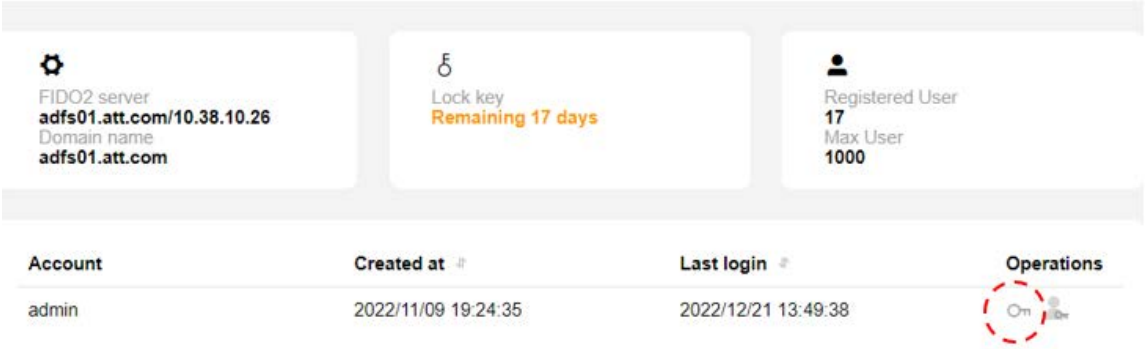
- ログインすると、ログイン ID とパスワードの変更を要求されます。



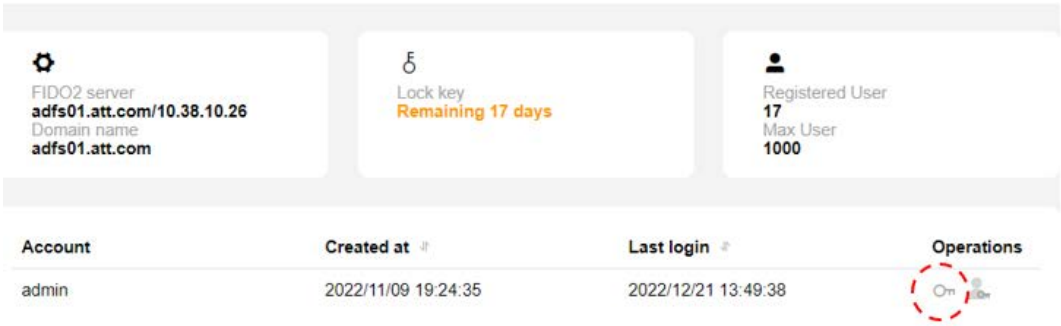




  - ✓ パスワードの代わりに ATKey.Pro をパスワードレスログイン認証機として登録することができます。
    - *管理者は ATKey.Pro をアカウントに登録する前に必ず Atkey.Pro に指紋を登録してください。*
  - ✓ ATKey.Pro を紛失したり、ログインが出来なってしまった場合に備えて“ID/Password”でのログインを許可する事は管理者のみ(1 人)が、行えます。

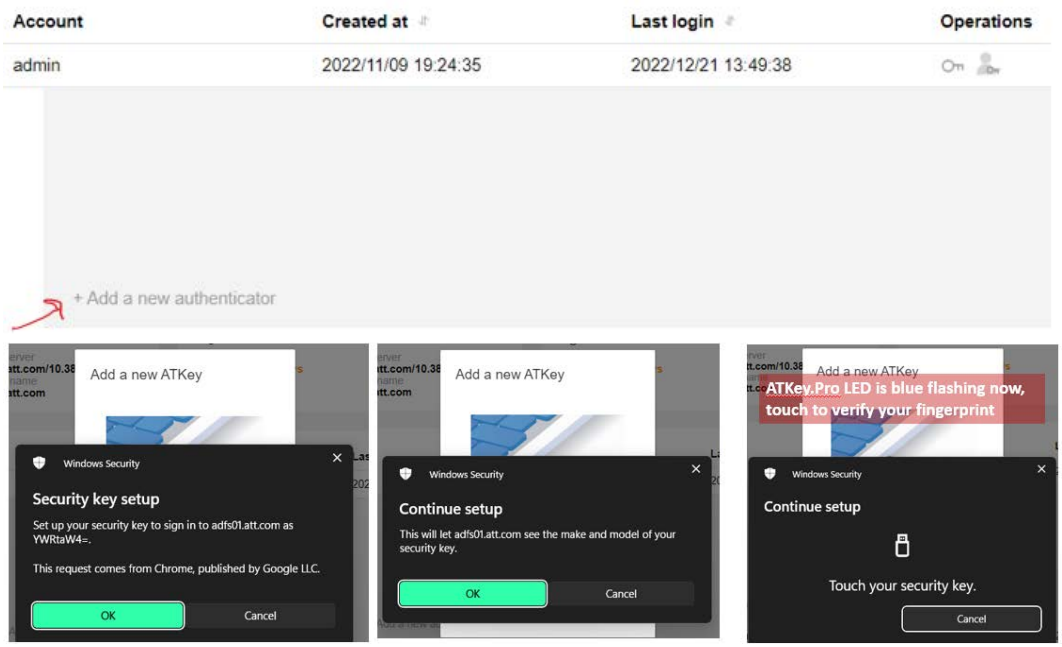
- ATKey.Pro を登録すると管理者はパスワードレスログインが可能になります。



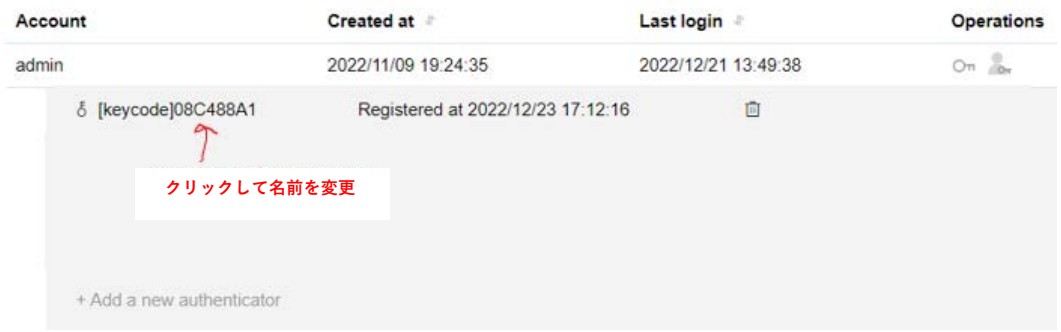

- “鍵”のアイコンをクリックします(赤丸でハイライト)




- “+ Add a new authenticator”(新しい認証機を追加)をクリック

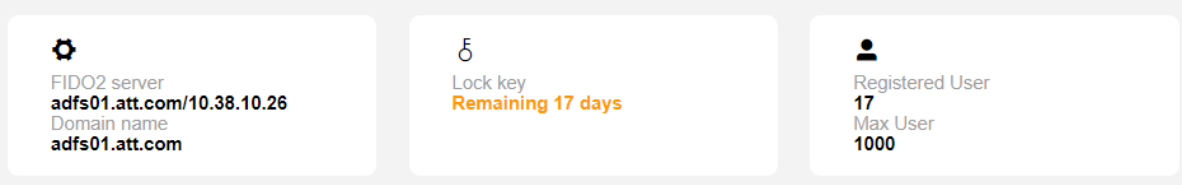



- 成功すると新しい認証機として追加/表示され、クリックすれば認証機の名前変更ができます。(ATkey.Pro 本体に刻印されたユニークキーコードを使用する事をお勧めします)



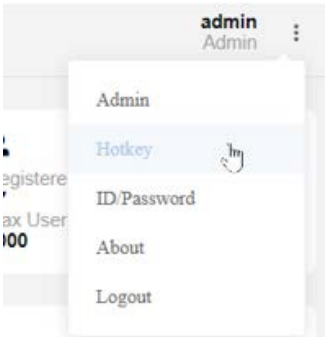

- ✓ *ATKey.Pro の紛失した際に備えて、管理者用アカウントには最低 2 つの認証機を登録することをお勧めしています。*

- ビジネスロックキーの状態を確認する。

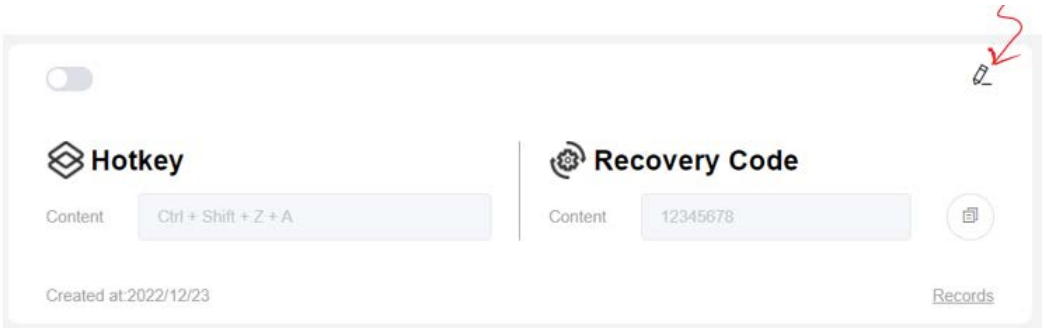



  - 1 ブロック目のサーバーと URL の情報です
  - 2 ブロック目の表示 – ビジネスロックキーの有効期間
    - ✓ ビジネスロックキーは初回ログインからカウントされます。(残り日数がカウントされます)
    - ✓ 残り日数が 30 日を切ると、文字が黄色になり、ビジネスロックキーの LED が黄色点滅し始めるのでビジネスロックキーを更新する為に新しいビジネスロックキーの交換をサービスプロバイダーに問い合わせしてください。
    - ✓ 期限切れになってしまうと文字が赤になり、ビジネスロックキーの LED も赤色点灯しサービスがロックされます(認証が出来なくなります)ので、新しいビジネスロックキーの交換をサービスプロバイダーに問い合わせしてください。

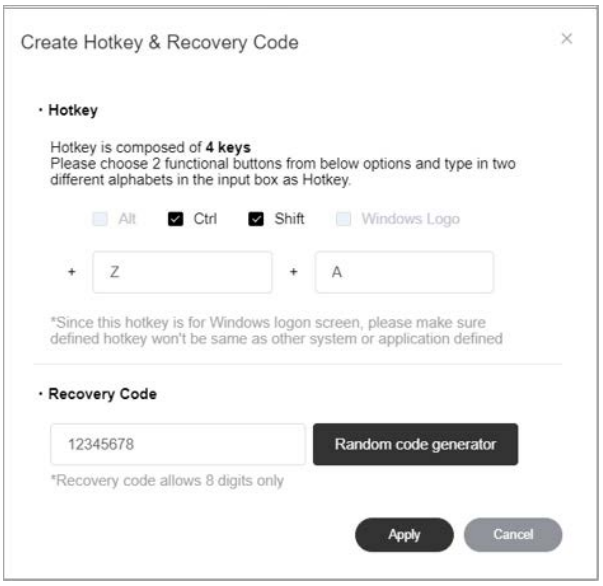
- “Hotkey”(ホットキー)と“Recovery Code”(リカバリコード)の設定
  - これはユーザーが緊急時にやむを得ず AD の ID/パスワードでログインができるようにする為の設定です。
    管理者画面のリスト項目から入ってください。



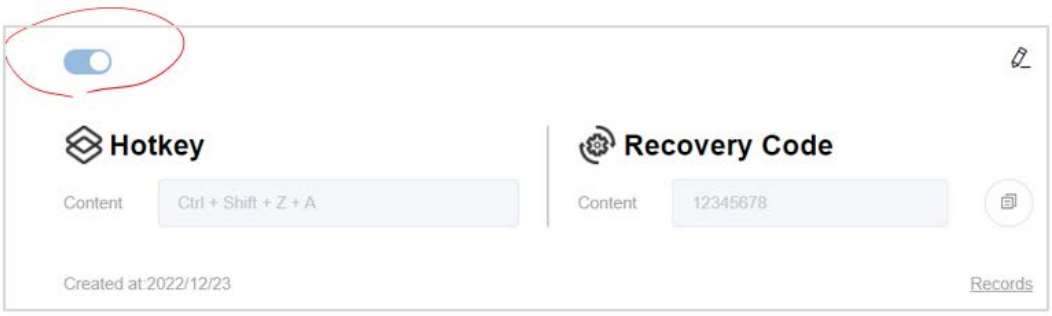
“edit”(編集)(ペン型のアイコン)をクリックして”Hotkey”(ホットキー)と”Recovery Code”(リカバリーコード)を設定します。




ホットキーのルールに従って設定し、リカバリーコードを入力するか、ランダムで生成します。



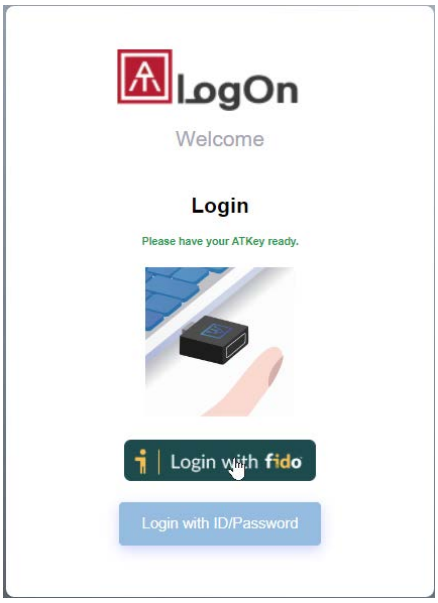

“Apply”の機能を ON にしてください。

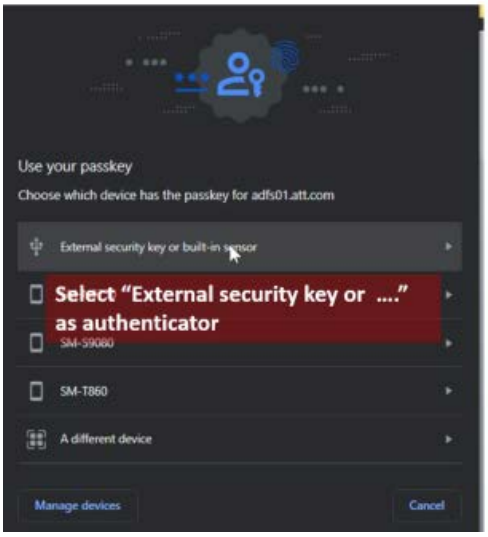


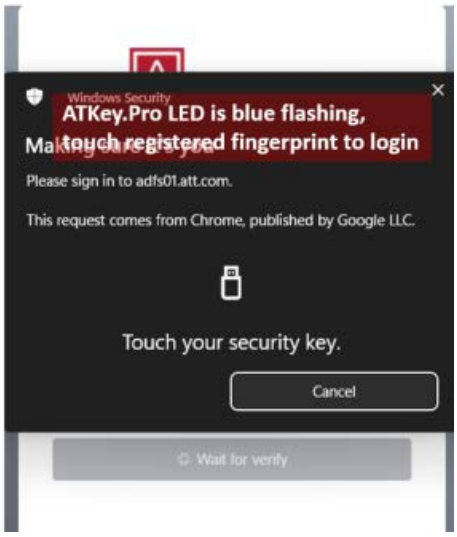

- ✓ Windows のログイン画面で、オンラインかつドメインに参加している場合、クライアントは「ホットキー」と「リカバリーコード」を同期し、ローカルで暗号化します。
- ✓ ”Hotkey”(ホットキー)と”Recovery code”(リカバリコード)を定期的に変更する、またはユーザーが一度でも利用した場合は、変更することをお勧めします。
- ✓ ホットキーとリカバリーコードの履歴が必要な PC（常にオフラインまたはドメイン外）は、”Records”(記録)をチェックして、ログインするためのホットキーとリカバリーコードを確認することができます。


