NO MORE PASSWORD

ATKey による Azure AD (Entra ID) の
パスワードレス認証 (2023年8月版)

AUTHENTREND

4 ステップ

1. [管理者] Azure AD の設定	a) デフォルトでは、電話番号またはMicrosoft Authenticatorアプリを登録してから、FIDOキーを登録するよう求められます。 b) FIDOキーのみ登録したい場合は、「一時的なアクセスパス」(Temporary Access Pass)を設定してから、FIDOキーを有効にしてください。
2. [ユーザー] ATKeyで指紋を利用	a) 標準的なFIDOのログイン方法に従う場合： Windowsの“設定”から指紋認証＋PINコードをATKeyに登録します。 b) または、PINコードは登録せずに指紋認証のみ（弊社特許技術-スタンドアロン登録）でログインしたい場合。
3. [ユーザー] ATKeyをAzure ADアカウントに登録する	a) デフォルトでは、電話番号またはMicrosoft Authenticatorアプリを登録してから、FIDOキーを登録するよう求められます。 b) FIDOキーのみ登録したい場合は、「一時的なアクセスパス」(Temporary Access Pass)を設定してから、FIDOキーを有効にしてください。
4. [ユーザー] ATKeyでログインする	• 「AzureADに参加」したWindows PCにパスワードレスでログイン。 • Microsoftサービス（Azure AD、Microsoft 365、OneDrive、Teams、.....）へのログイン

ステップ 1. [Admin] Azure ADの設定(a)

a)　デフォルトでは、電話番号またはMicrosoft Authenticatorアプリを登録してから、FIDOキーを登録するよう求められます。

1. 管理者権限でAzureポータル(https://portal.azure.com/)にサインインしてください。
2. **Azure Active Directory＞セキュリティ＞認証方法＞ポリシー**を開いてください。 Fig. 1-1
3. **「FIDO2セキュリティーキー」**をクリックして、**「全てのユーザー」**を選ぶか、**「グループの選択」**から**「グループの追加」**で特定のグループを選択してください。 *セキュリティグループのみサポートされます。*
   Fig. 1-2 – *保存した設定はすぐには反映されず、反映されるまで時間がかかる場合があります。*
4. 設定を**「保存」**します。

Fig. 1-1

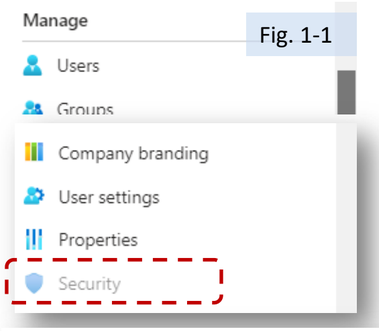
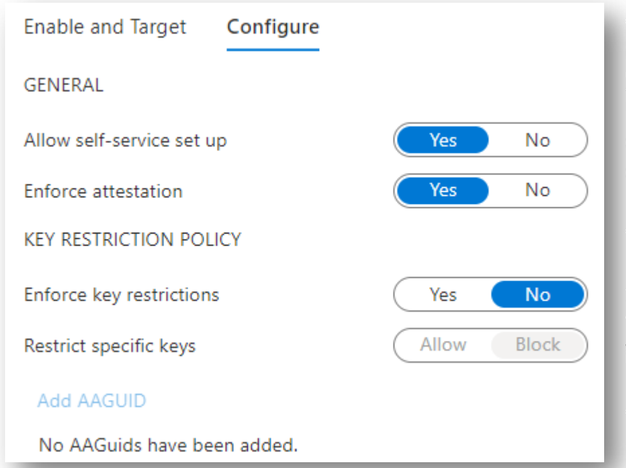


Fig. 1-2

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

5. FIDOセキュリティキーオプション設定



- **「セルフサービス設定を許可」**は**「はい」**に設定したままにします。「いいえ」に設定してしまうと、ポリシーで有効になっていても、ユーザーは「セキュリティ情報」の「サインイン方法の追加」からFIDOキーの登録ができなくなります。

- **「構成証明の適用」**を**「はい」**に設定すると、FIDOセキュリティキーのメタデータが公開され、FIDOアライアンスメタデータサービスで検証され、Microsoftの追加の検証テストに合格する必要があります。