- AT.LogOn.Server の設定と初期化が完了したら
  - 手動でログアウトするか、ブラウザを閉じてセッションを終了してください。
  - 管理者がログアウトまたはブラウザのタブを閉じなかった場合、10 分後に自動的にログアウトしますが、その間の１０分間は同じ管理者アカウントでログインすることはできません。

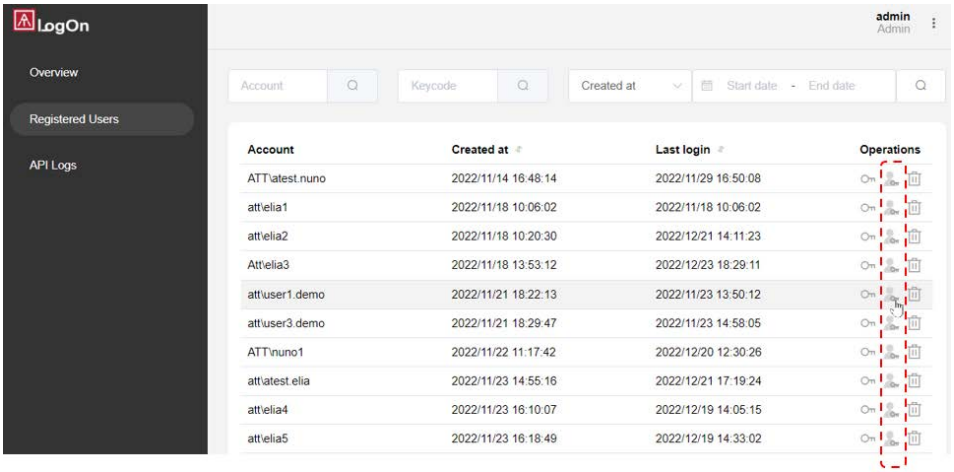
- ２回目のログインから
  - 登録した ATKey.Pro でログインします。



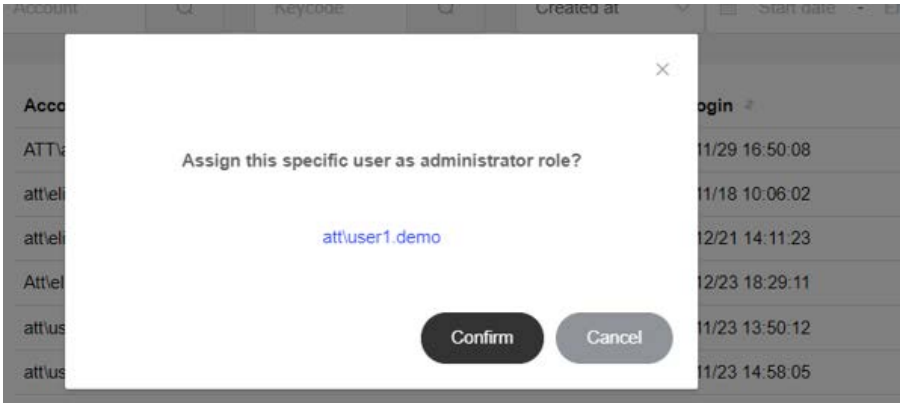


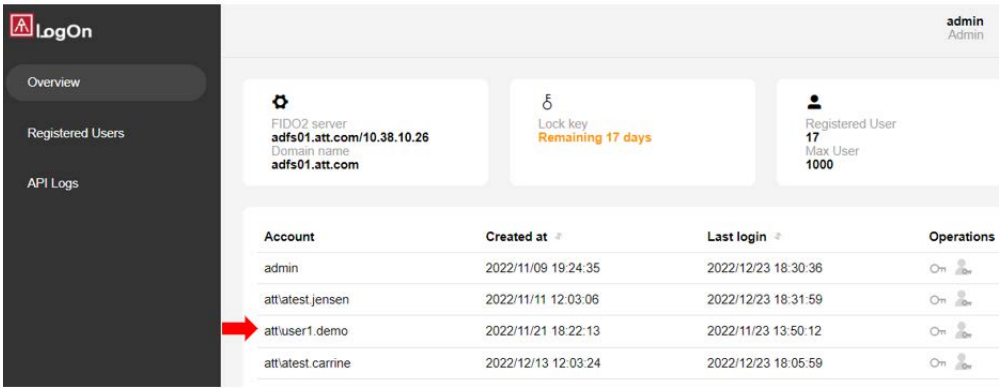

- より多くの管理者を割り当てる場合
  - 管理者は“Registered Users”(登録したユーザー)を選択して、管理者権限を付与することができます。
    - ✓ ユーザーを選択して、以下のように”admin icon”(管理者アイコン)をクリックします。



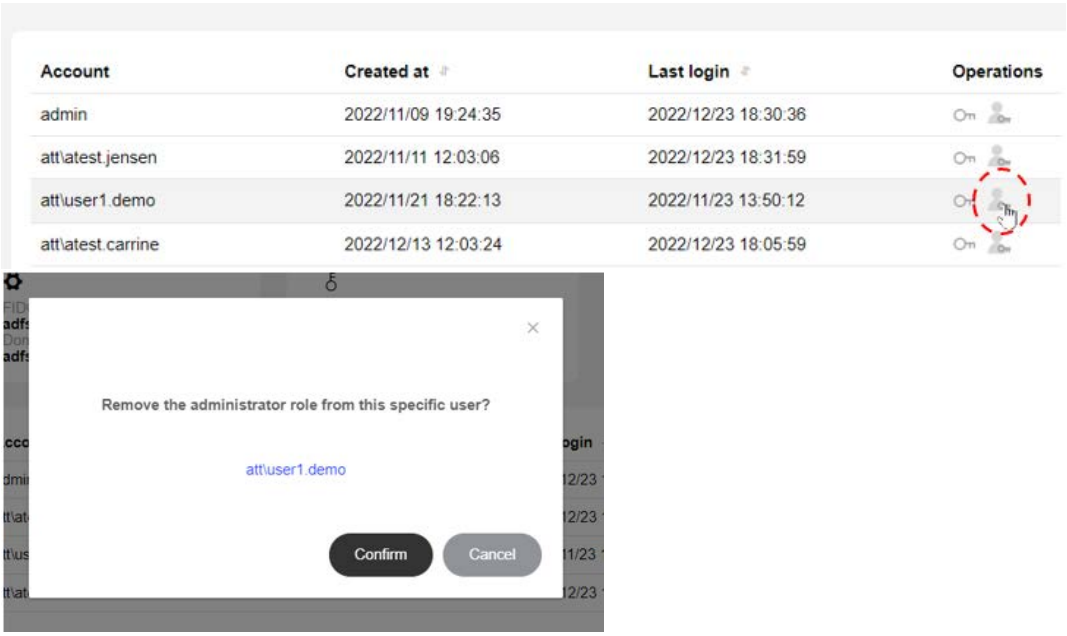

    - ✓ ユーザーの確認をします。
    - ✓ “Overview”画面に選択したユーザーが表示され、そのユーザーが管理者としてログイン出来るようになります。



✓ 管理者の ATKey.Pro で AT.LogOn.Server のダッシュボードにアクセスできます。

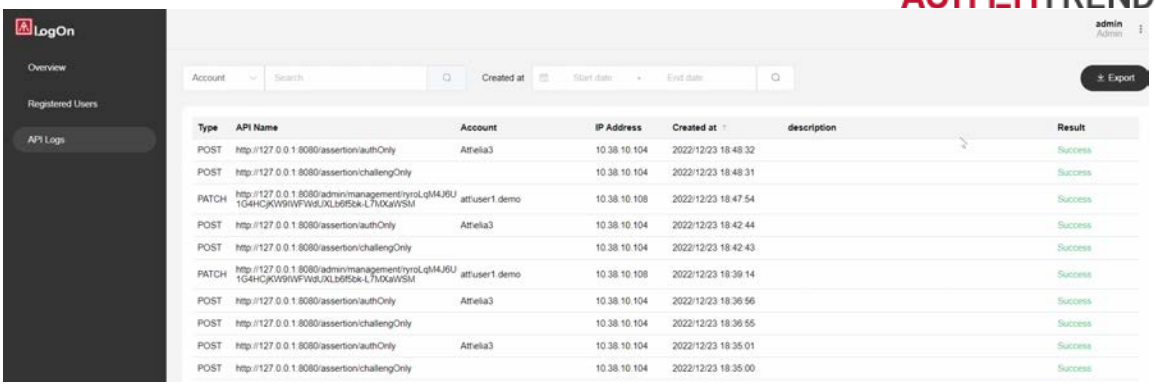



- ログインした管理者は、別の管理者をリストから削除することもできます。




- 複数の管理者、または 1 人の管理者が複数のキー(ATKey.Pro)を持つ場合。
  - ✓ 複数の管理者のログインを許可することはできますが、異なるアカウントでなければなりません（同じアカウントが ID/パスワードまたは異なる登録 ATKey.Pro を介して並行してログインすることはできません）。
  - ✓ すべての設定や管理を終えたら、「ログアウト」してください。

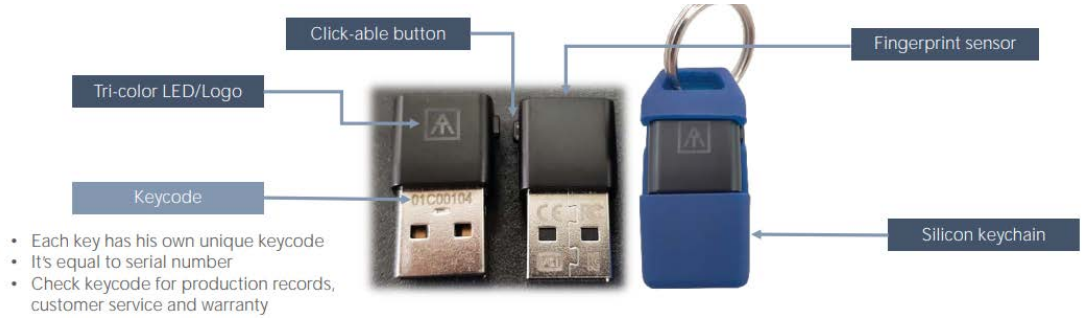
- API ログ
  - 要求するログの確認または検索（各 API から）




- デバッグに必要なログ（日付、種類、...等）をエクスポートして送信します。
  - API ログは膨大な記録(全 API の記録)になる可能性があるので、デバック用にファイルとしてエクスポートする場合は、エクスポートファイルの期間を 3 日間にしてください。
  - エクスポートファイルはブラウザからダウンロードできます。（ブラウザのデフォルトのダウンロードフォルダに保存されます）ファイル名は常に "ExportLog.csv" です。

## c) ATKey.Pro を従業員に割り当てる

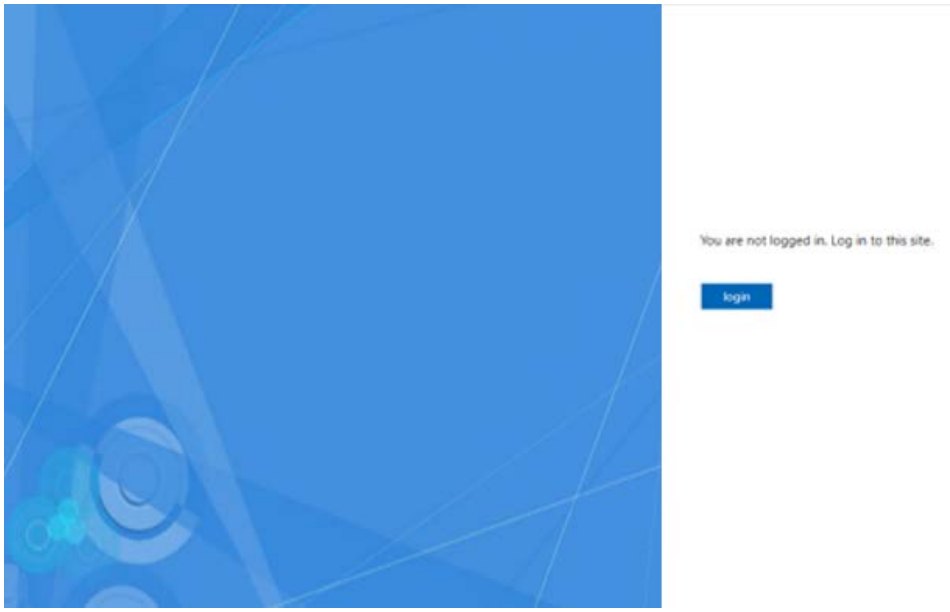
- ATKey.Pro と従業員(keycode)
  - 理想的には 1 人の従業員に対して 1 つのキー(ATKey.Pro)で、それぞれのキーには固有のキーコードがレーザーインクで本体に印字され、キー内部のハードウェアチップにも保存されています。
  - AD アカウントへ ATKey.Pro を登録する時は、管理しやすいようにユーザー(従業員)はキーコードを入力する必要があります。
    - キーコード（8 桁）は、ハードウェアチップ内の固有コードで、各 ATKey.Pro のシリアル番号でもあります。



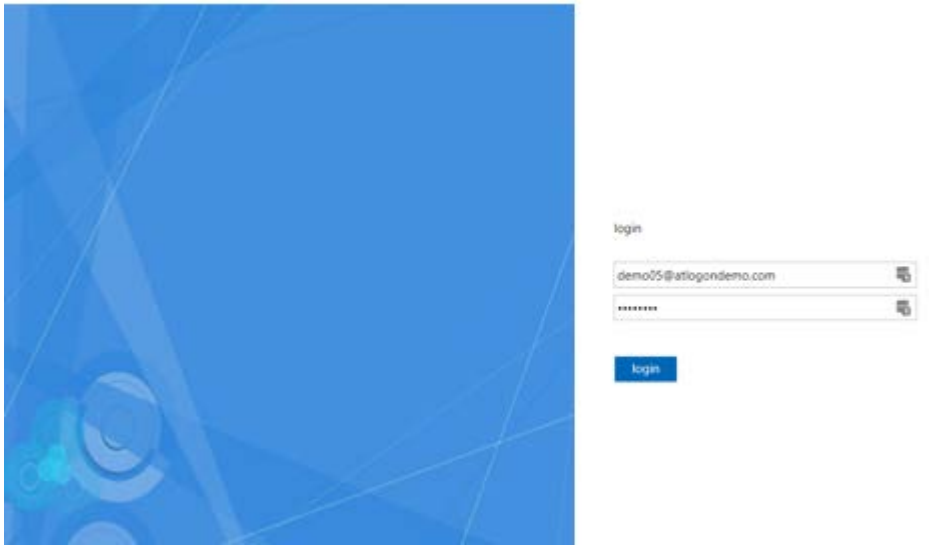

  - 1 人のユーザー(従業員)は複数の ATKey.Pro を登録できます、一つの ATKey.Pro には最大 10 個の指紋が登録できます。
    - 管理者にはキーを紛失してしまった場合に備えて 2 個の ATKey.Pro を登録するか、複数の管理者を割り当てることを推奨しております。
    - 万が一登録した指に問題が生じて認証できなくなってしまった場合に備えて、それぞれの ATKey.Pro に最低でも 2 本の指紋を登録することを推奨しています。

- 従業員に指紋の登録を案内してください。
  - ATKey.Pro に指紋を登録する方法は下記の方法でできます。
    - Windows の設定(Windows 10 build 1903 以降)
    - Chrome ブラウザ (セキュリティとプライバシー) ※Windows を除く
    - Standalone enrollment: https://youtu.be/NnNqXbrf7vA (AuthenTrend 特許技術)
  - 指紋の登録方法については動画でご確認ください： https://youtu.be/bCLPMtZJhkM
  - ATKey.Pro に最低でも 2 本の指紋を登録することを推奨しています。

- AD アカウントへの登録(ATKey の登録 URL)
  - chrome ブラウザを開いて割り当てられた ATKey の登録 URL を入力します。
    (例): https://fs.domainname.com/adfs/ls/idpinitiatedsignon

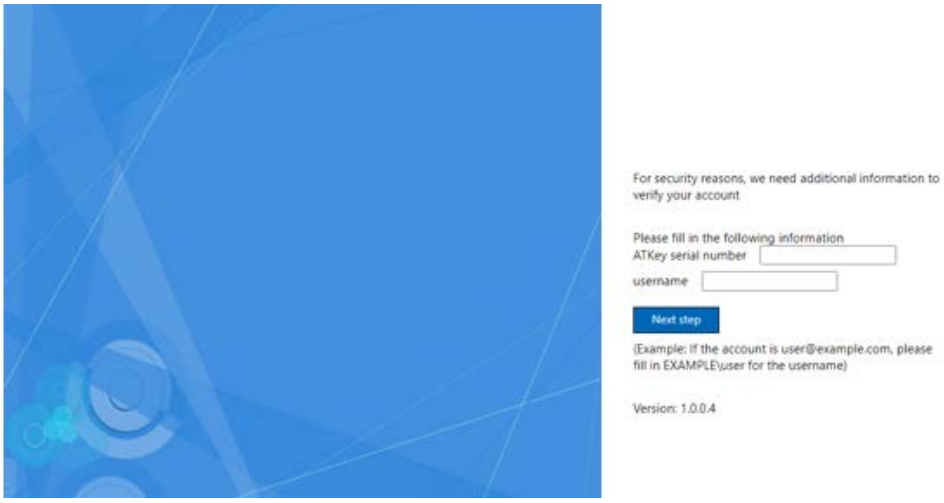



  - ユーザー(従業員)の AD ID/PWD でサインインします。

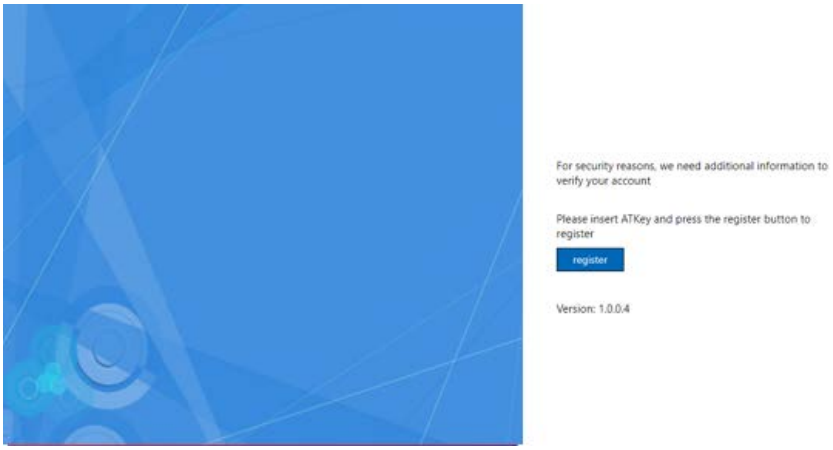


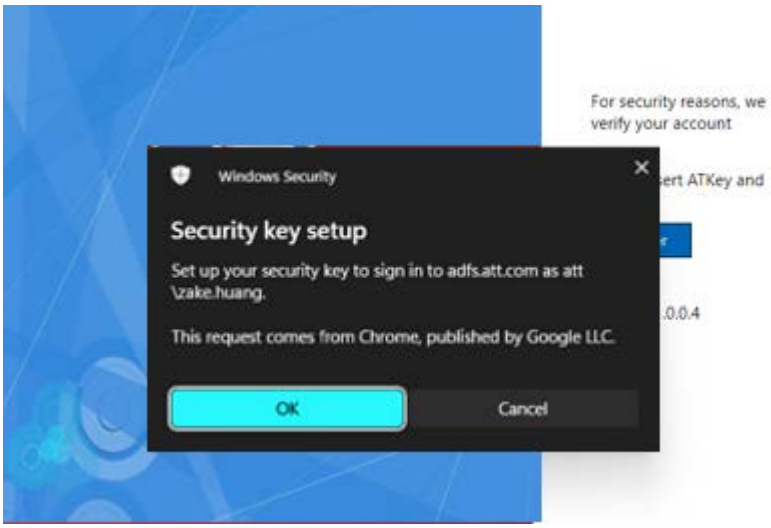

  - 初めて FIDO 認証を行う場合 - ATKey.Pro のキーコードとユーザー名を入力してください。
    - Keycode(キーコード) – ATKey.Pro のどこにキーコードが表示されているか？下記の写真をご覧ください。キーコードは 8 桁のユニークコードで本体表面にレーザーインクで刻印されており、内部にも保存されています。

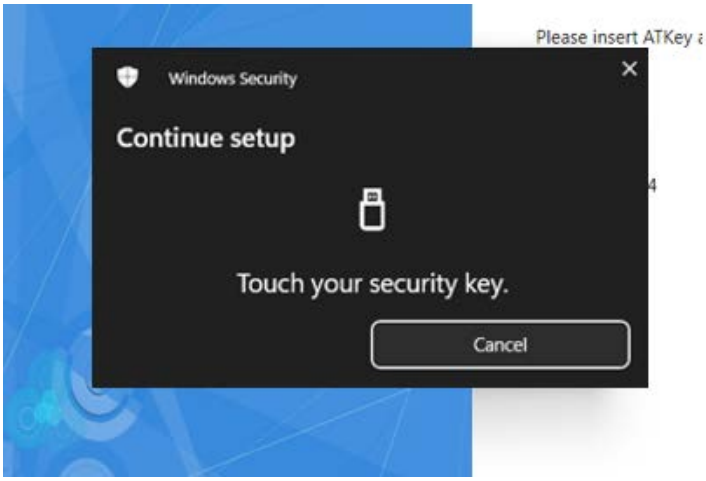
- ご注意：”username”(ユーザーネーム)は変更が出来ないので、必ず正しく入力してください。
  - Format:  domainname¥username




- Register を押して ATKey.Pro の指紋を照合したら完了です。

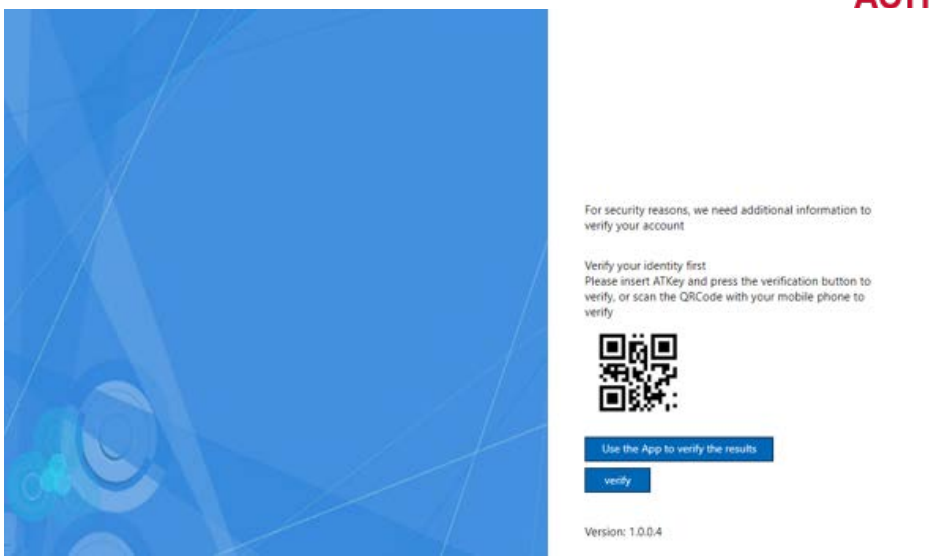


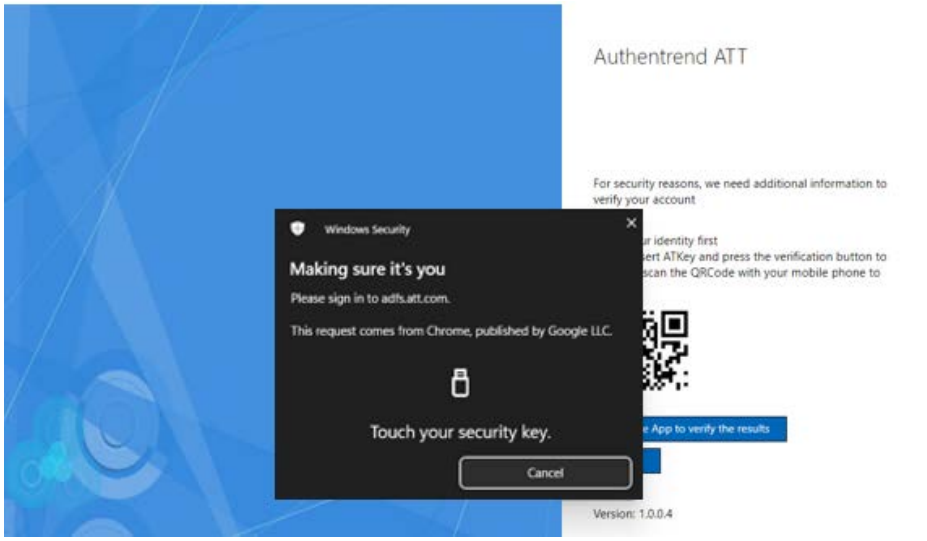


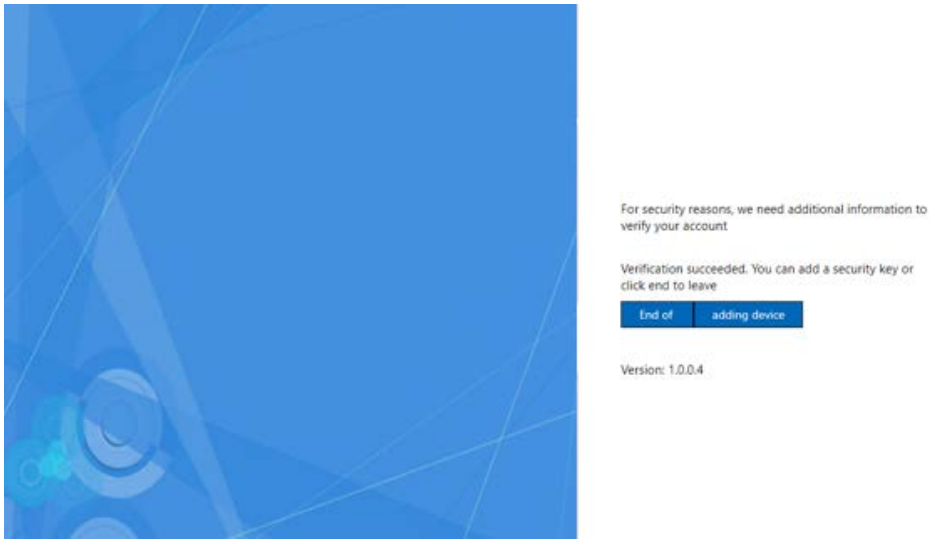




- 管理者は”Dashboard”(ダッシュボード)から登録されたユーザーのレコード(ユーザー名とタイムスタンプ)を見つけてください。

- ユーザーアカウントに他の ATKey.Pro が既に登録されている場合、セキュリティ上の理由から、既に登録されている ATKey.Pro の認証を行う必要があります。その場合、”Verify”(確認)のボタンをクリックします。



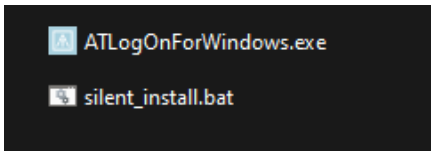

“Adding device”をクリックし, 上に表示されている“Add new key”に戻る – keycode, username, register

r

- 但し、万が一最初に登録した ATKey.Pro を紛失してしまったりして認証ができない場合、管理者は登録されているその ATKey.Pro を Dashboard(ダッシュボード)から削除することもできます。