- あなたの組織がAAGUIDsによって識別される特定のセキュリティキーのみを許可、又は拒否したい場合にのみ**「キーの制限の適用」**を**「はい」**に設定してください。セキュリティキープロバイダーと協力してデバイスのAAGUIDsを確認する事ができます。キーが既に登録されている場合、AAGUIDはユーザーごとのキーの認証方法の詳細を見る事によっても見つけることができます。
  - ATKeyのAAGUIDについては、以下のリンクをご確認ください：
    https://authentrend.com/atkey-fido2-security-key-aaguids/

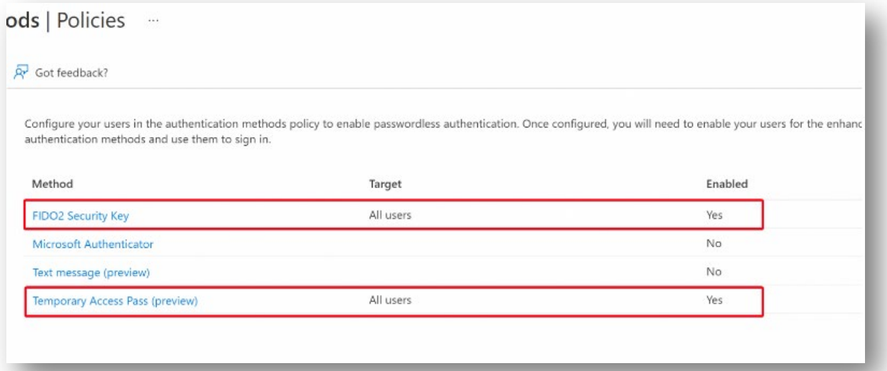
詳細は下記リンクをご参照ください:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key

ステップ 1. [Admin] Azure ADの設定(b)

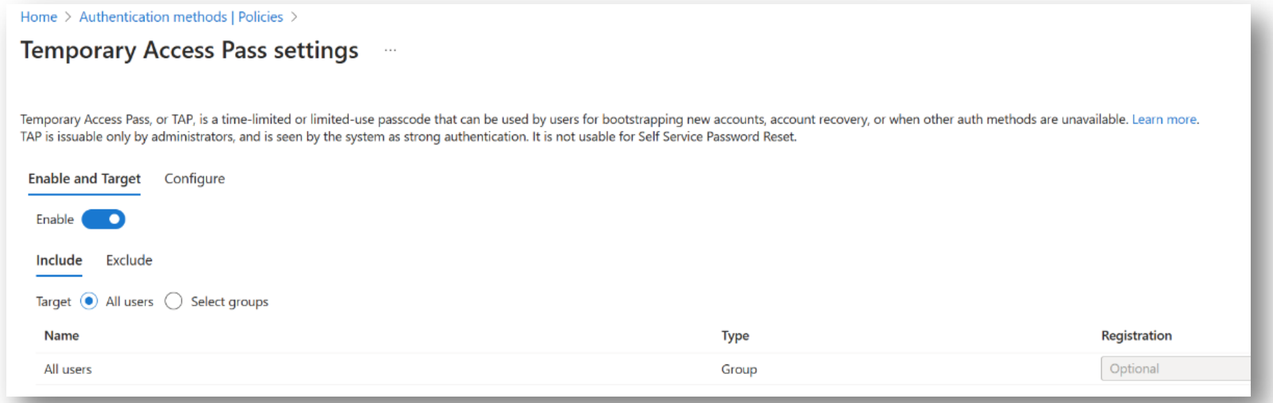
a)　FIDOキーのみ登録したい場合は、「一時的なアクセスパス」(Temporary Access Pass)を設定してから、FIDOキーを有効にしてください。

「一時アクセスパス」は1回限り、または複数回使用できるように設定可能な制限付きパスコードを設定できます。ユーザーはMicrosoft Authenticator、FIDO2、またはWindows Hello for Business等のパスワードレス認証を含む他の認証方法を実装する為に、一時アクセスパスでサインインする事が出来ます。