## d) “AT.LogOn for Windows”を従業員の PC にインストールしてください。

- インストールするには 2 つのファイルが存在します。




  - サイレントインストール用にカスタマイズしたバッチファイルまたは管理者が以下の 3 項目のバッチファイルを修正することもできます：


    - 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="
```

- “Silent_install.bat”でインストールする。

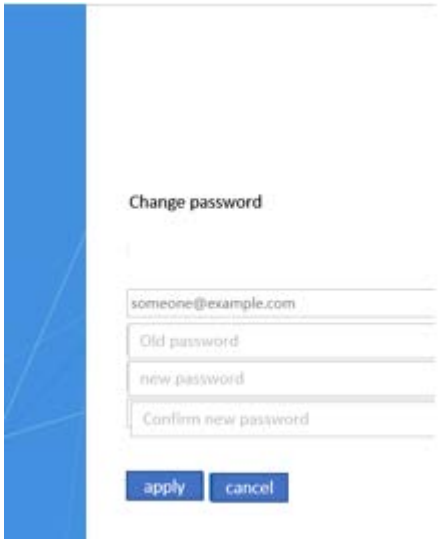
## e) 管理者のユーザーケース

- (ユーザーケース d.1) 既存の従業員、既存の PC
  - ATKey.Pro をユーザーに割り当てる
  - ユーザーが ATKey.Pro に指紋を登録(最低 2 本の指を登録する事を推奨)
  - ATKey.Pro をユーザーの AD アカウントを登録します。
  - ユーザーの PC に(AT.LogOn for Windows)をインストールします。
  - 登録した ATKey.Pro の指紋認証で Windows にログオン
    - 1 回目: ユーザーは AD パスワードを入力して認証する必要があります。– 接続のため、オンラインかつドメイン内で行う必要があります。
    - 2 回目以降: ユーザーは指紋タッチでログインができます。
    - 但し、AD のパスワードが定期的なメンテナンスや手動などで変更された場合、指紋認証した後システムは変更されたパスワードを入力するように要求されます。1 回目と同

じように一度 AD パスワード入力認証を行えば 2 回目位以降は指紋認証でログインができます。

- (ユーザーケース d.2) 新入社員や転職写真(初回のパスワード変更)
  - 既にデフォルトの AD アカウントとパスワードが割り当てられていて、ユーザーが初めてログインした時にアカウントとパスワードを変更する必要がある場合
    - 初回のログインは ADFS のページで行われます(AD アカウントに ATKey を登録)
      - ADFS のページからログインして、パスワードを変更する必要があります。
        - 割り当てられた ID とパスワードを入力してログインします。


        - ID を入力: account@domain.com 又はドメイン\アカウントに割り当てられたパスワードと新しいパスワードを入力したら、適用して確定します。




        - 完了です。手動で ADFS のページに戻ってください。

- (ユーザーケース d.3) ユーザーアカウントが AD から無効又は削除されてしまった。
  - ユーザーは ATKey.Pro でログイン(指紋照合による)を行うことは出来ますが、メッセージによる拒否の代わりに「パスワード変更ダイアログ」がポップアップ表示されます。(ただし、メッセージが完全に正しいわけではなく、削除されたアカウントは「パスワードが変更されたようです」等と表示されます)
  - パスワード入力後、エラーメッセージが表示され、ログインが拒否されます。
  - AD からユーザーが無効又は削除された場合、AT.LogOn サーバーのダッシュボードからユーザーを削除して、ATKey.Pro を返却(新しいユーザー用にリセットする為)してもらってください。これにより、そのユーザーはオンラインとオフラインの両方でログインすることができなくなります。

- (ユーザーケース d.4)ユーザーAD のパスワードが変更されたか、有効期限が切れた。
  - ユーザーは ATKey.Oro でログインする為に指紋を照合すると新しいパスワードを入力要求するダイアログがポップアップ表示されます。

- (ユーザーケース d.5) 一つの ATKey に複数のアカウント
  - 1 つの ATKey.Pro が複数のアカウントに登録されている場合、ATKey.Pro は複数の「FIDO クレデンシャル」を保存していることになります。FIDO 仕様に沿ったパスワードレスログインなので、ログインには「最新の」クレデンシャルが使用されることになります。
    例:
    - ATKey.Pro#1 が user#A1, user#B2, user#C3 に登録され、最終ログインが user#C3 の場合、ATKey.Pro#1 でログインすると、ユーザー#C3 アカウントにログインすることになります。
    - ユーザーは Chrome ブラウザ又は AuthenTrend の管理ツール”SecurityKeyVault”から特定の指紋情報を削除することが出来ます。例えば、User#B2 と User#C3 を削除して User#A1 のみ残す等。
    - 又はユーザーは管理者に依頼をして AT.LogOn サーバーのダッシュボードから ATKey.Pro#1 の User#B2 のアカウントを削除する事も出来ます。

- (ユーザーケース d.6) 複数キー vs 一つのアカウント
  - ユーザーは自分のアカウントに複数の ATKey.Pro が登録されている場合、登録された ATKey.Pro であれば、どれでも自分のアカウントにログインすることができます。
  - しかし、ADFS のページで新しい ATKey.Pro を登録する場合、登録済みの ATKey.Pro で認証を行ってから新しい ATKey.Pro を登録する必要があります。

- (ユーザーケース d.7) #222 AD ログイン失敗回数
  - AD ポリシーがユーザーログインのパスワード失敗を「N」回許可する場合、AT.LogOn では、実際のカウントはパスワード変更または期限切れで「N-1」になります。これは、AT.LogOn が最初に（ATKey.Pro で）ログインして間違ったパスワードを見つける必要があり、ユーザーはパスワードを入力しなかったのでこの失敗に気づかない場合があります。

        - 例えば、account#A の失敗カウンターの最大値は 3 とした場合、AT.LogOn でユーザーパスワードに 2 回失敗すると、ATKey.Pro ログイン時に 1 回目の失敗が起こったとともになっている為、ロックされます。

- (ユーザーケース d.8) #219 セーフモード
    - ユーザーが WindowsPC をセーフモードで起動した場合、セーフモードでは Windows の通常通り ID /Password を入力してログインします。

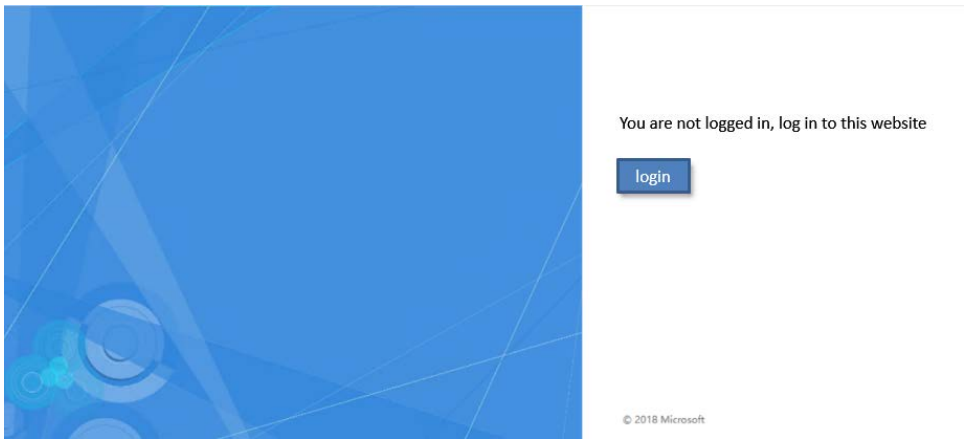
# 3. 従業員の Windows ログイン

## a) 指紋の登録

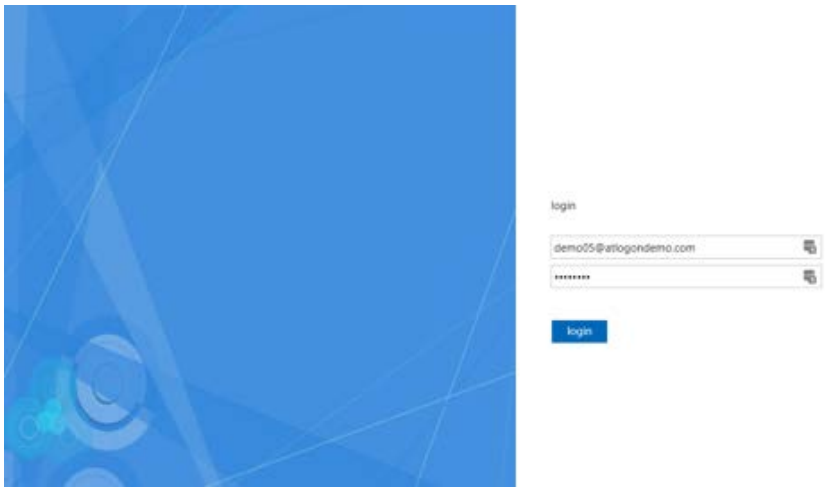
a. ATKey.Pro に指紋の登録する方法以下いくつかございます。
   i. Windows の設定 (Windows 10 build 1903 and later versions)
   ii. Windows 以外の OS からは Chrome ブラウザ (Security and privacy)
   iii. スタンドアローン: https://youtu.be/NnNqXbrf7vA
b. 正しい指紋登録方法については右記リンクの動画を参考に行ってください。: https://youtu.be/bCLPMtZJhkM
c. .弊社では 1 つの ATKeyPro に最低でも 2 本の異なる指を登録することを推奨します。

## b) ATKe.Pro を AD アカウントに登録する

a. Chrome ブラウザを開き、割り当てられた ADFS の URL を入力します
   例: https://fs.domainname.com/adfs/ls/idpinitiatedsignon



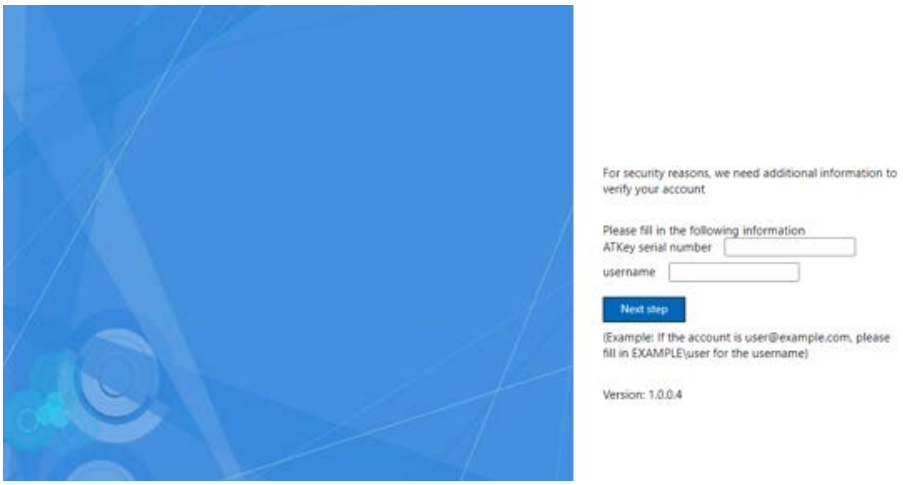

b. ユーザーの AD の AD/Password でサインインします。



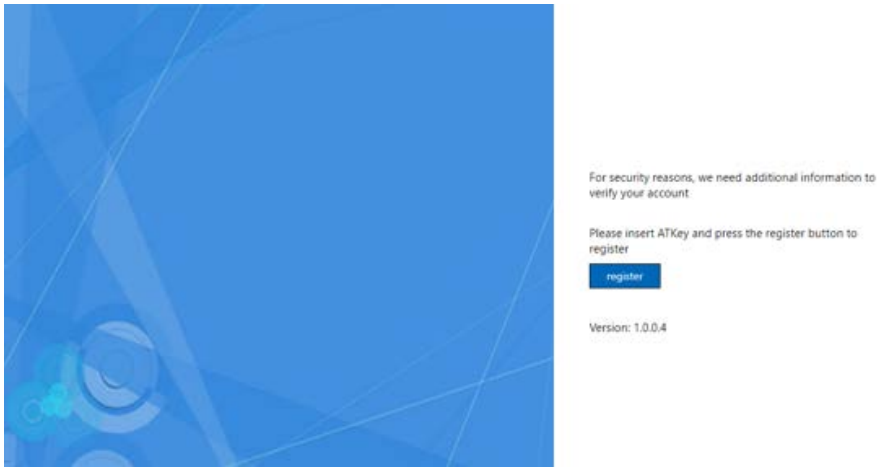

c. FIDO の認証機を初めて登録する場合 - ATKey.Pro の Keycode と User name を入力
   i. Keycode - “ATKey.Pro”の Keycode の場所は下記の写真をご覧ください。key.Keycode は 8 桁のユニークコードで Atkey.Pro の本体表面に印字され、本体にも格納されています。

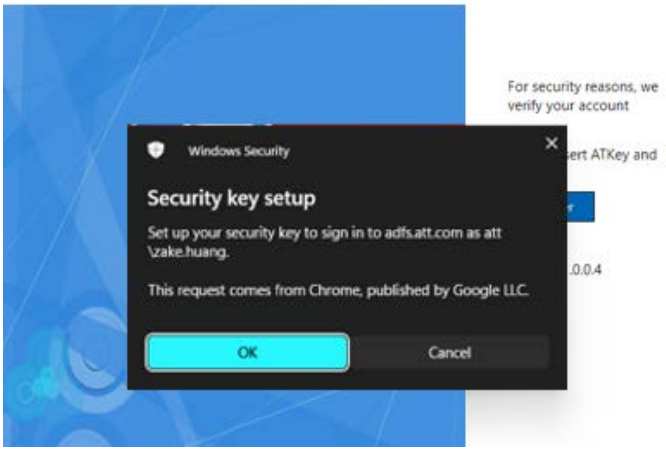
ii. ご注意 – “username”(ユーザーネーム)は絶対に間違いの無いよう入力してください。変更ができません。

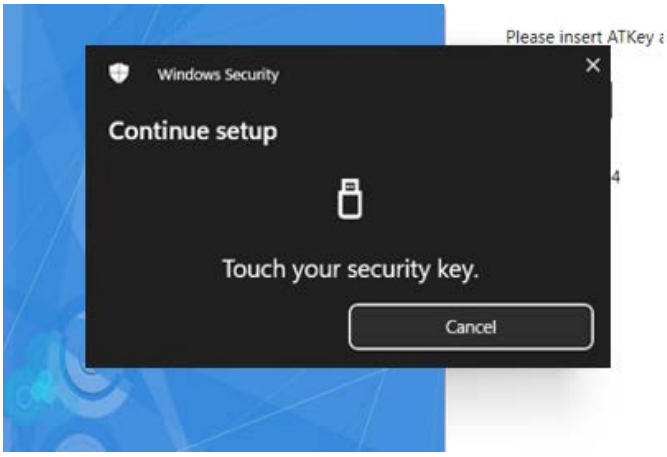
1. フォーマット：domainname¥username




d. “Register”をクリックし ATKey.Pro に指紋の照合を行えば完了です。

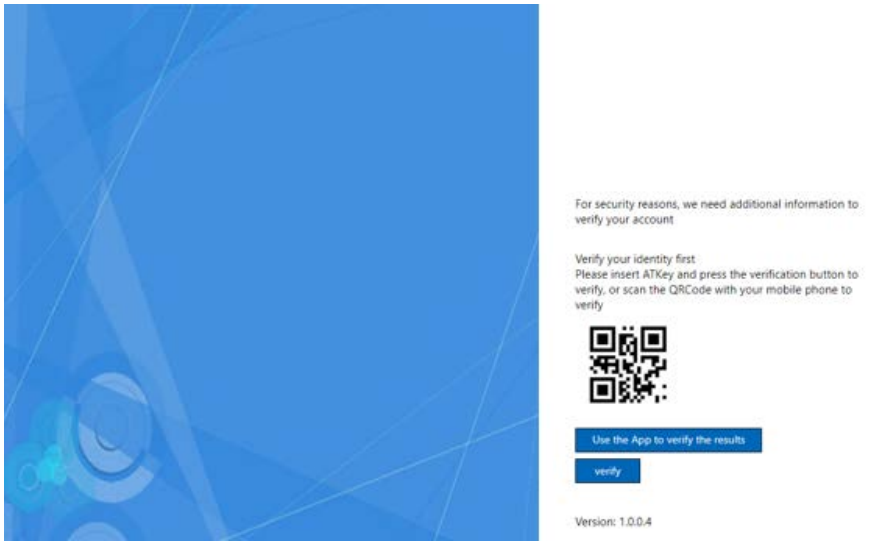


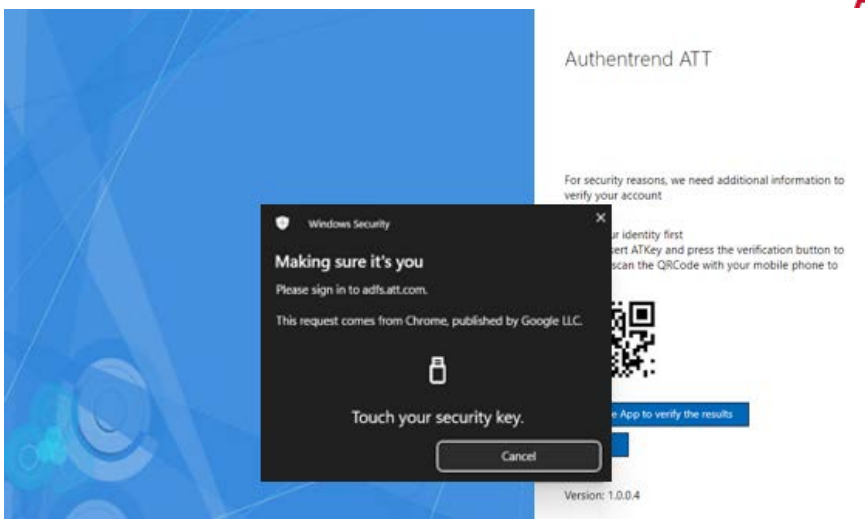


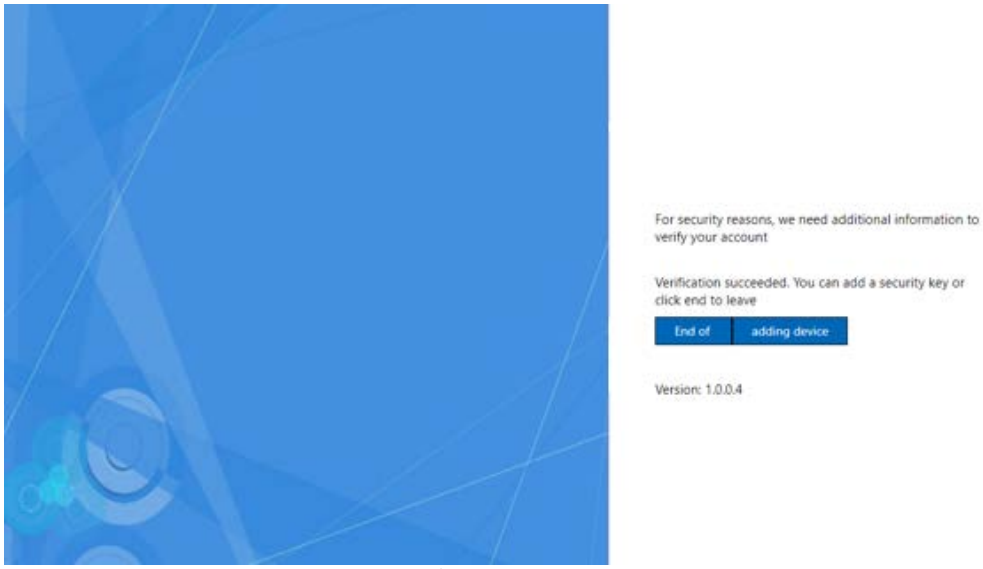




e. その後、管理者はダッシュボードからユーザーの記録を確認することができます。(ユーザー名と登録されたタイムスタンプ)

f. もしユーザーのアカウントに他の ATKey.Pro が登録されていた場合、セキュリティの仕様上、登録された ATKey.Pro と登録された指紋を照合してから”Verify”ボタンをクリックします。






“Adding device”をクリックし, 上に表示されている“Add new key”に戻る – keycode, username, register

g. 最初に登録した ATKey.Pro を紛失した場合、管理者は Dashboard の Registered Users からその ATKey.Pro を削除し、新しい ATKey.Pro を登録することができます。

## c) 初回ログインと 2 回目以降のログイン

a. 登録された ATKey.Pro で指紋認証による Windows ログイン
   i. 初回： ユーザーは AD パスワードを入力して確認する必要があります。–AD が必要となりますので必ずドメイン内でオンラインで行ってください。
   ii. 2 回目以降: ユーザーは指紋認証するだけでログインできます。
   iii. もし AD パスワードが変更された場合(手動又は定期的に)、指紋認証後するとシステムから変更されたパスワードを入力して再度ログインするよう要求します。以降は指紋認証でログインできます。

## d) 内部ドメインと外部ドメイン

a. 内部ドメイン(企業内または VPN 経由)

i. オンラインとオフライン両方に対して ATKey.Pro でログインすることができます。

b. 外部ドメイン

i. オンラインとオフライン両方に対して ATKey.Pro でログインすることができます。

c. ご注意 – ATKey.Pro を AD アカウントに登録し、初回ログイン時には、AD 権限が必要なため、オンラインかつドメイン内にあることが必要です。

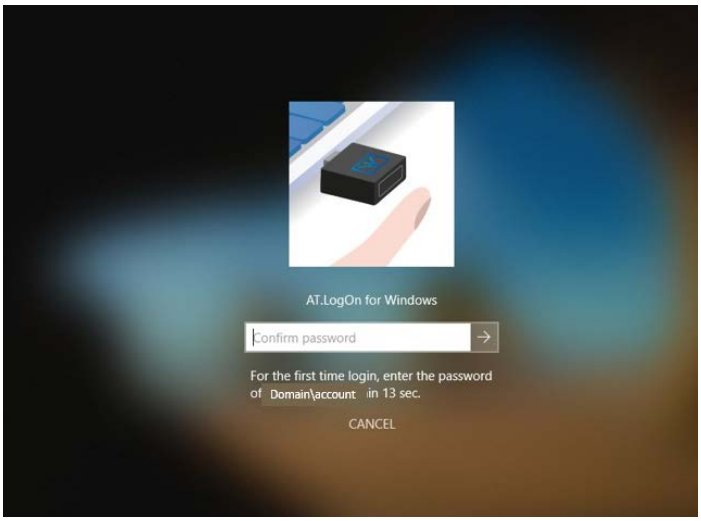
## e) オンライン/オフライン

a. PC がオンラインでもオフラインでも、ATKey.Pro で PC にログインできます。これは、FIDO ハードウェア認証の利点でもあります。

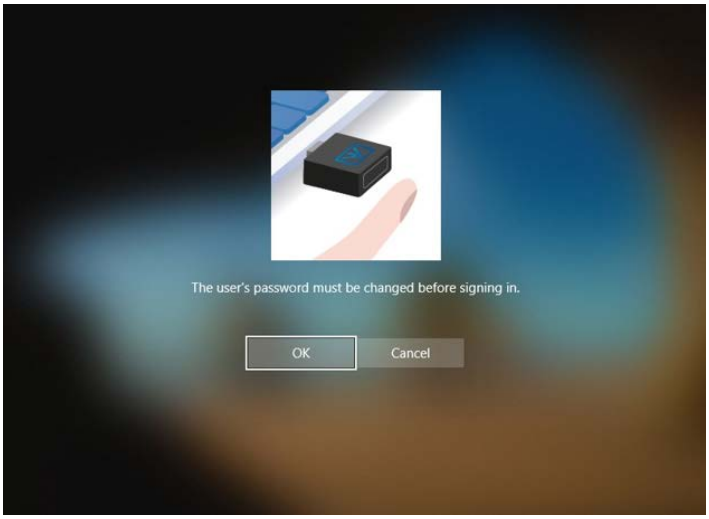
## f) ATKey のユーザーケース(従業員向け)

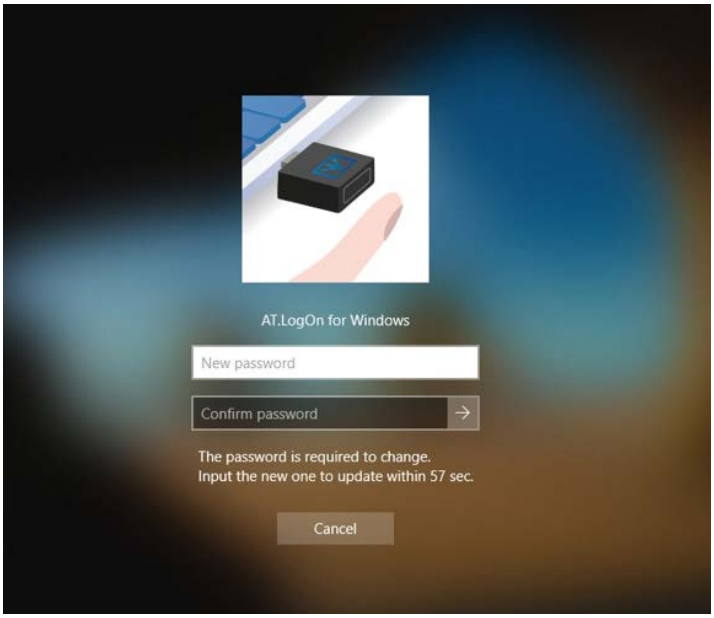
- (ユーザーケース f.1) AD パスワード変更
  - Windows のログオン画面で ATKey.Pro が認証されるとログイン確認の為パスワード入力が求められます。

- (ユーザーケース f.2) AD パスワード期限切れ(#226)
  - Windows のログオン画面で ATKey.Pro が認証されると、下記が要求されます:
    - 期限切れとなったパスワードの確認



- その後新しいパスワードを要求されますので入力、確認してログインします。




- (ユーザーケース f.3) ATKey を忘れてしまった場合
  - ユーザーは管理者の指示に従い下記の方法でログイン出来ます:
    - 定義された"Hotkey"(ホットキー)を押す(AT.LogOn Server ダッシュボードで管理者が定義した 4 つのキーを同時押しする)
    - "Recovery code"(リカバリコード)を入力 – AT.LogOn Server ダッシュボードで管理者が定義したものになります。
    - ユーザーは ID とパスワードでログイン出来ますが、入力形式は下記となります。
      - Domainname¥accountID+password
  - 管理者は AT.LogOn Server のダッシュボードからいつでも"Hot-Key"(ホットキー)と"Recovery Code"(リカバリーコード)を変更できます。一部のユーザーが前回り用したホットキーとコードを必要とする場合に備えて、すべての記録を保持できます（オンラインで同期することはありません）

- (ユーザーケース f.4) ATKey を紛失した場合

- 新しい ATKey.Pro を登録する
  - Admin は AT.LogOn Server ダッシュボードからユーザーの古い ATKey.Pro を削除することができます。
  - その後ユーザーは新しい ATKey.Pro を ADFS ページから登録することができます。
- ユーザーが社外にいる時や新しい ATKey.Pro の入手が困難な場合
  - ユーザーケース f.3 と同じように、定義された”Hotkey”(ホットキー)を押す(AT.LogOn Server ダッシュボードで管理者が定義した 4 つのキーを同時押しする)
  - “Recovery code”(リカバリコード)を入力 – AT.LogOn Server ダッシュボードで管理者が定義したものになります。
  - ユーザーは ID とパスワードでログイン出来ますが、入力形式は下記となります。
    - Domainname¥accountID+password
- 管理者は AT.LogOn Server のダッシュボードからいつでも”Hot-Key”(ホットキー)と”Recovery Code”(リカバリーコード)を変更できます。一部のユーザーが前回り用したホットキーとコードを必要とする場合に備えて、すべての記録を保持できます（オンラインで同期することはありません）