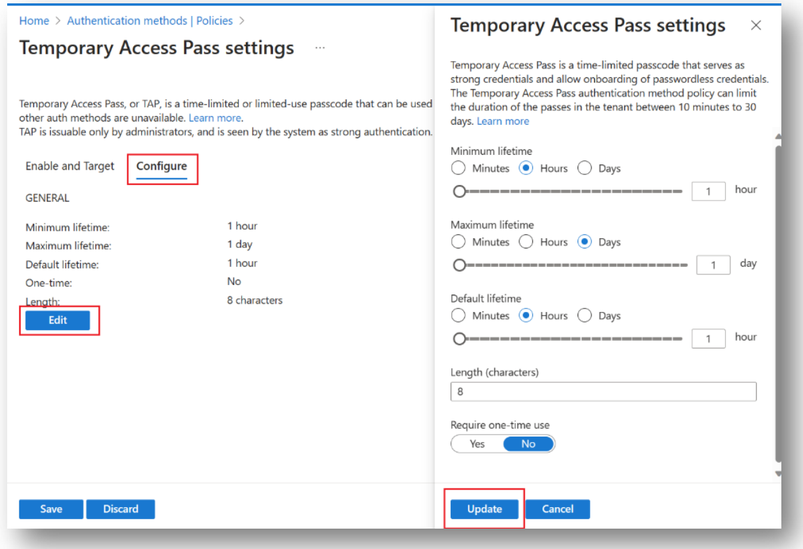
1. グルーバル管理者権限を持つアカウントでAzure Portalにサインインします。
2. **「Azure Active Directory」**を選択し、左側のメニューから**「セキュリティ」**を選択します。
3. 左側メニューから**「認証方法」**＞**「ポリシー」**を選択します。
4. **「メソッド」**のリストから**「一時アクセス パス」**と**「FIDO2 セキュリティキー」**の有効が**「はい」**になっている事を確認し、



5. ポリシーに含めるユーザーと除外するユーザーを選定します。



6. (オプション)**「構成」**を選択して、**「編集」**をクリックしたら、**「最大有効期間」**や**「文字の長さ」**の設定など、デフォルトの**「一時アクセス パス」**設定を変更出来ます。**更新**をクリックし**保存**をクリックして確定します。



詳細は下記リンクをご参照ください:

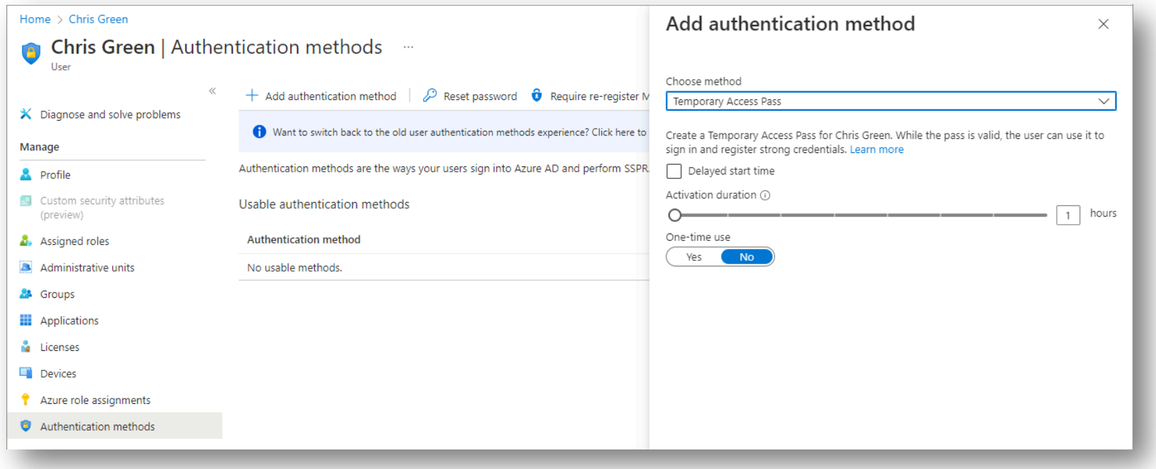
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass

ステップ 1. [管理者] ユーザーに“一時アクセス パス”を発行する(b)

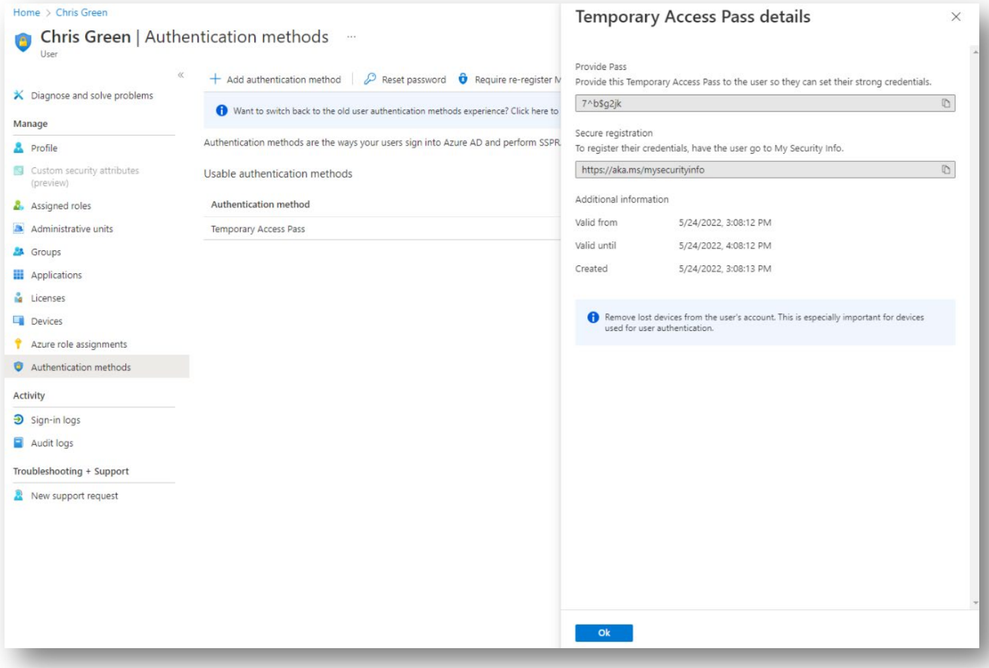
b) FIDOキーのみ登録したい場合は、「一時的なアクセスパス」(Temporary Access Pass)を設定してから、FIDOキーを有効にしてください。

「一時アクセスパス」は1回限り、または複数回使用できるように設定可能な制限付きパスコードを設定できます。ユーザーはMicrosoft Authenticator、FIDO2、またはWindows Hello for Business等のパスワードレス認証を含む他の認証方法を実装する為に、一時アクセスパスでサインインする事が出来ます。

1. 前述のロール(管理者)を使用してAzure Portalにサインインします。
2. **「Azure Active Directory」**を選択し、「ユーザー」をクリックし、設定を適用したいユーザー(ここでは*Chris Green*)を選択し、**「認証方法」**を選択します。
3. 必要に応じて、**「新しいユーザー認証方法のエクスペリエンスに切り替えてください」**をクリック
4. **「認証方法の追加」**をクリック。
5. **「方法の選択」**プルダウンメニューから**「一時アクセス パス」**を選択します。
6. アクティブ化時間や期間を設定し、**「追加」**ボタンをクリックします。



7. 追加されると「一時アクセス パス」の詳細が表示されます。実際の「一時アクセス パス」をユーザーに提供します。**「OK」**ボタンをクリックすると「一時アクセス パス」を再表示する事は出来ません。必要に応じてメモ等してください。

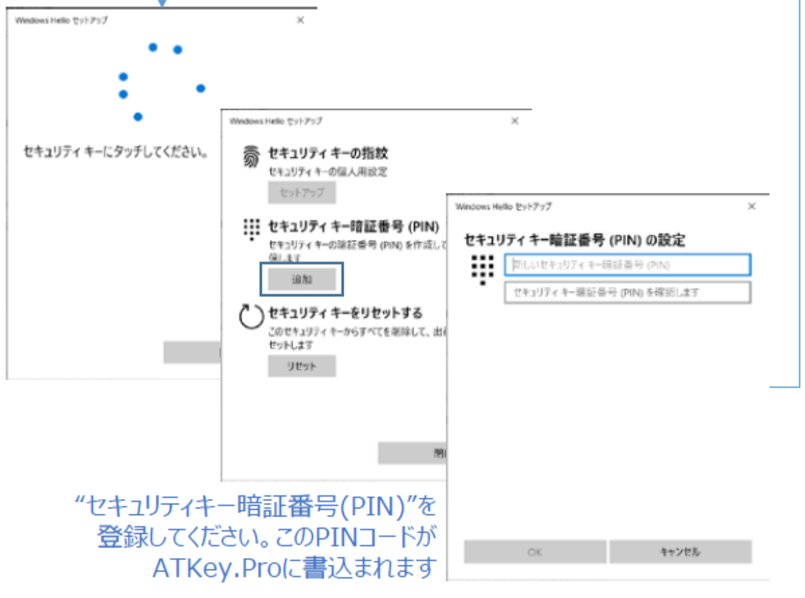


詳細は下記リンクをご参照ください:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass

Step 2. [ユーザー] ATKeyで指紋を利用(a)

a) 標準的なFIDOのログイン方法に従う場合： Windowsの“設定”から指紋認証＋PINコードをATKeyに登録します。

“管理”をクリック
指紋をセンサーにタッチして
セットアップ



“セキュリティキー暗証番号(PIN)”を
登録してください。このPINコードが
ATKey.Proに書込まれます

- “セキュリティキーの指紋”を設定します
- PINコードを入力して画面に従って指紋の登録を完了してください

Helpful Tips

指紋を上手に登録することで、本人確認をより迅速かつ簡単に行うことができます：
https://youtu.be/bCLPMtZJhkM (English)
https://youtu.be/G-p30PEBUQc (Japanese)