- (ユーザーケース f.5) どの ATKey.Pro が自分のものかわからなくなってしまった場合
  - ATKey.Pro の外観は全て同じのため、見分けることは難しいですが、ユーザーは ATKey.Pro 本体に印字されている”Keycode”(キーコード)から見分けることができます。

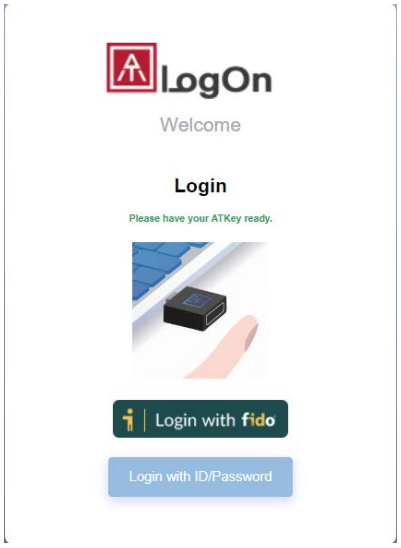
  - 又は管理者が AT.LogOn Server のダッシュボードから”KeyCode”(キーコード)を検索して、誰がこのキーを登録しているか確認することができます。

- (ユーザーケース f.6) 共有 PC 又はワークステーション
- ユーザーはどの共有 PC でもアカウントに登録されている ATKey.Pro からログインすることが出来ますが、初回ログインと同じようにパスワードの入力と確認が必要となります。

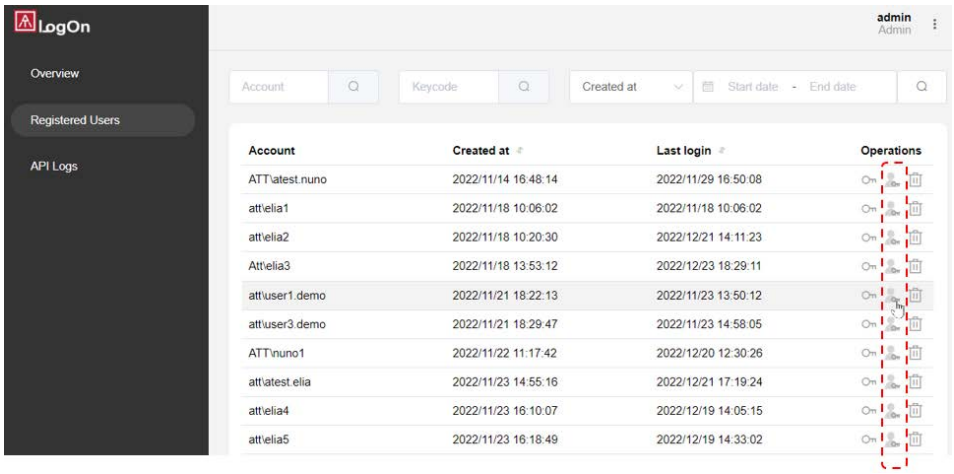
# 4. AT.LogOn Server 管理

## a) admin の割り当て

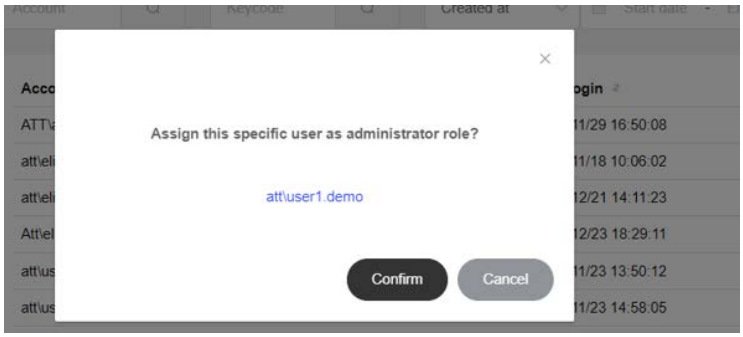
- Admin は登録された ATKey.Pro 又は割り当てられた ID/Password からログイン出来ます。(ex. https://adfs01.domainname.com/dashboard/ )



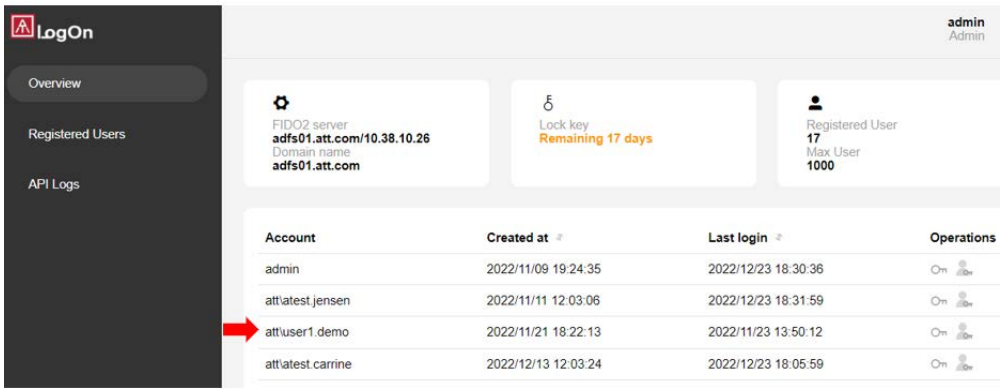

- “Registered Users”(登録されたユーザー)から
  - Admin「登録されたユーザー」を選択して管理者権限を付与することが出来ます
    - ユーザーを指定して下記の“admin アイコン”をクリックしてください。




    - ユーザーを確認
    - すると”Overview”画面に管理者の一人として表示され、特定のユーザーがログインできるようになります。



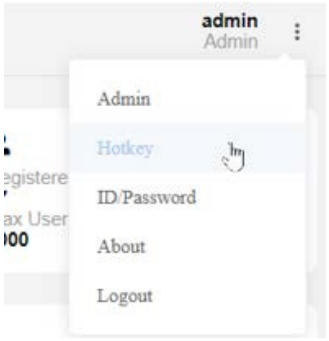

- ATKey.Pro で AT.LogOn Server のダッシュボードを使用する。



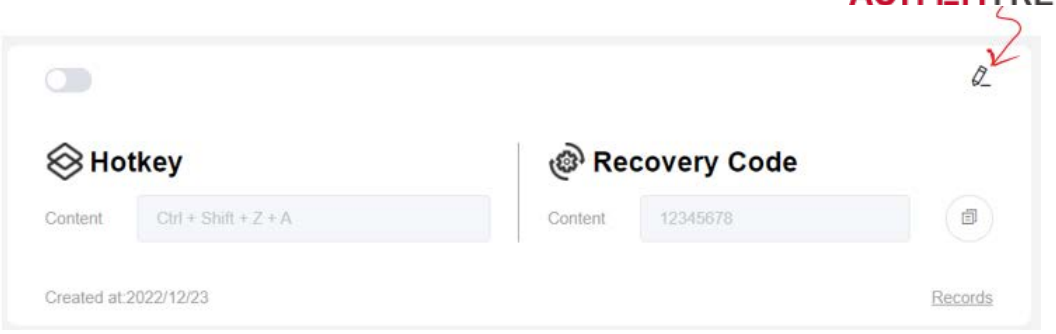

- ログインした管理者は、他の管理者を追加・削除することができます。

## b) “Hotkey”(ホットキー)と”Recovery code”(リカバリコード)

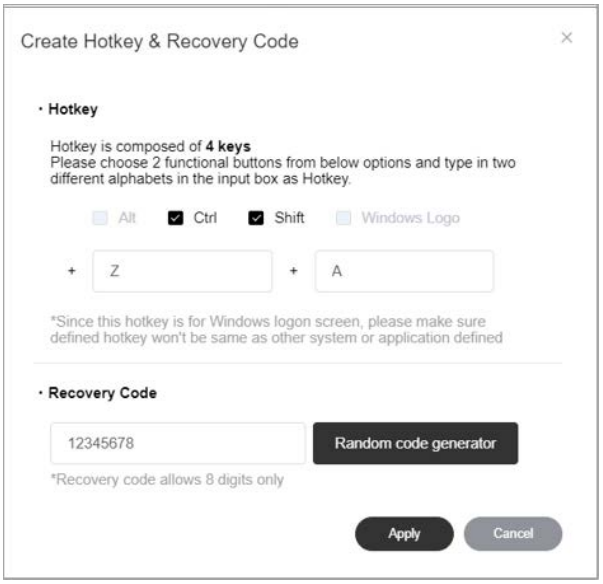
- “Hotkey”(ホットキー)と“Recovery Code”(リカバリコード)の設定
  - 緊急時に必要な場合（キーが手元にない、キーを紛失した、キーが破損した、社外にいる…等）に AD ID/Password でログインするためのものです。
    - リストボックスから入ります



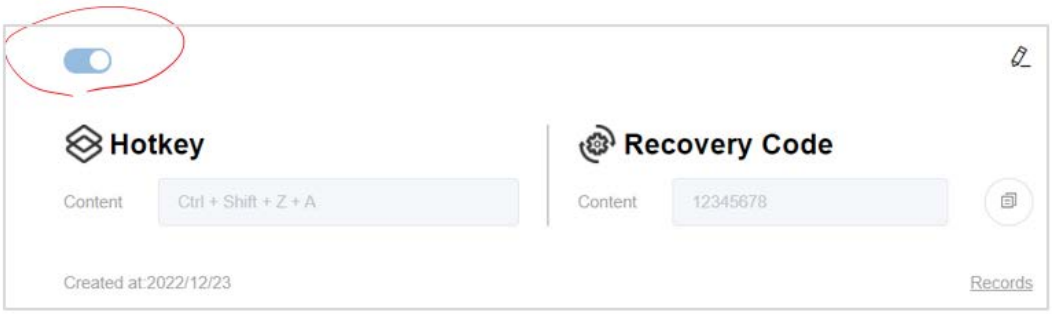

- “edit”(ペン型アイコン)をクリックして”Hotkey”と”Recovery”を設定を開始します。




- ホットキーのルールに従って設定し、リカバリーコードを入力するか、ランダムで生成します。



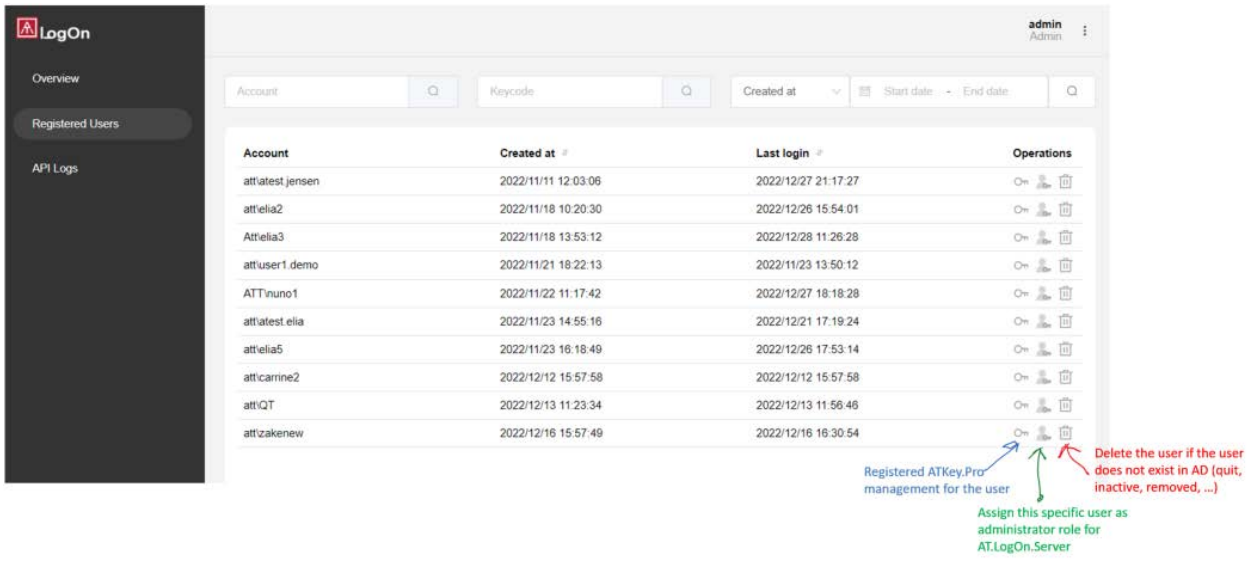

- 必ず“Apply”ボタンを押して機能を有効にしてください。



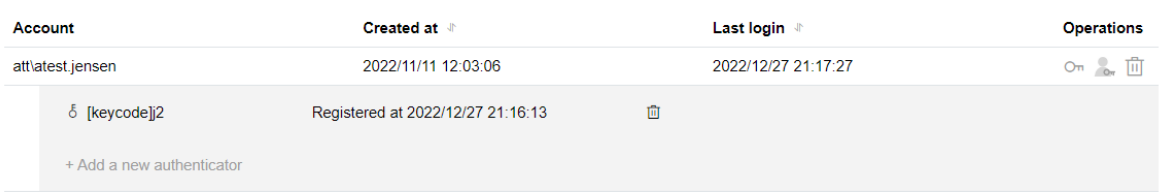

  - Windows のログイン画面で、オンラインかつドメインに参加している場合、クライアントは”Hotkey”(ホットキー)と”Recovery Code(リカバリーコード)を同期し、ローカルに暗号化されます。
  - より良いセキュリティと管理のために、弊社では”Hotkey”(ホットキー)と”Recovery Code”(回復コード)を頻繁に変更すること、またはユーザが一度でも利用した場合に変更することをお勧めします。
  - PC が過去に利用した”HotKey”(ホットキー)と”Recovery Code”(リカバリーコード)を必要とする場合（常にオフラインまたは ドメイン外）、ログインするためのホットキーとリカバリーコードを確認するために”Records”(記録) をチェックすることができます。


## c) 登録ユーザーの管理

- ダッシュボードにログインして”Registered Users”(登録ユーザー)を選択すると、ユーザーの一覧が最終ログイン時間順に表示されます。
  - “Created time”(作成時間): ADFS のウェブページ (https://fs.domainname.com/adfs/ls/idpinitiatedsignon)から登録された ATKey.Pro; ソートボタンをクリックして、最新の「作成ユーザー」または最も古い「作成ユーザー」の並び替えができるようになりました。
  - “Last login time” (最終ログイン時間)：そのアカウントに最後にログインした時間（PC ログイン）、横にあるクリック式のソートボタンで、最新の「ログインユーザー」または最も古い「ログインユーザー」でソートすることができます。




  - 特定ユーザーから登録された ATKey.Pro を確認または削除します。
    - Click “key”(鍵)アイコンをクリックするとドロップダウンリストが表示されます

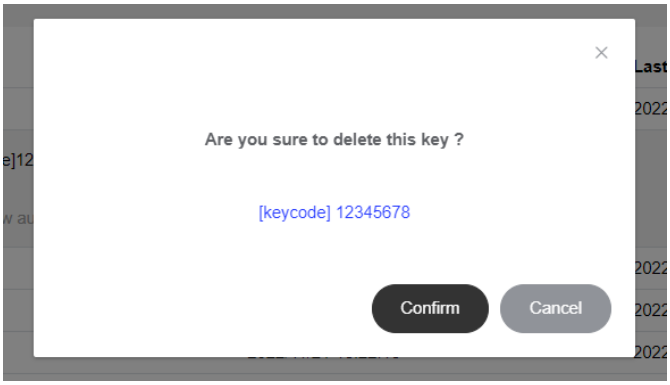


- ADFS ページで ATKey.Pro を登録した時に Keycode を入力ミスした場合に備えて“[keycode]”エリアをダブルクリックすると、キーコードを編集するためのテキストボックスが表示されます。



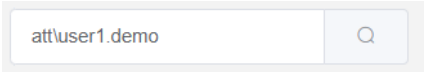
<= 各 ATKey.Pro に刻印されているキーコードはこちらです。

- ユーザーが複数 ATKey を登録した場合、登録された時間がここにリスト表示されます。
- Admin はキーを無効化するため AT.LogOn server から登録された ATKey.Pro を削除できます。
  - ユーザーが ATKey を紛失した場合
  - ユーザーが Atkey をリセットしたり、壊したりして、別の Atkey に交換した場合
- "+ Add a new authenticator”をクリックすると、ADFS web ページに移動しユーザーがログインと新しい ATKey の登録ができるようになります。

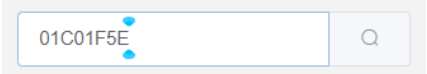



- [Keycode]エリアをダブルクリックすると、正しい Keycode を編集するためのテキストボックスが表示されます（ADFS ウェブページで ATKey.Pro を登録したときに Keycode を入力ミス/タイプミスした場合に備えています）。

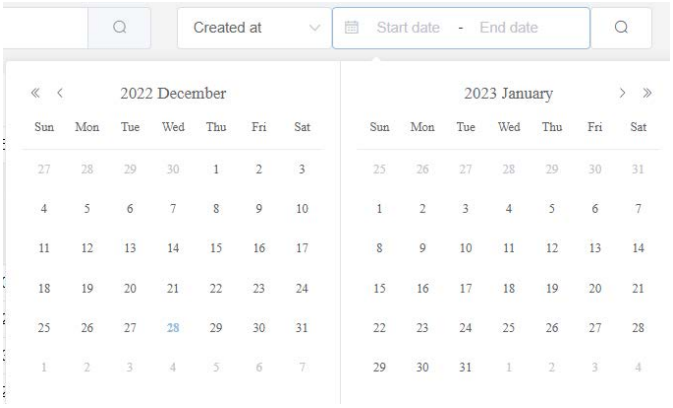
- AT.LogOn.Server の管理者の役割を 特定のユーザーに割り当てます。
- AT.LogOn.Server の FIDO データベースから特定のユーザーを削除します。
- 検索
  - User name (ユーザー名): フォーマットは ADFSWeb ページで ATKey.Pro の登録を行なう時に入力するフォーマットと同じで、“domainname¥accoutname”となります。