Step 2. [ユーザー] ATKeyで指紋を利用(b)

b) PINコードは登録せずに指紋認証のみ（弊社特許技術-スタンドアロン登録）でログインしたい場合。

スタンドアローンで指紋の登録をする

アプリケーションやソフトウェアのダウンロードは不要

- 必要な物：USBポートからの給電(パソコン、モバイルバッテリーからも可能)
- 同じ指を少し異なる確度の位置で登録してください

Tutorial video

・ATKey.ProをUSBポートに差込みます。
・ATKey.ProのLEDがシアン色に点灯します。
・本体横の小さいボタンを3回連続でクリックするとスタンドアローンモードに切替わります。

✓ LEDが白点滅の場合：指紋をセンサーにタッチしてください。タッチ時LEDが緑色に点く場合は指紋を認識登録されている状態を意味しており、タッチ時にLEDが赤色に点く場合は認識されていない状態を意味します。
✓ 指紋の登録タッチは、おおよそ12回認識登録を繰り返し、登録完了が間近になると白LEDの点滅が早くなります。登録が完了するとLEDが青色に切り替わります。

- 指紋登録を途中やめたい場合は本体横のボタンを1回クリックするとLEDが青色に戻ります。
- 既に指紋が登録されている状態でスタンドアローン登録を行うと、第三者が勝手に指紋を登録できないように、登録された指紋の照合を求めてきます。この時LEDは緑色に点滅しますので、既に登録した指紋を照合してから、新しい指紋を登録してください。

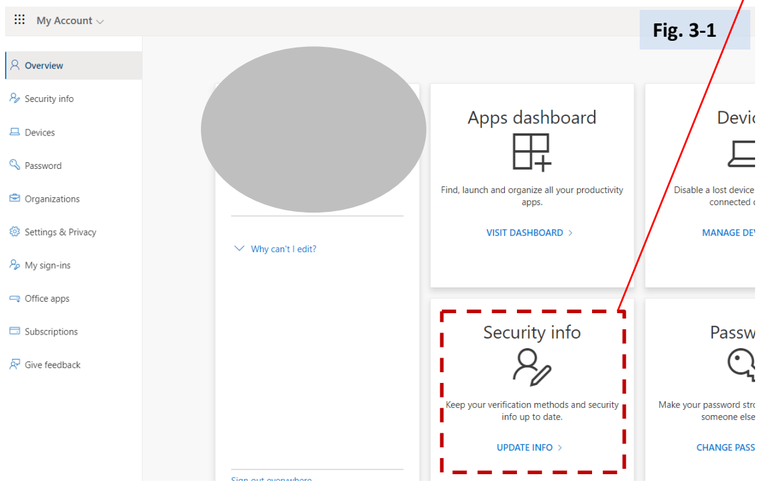
Helpful Tips

指紋を上手に登録することで、本人確認をより迅速かつ簡単に行うことができます：
https://youtu.be/bCLPMtZJhkM (English)
https://youtu.be/G-p30PEBUQc (Japanese)

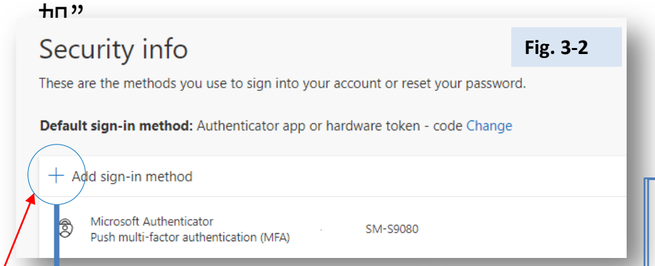
Step 3. [ユーザー] ATKeyをAzure ADアカウントに登録する(a)