  - Keycode (キーコード): 万が一紛失した ATKey.Pro が見つかった場合に、持ち主がわからない時は、管理者はその ATKey.Pro の Keycode を検索して所有者を探すことが出来ます。

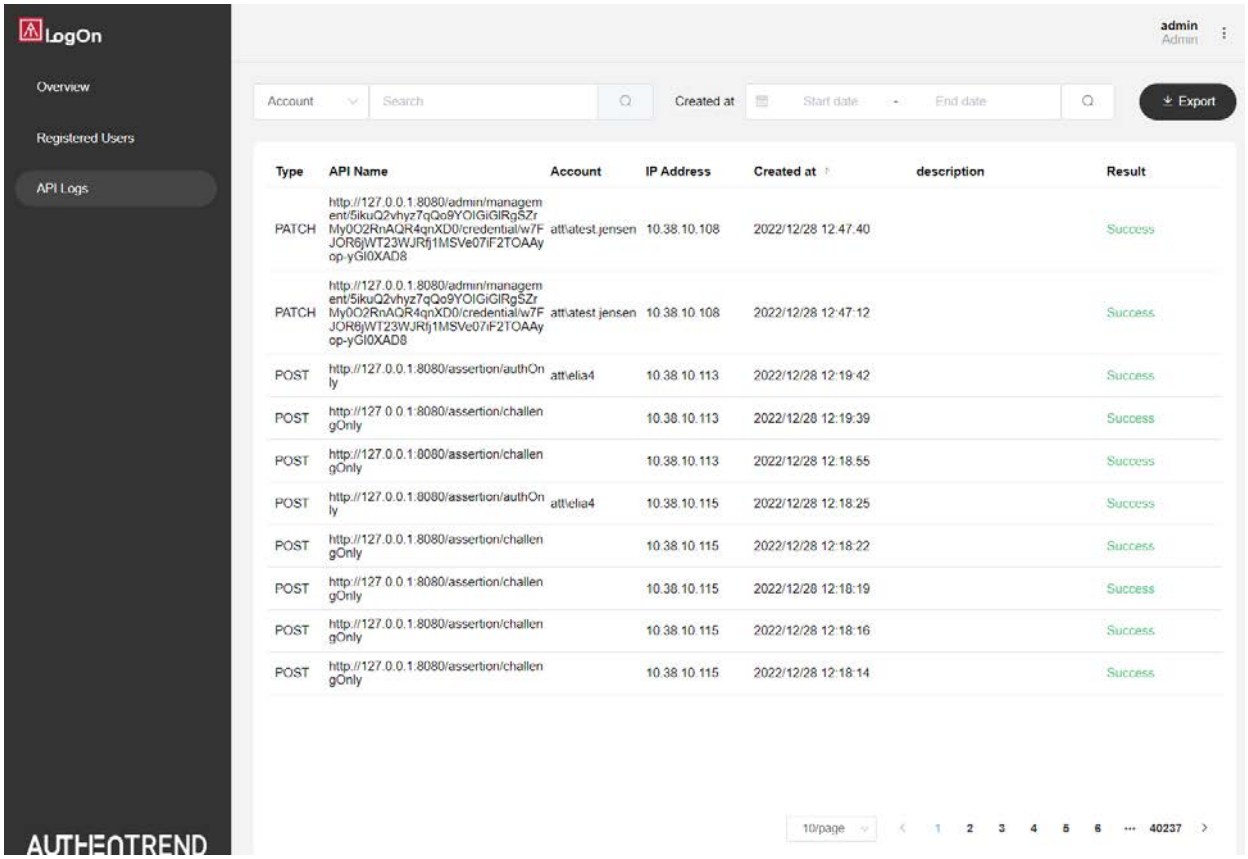



  - 日付と時間: 管理者はユーザーのログイン記録を、期間を特定して検索することができます。



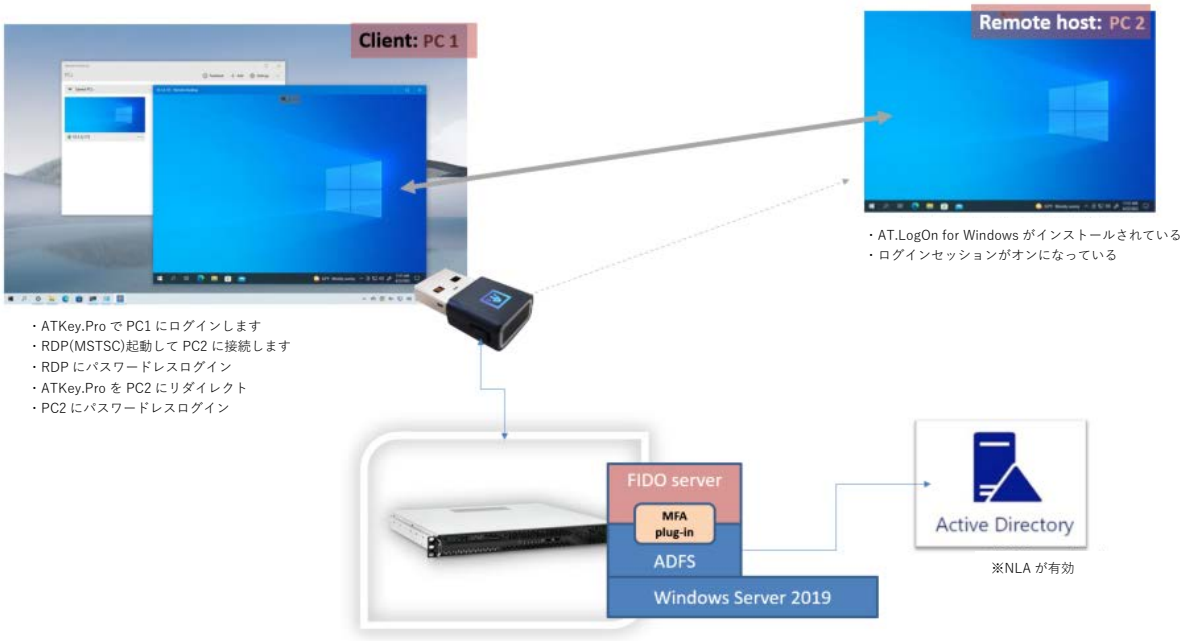

## d) API ログ

- 全ての API ログを記録しています。 (every action to AT.LogOn.Server への全ての行動)




- Debug のログ
  - 必要に応じて範囲を限定しログをファイルにエクスポートして Debug 用に送り返すことが出来ます。
- ユーザーの行動
  - 特定のユーザーの全ての行動を確認します。
- API のログは容量が重くならないように最大で１２ヶ月保存されます。

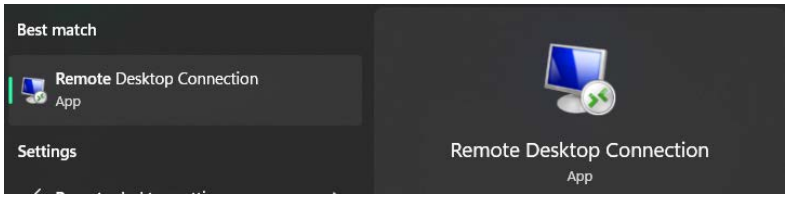
# 5. RDP – リモートデスクトップ




*デモ動画: https://www.youtube.com/watch?v=Jrj7ec-BD1M*

## a) ホスト PC、リモート PC、AD の設定基準

- リモートデスクトップ接続のサポート (mstsc)




AT.LogOn for Windows がインストールされているか
AD クライアント参加

- 各役割の基準は下記の通りとなります。


クライアント PC と ATKey.Pro 側

**AD 参加済みのドメインアカウントでなければならないか？**

参加済み、非参加 AD アカウントどちらも OK です

**AT.LogOn for Windows のインストールは必要か？**

参加済み AD クライアントにはインストール。
非参加 AD クライアントにはインストールなし

**管理者権限のアカウントでなければならないか？**

必須です。

**管理者として実行(リモートデスクトップクライアント-mstsc)しなけ r ばならないか？**

管理者として実行する(推奨)
又は直接実行どちらも可能です。

**その他**

ATKey.Pro は、リモートホストアカウントに登録する必要があります。


リモートホスト側

**AD 参加済みのドメインアカウントでなければならないか？**

必須です。
(AD に参加していない PC には AT.LogOn はインストールされません)

**AT.LogOn for Windows のインストールは必要か？**

はい(インストール済みです)
初回のログインにはパスワードの入力が必要です。

**AD で RDP が許可されたアカウントが必要か？**

必須です。
AD admin アカウントでも OK です。

**その他**

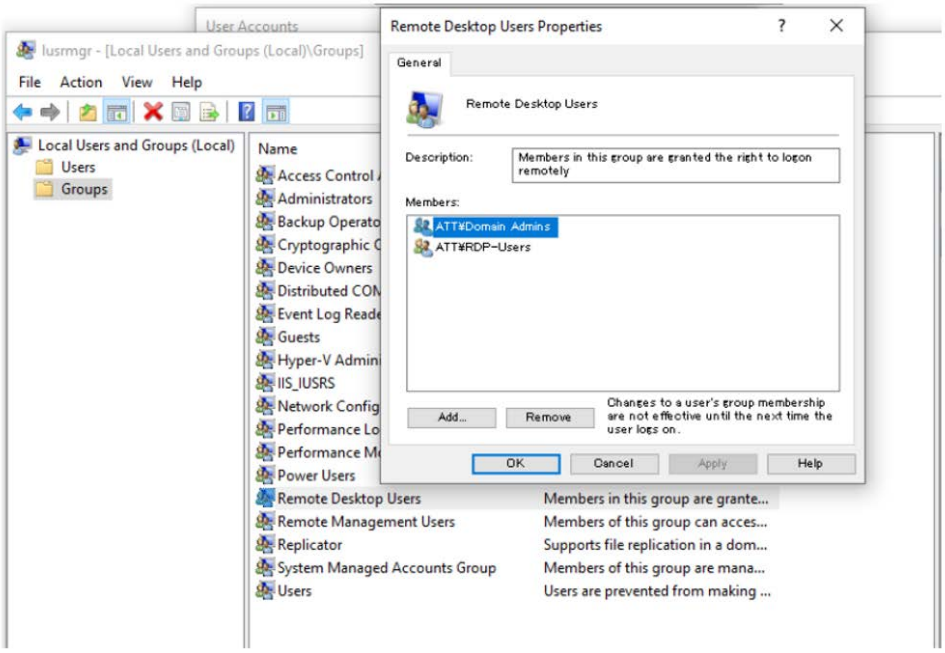
**ATKey.Pro をこのリモートホストアカウントに登録し、ATKey.Pro をリモートホストにリダイレクトする必要があります。**
**しかし、リモート PC は「ログインセッション」の準備が必要なので、リモート PC がクールブートやウォームブートの後であれば「ホットキー＋リカバリコード」→「ID/パスワード」でログインできますが、その後はログインセッションが準備されているので、ATKey.Pro のリダイレクトはログインセッションが整っているため、動作が可能となります。**


AD 側

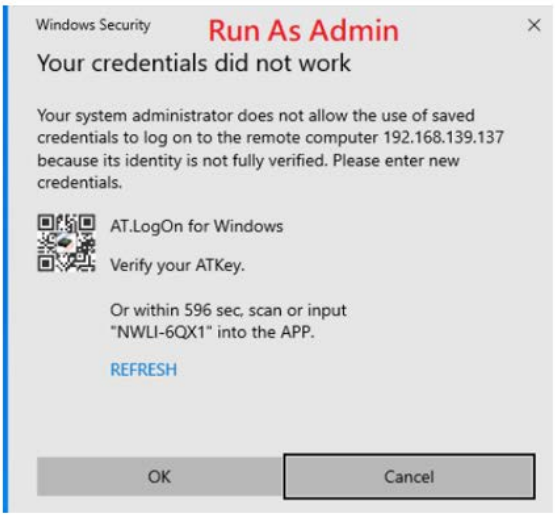
**NLA が AD 有効にする必要があるか？**

必須です。

- アカウントには AD からログオンリモート権限が割り当てられている必要があります。




- リモートデスクトップ接続(mstsc)
  管理者として実行(ATKey.Pro による認証)と非管理者として実行(パスワードによる認証)の比較




管理者として実行(ATKey.Pro による認証)


非管理者として実行(パスワードによる認証)

## b) RDP のユーザーケース

- (ユーザーケース b.1) #248 リダイレクトする ATKey.Pro はリモートホストと同じユーザーアカウントに登録されている必要があります。
  - アカウント#A がクライアント、アカウント#B がリモートホスト
  - ATKey.Pro#2 がアカウント#B に登録されている。

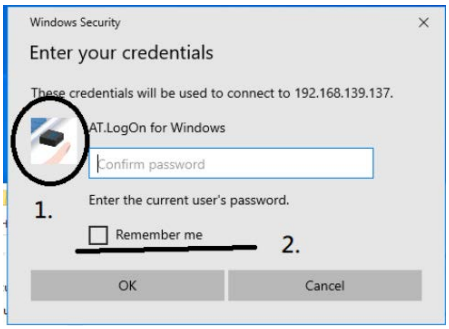
- ATKey.Pro#2 はクライアントホスト側に有り、リモートホストのアカウント#B にリダイレクトされます。
- ATKey.Pro#1 がアカウント#A に登録されている場合にリモートホストのアカウント#B にリダイレクトすると、フリーズしたり、応答しなくなったります。

- (ユーザーケース b.2) ATKey.Pro でリモート PC にリダイレクト（#258）して、リモートログインやリモート Web サービスを実現出来ます。
  - ATKey.Pro を RDP で使用する目的としては主に 2 種類あります。
    - ATKey.Pro でリモート PC にパスワードレスログインする。
      - こちらは問題ないです。ログインするためにリダイレクトをするだけです。

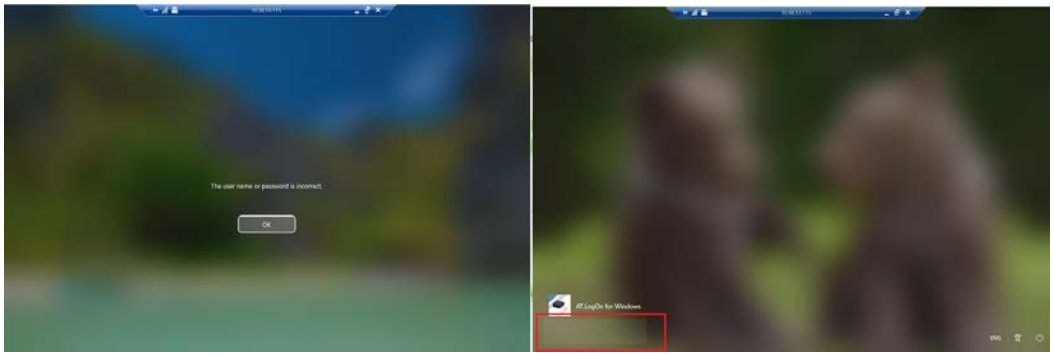

      - ATKey.Pro は”ホスト機”の FIDO Key として属しています。
    - ATKey.Pro を FIDO2 対応のウェブサービスとしてもご利用頂けますし、AT.LogOn.Pass としてもご利用頂けます。
      - ATKey.Pro (FIDO2 認証機として)は WebAUTHN(W3C)を通じてブラウザと連動します。Microsoft では Windows10 バージョン 21H2 及び Windows11 22H2 からリモート PC への FIDO2 認証ツールのリダイレクトが許可されるように変更されました。これ以前のバージョンではリダイレクトは拒否されます。
      - リモート PC で ATKey.Pro を FIDO2 対応のウェブサービスにも下記の条件でご利用いただけます。
        i. Windows 10 21H2 build 又は Windows 11 22H2 build 又はそれ以降のバージョンであること。
        ii. ツールバーから ATKey.Pro リダイレクトのチェックを外すと、ATKey.Pro をブラウザの FIDO2 認証機として WebAUTHN にリダイレクトすることができるようになります。

- (ユーザーケース b.3) ATKey.Pro はリモート PC にリダイレクト(#249)するが、クライト PC の画面がログオン画面になってしまう。
  - ATKey.Pro が既にリモート PC にリダイレクトしている為、クライアント PC に現時点では ATKey でログイン出来ません。
    - Wi-Fi やネットワークから切断するかログアウトしてください。

- (ユーザーケース b.4) パスワードの失敗カウンターは”N-1”(1 回分を減算しています)です。
  - 例えば、AD で割り当てられたアカウントのパスワード失敗カウンターが 3 の場合で、AD のパスワード有効期限が切れた場合で次回以降ログイン時に変更する必要がある場合には 1 回失敗カウントされます。
- ATKey.Pro を使って初回のパスワードでログインするので、1 回失敗したことになり、新しいパスワードの入力を要求されます。その為、2 回パスワードを間違えると AD のカウンターでは 3 回とみなされるので、アカウントがロックされます。
- (ユーザーケース b.5) #247 非管理者として実行している場合、ユーザーはパスワードを入力してログインが出来ますが、チェックボックスの”Remember me”は無効の機能となっております。




- (ユーザーケース b.6) #244　リモートホストにリモート接続する時、”The user name or password is incrrect”「ユーザー名又はパスワードが正しくありません」と表示されることがありますので、”OK”をクリックして続行してください。すると、画面の左下に空白のオプションが表示され、「AT.LogOn for Windows」をクリックするとパスワードレスのログイン画面が表示されます。



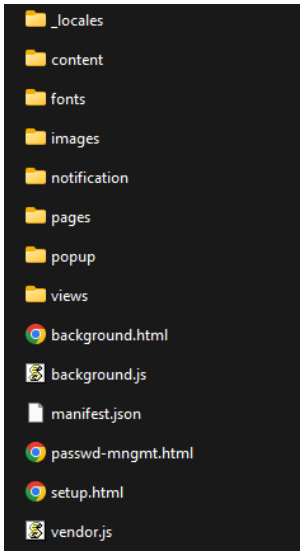
# 6. AT.LogOn.Pass

弊社ではレガシーサービスを含むすべてのイントラネット Web サービスに対応した、Chrome のホワイトリスト制御が可能な指紋認証ハードウェアパスワードマネージャー、**AT.LogOn.Pass** を開発しました。

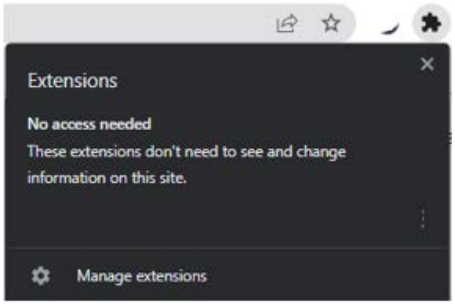
**AT.LogOn.Pass** は、ユーザー名やパスワードなどのユーザー情報を、ウェブブラウザのキャッシュやリモートサーバーやクラウドサーバーに保存するパスワード管理システムとは異なり、ハードウェアベースのパスワード管理ツールです。AT.LogOn.Pass は、認証情報をチップセット内に暗号化して安全に格納し、ユーザーが指紋認証に成功した時のみアクセスできるようにしております。

## a) Chrome extension(Chrome 拡張機能)

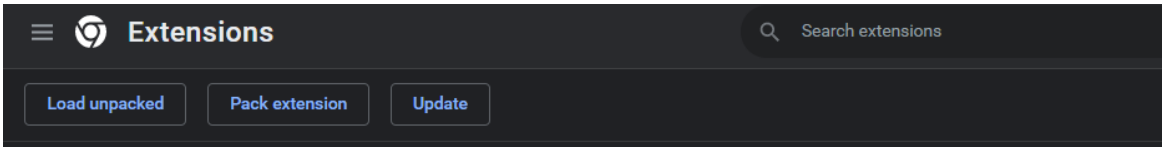
- 以下はインストレーションのソースファイルとなります。

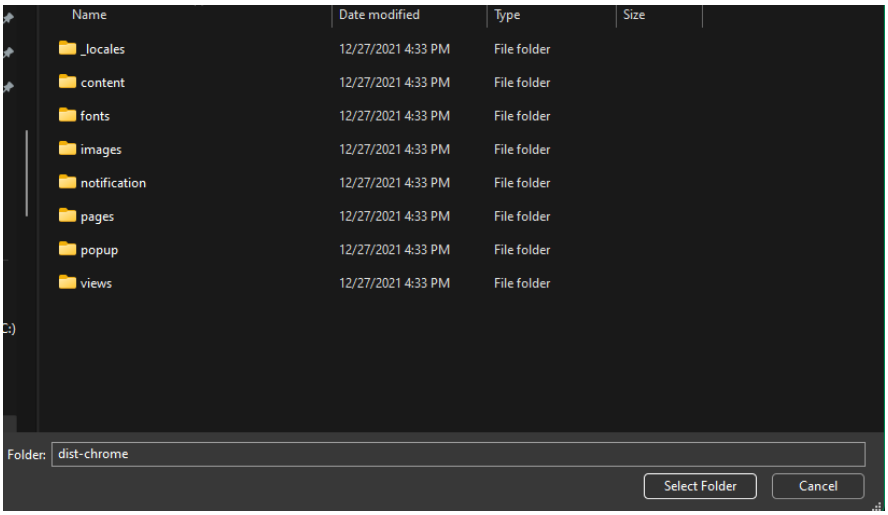



- Chrome の “Extensions”(拡張機能) アイコン => 拡張機能を管理

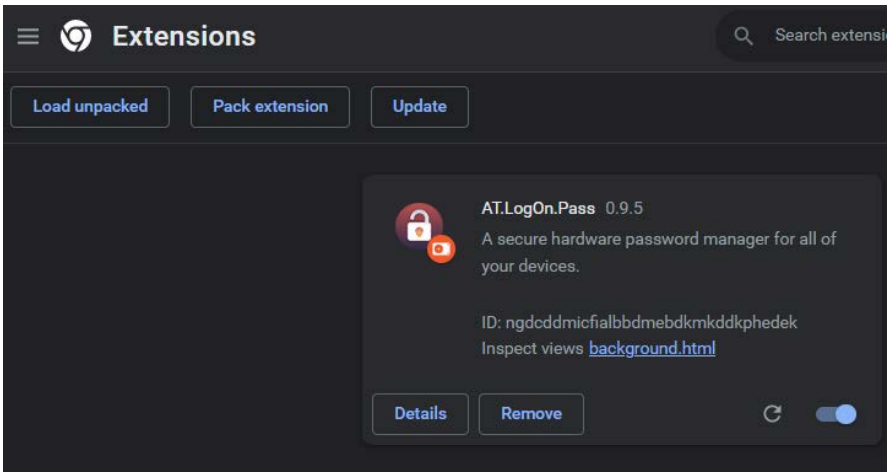



  - “Load unpacked”(パッケージ化されていない拡張機能を読み込む)をクリックして,フォルダを選択します。

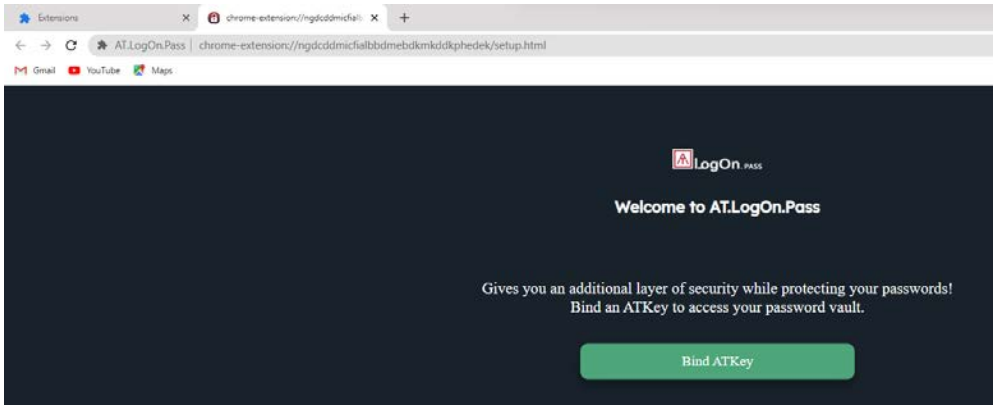




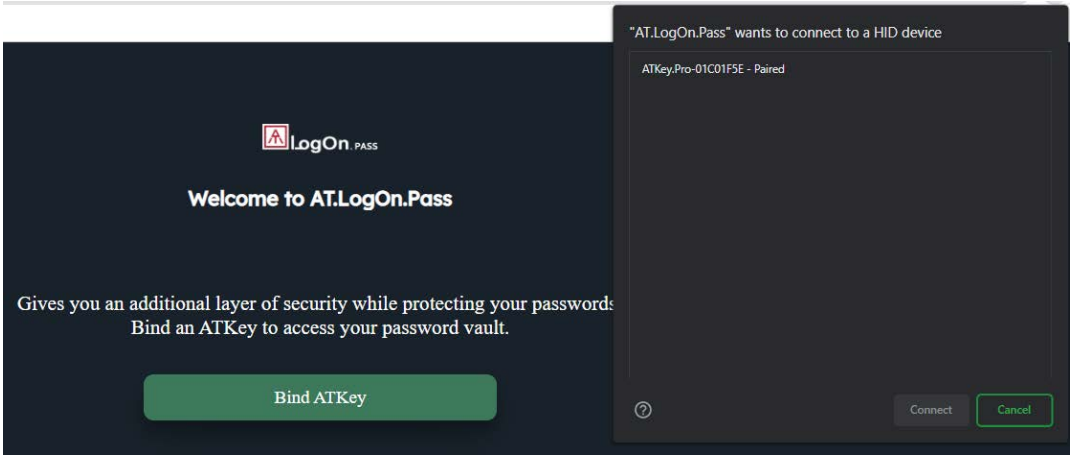

- Then AT.LogOn.Pass のインストールが完了すると、下図のように表示されます。



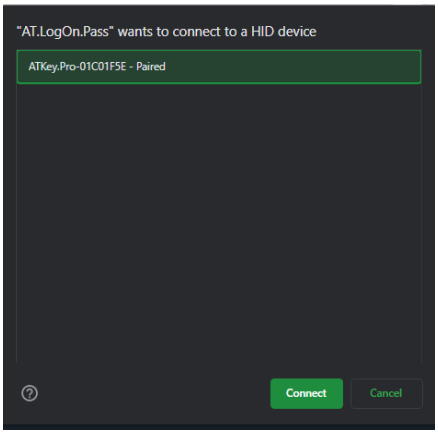

- ATKey.Pro のバインディングを開始します。




- ATKey.Pro を USB ポートに挿入し、"Bind ATKey "をクリックすると、ATKey.Pro とキーコードがリストにポップアップ表示されます。

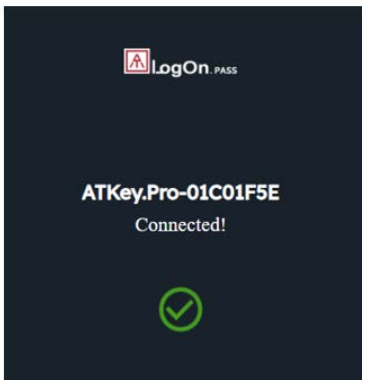



リストの ATKey.Pro を選択して“Connect”をクリックします。

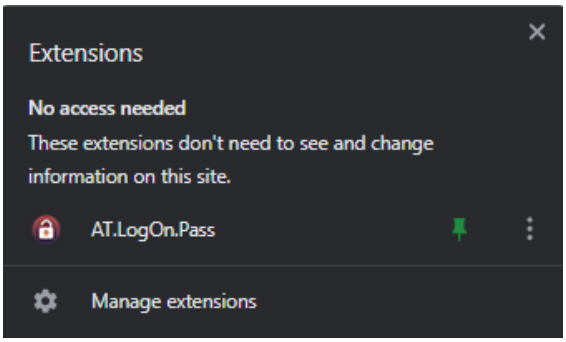



ATKey.Pro の LED が青く点滅したら、指紋を照合してください。


指紋照合が完了すると、バインディング完了です。

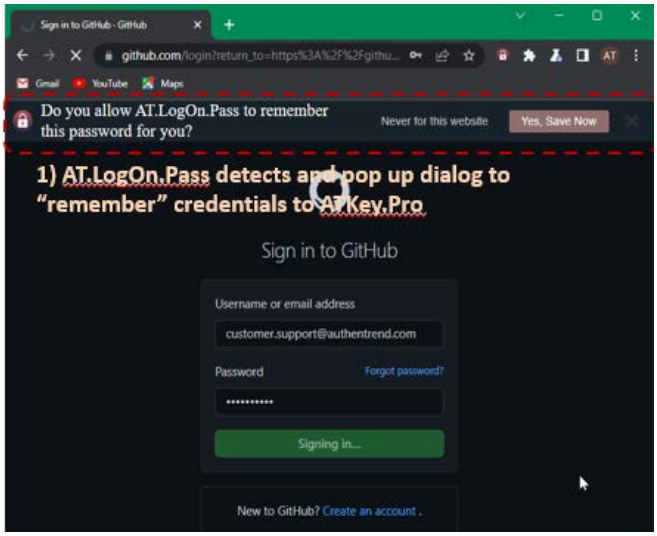




AT.LogOn.Pass がインストールされ、Chrome ブラウザの拡張機能バーにアイコンが表示されます。(常に表示するにはピン留めしてください)



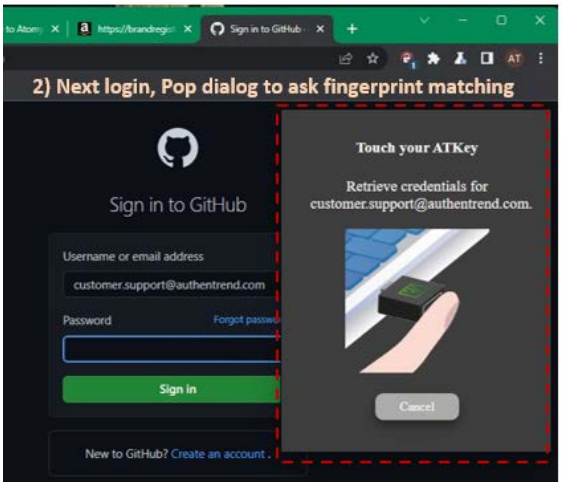

- 暗号化されたクレデンシャルを ATKey.Pro に格納する。
  - Chrome のホワイトリストを有効にすると、これらの URL のみが検出され、ATKey.Pro に保存するか要求されます。

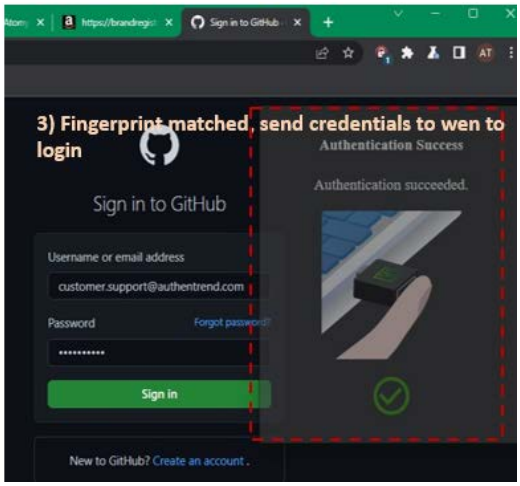
その URL に、ID/パスワードでログインすると、以下のようなポップアップメッセージが表示されます。
“Yes, Store now”をクリックすると、クレデンシャルが暗号化され、ATKey に保存されます。




次回以降、保存した URL にアクセスすると、AT.LogOn.Pass が”Touch your ATKey”ダイアログをポップアップします(この時 ATKey.Pro の LED が青色点滅します)ので、登録された指紋を

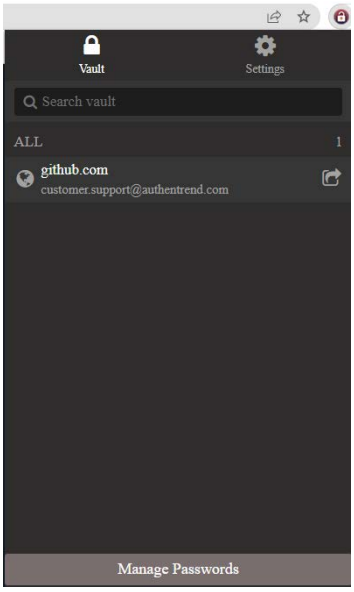
ATKey.Pro に照合すると ATKey.Pro に格納されている ID/Password が自動入力されます。




動画をご参照ください: https://www.youtube.com/watch?v=7g3gjnb5mPA
(Github のアカウントでデモを行なっています)

- AT.LogOn.Pass の管理
  - Chrome ブラウザの AT.LogOn.Pass アイコンをクリックすると、保存された全ての URL が表示されます。

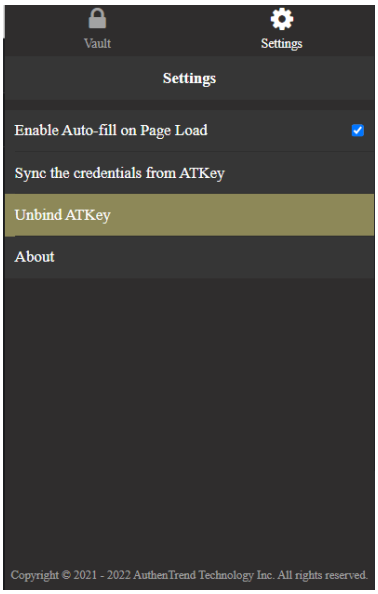



  - リスト表示されている URL をクリックすると Web サイトに移動します。
  - “Manage Passwords”


パスワードの確認・編集ができます（要指紋認証）
保存された URL の削除ができます（要指紋認証）

手動で新規に URL/ID/パスワードを追加することができます

- Settings



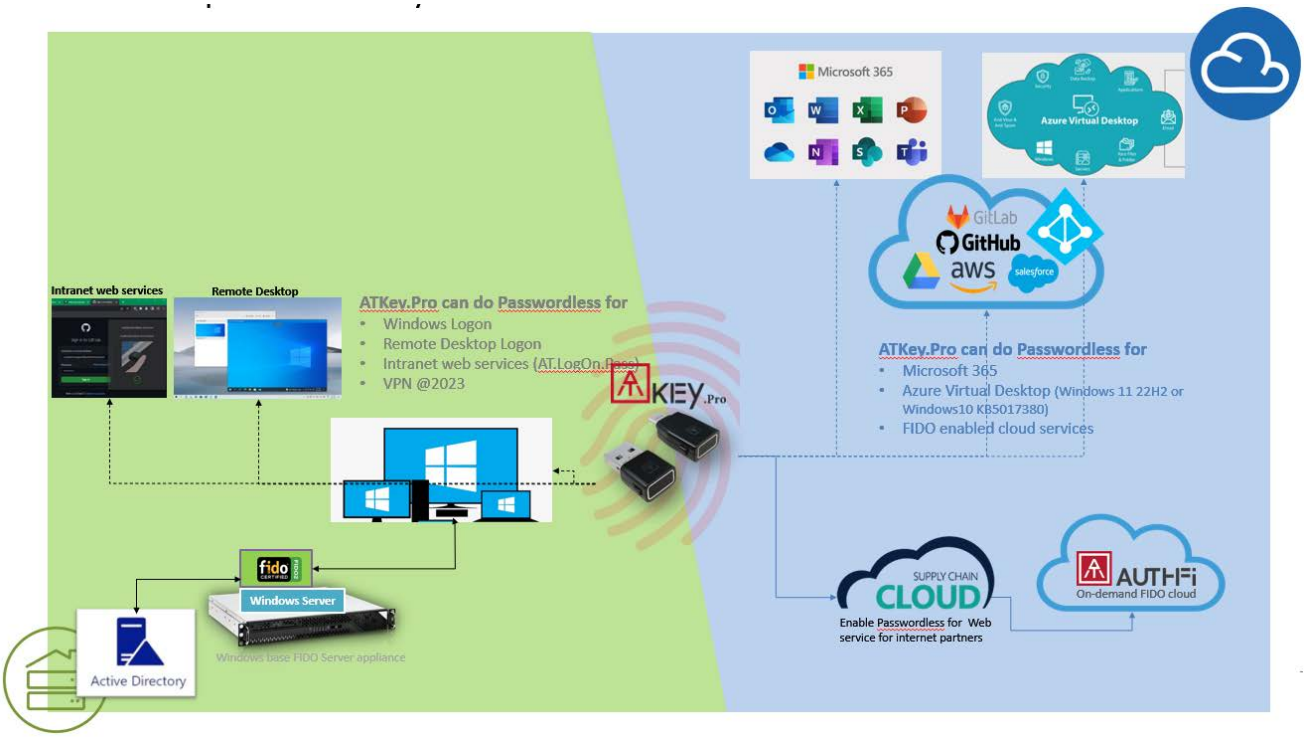

バインドされている ATKey.Pro を紛失した場合や、新しいキーをバインドする場合、バインドされている ATKey を解除してください。
※クレデンシャルのインポートエクスポートには対応しておりません。

## b) Chrome whitelist

- 組織内で許可されたイントラネットやインターネット上の URL に対してのみ、Chrome のホワイトリストを有効にすることをお勧めします。インターネット上のすべての URL に対してこの機能を利用してしまうと、管理者の負担が増え、あまりにも多くの種類の URL と WW があるため、ユーザーが問題に直面した場合、一つ一つ対処することはできません。管理者が許可したイントラネットまたはインターネット URL の動作のみサポートします。

# 7. More from ATKey.Pro

ATKey.Pro は FIDO2 の認定を受けているため、AT.LogOn に限らず、FIDO2/U2F に対応したあらゆる Web サービスと連携することが可能です。




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