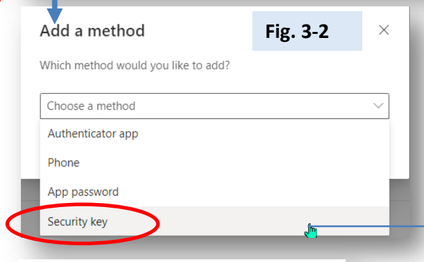
a) デフォルトでは、電話番号またはMicrosoft Authenticatorアプリを登録してから、FIDOキーを登録するよう求められます。

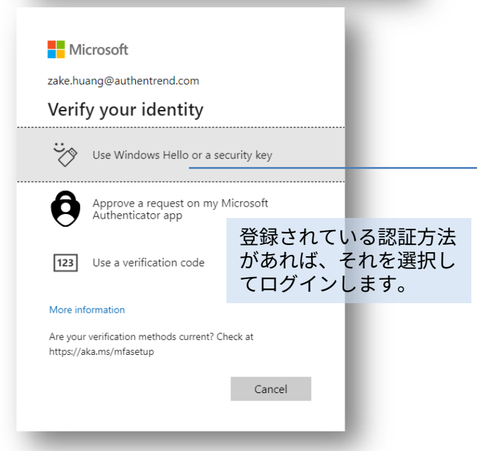
1. https://myprofile.microsoft.comにサインインしてください。
2. **「セキュリティ情報」**をクリック。Fig. 3-1
   1) ユーザーが既にAuzreAD Multi-Factor Authentication(多要素認証)の方法を1つ以上登録している場合(Microsoft AuthenticatorやSMS認証など)は、すぐにFIDO2セキュリティキーを登録できます。
   2) １つも多要素認証の登録が無い場合は、最低1つ追加する必要があります。
   3) 管理者は一時アクセス パスを発行する事で、ユーザーがパスワードレス認証の方法を登録出来るようにすることが出来ます(次ページ参照)
   4) **「認証方法の追加」**をクリックして**「セキュリティキー」**を選択し、**「FIDO2セキュリティキー」**を追加します。Fig. 3-2
   5) **「USBデバイス」**又は**「NFCデバイス」**を選択します Fig. 3-3
   6) **「FIDO2セキュリティキー」**を用意し、**「次へ」**を選択します。
   7) **「FIDO2セキュリティキー」**を登録する必要な手順(指紋タッチ等)を実行します。
   8) ユーザーは登録したFIDO2セキュリティキーを簡単に識別出来るように名称を入力するよう求められますので、入力して**「次へ」**をクリックします。Fig. 3-4
   9) 「完了」をクリックしてプロセスを完了します。



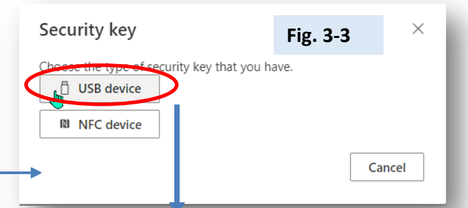
- セキュリティ情報 => “+ サインイン方法の追加”

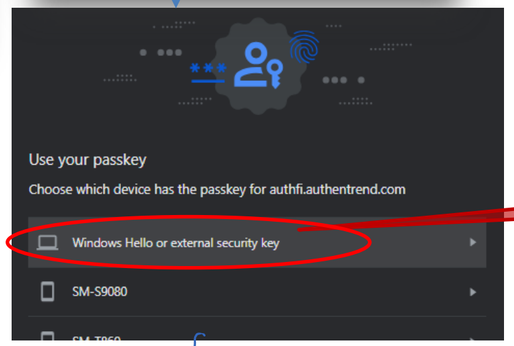




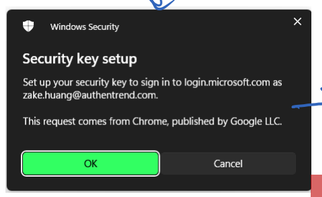


登録されている認証方法があれば、それを選択してログインします。



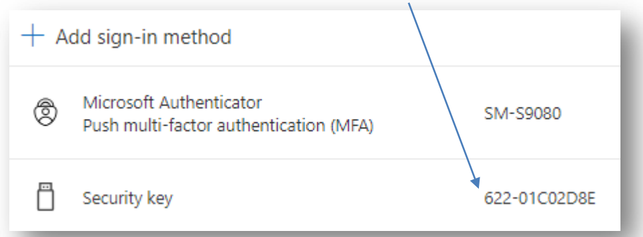


こちらを選択



ATKeyに指紋をタッチして登録

キーの名前を付ける

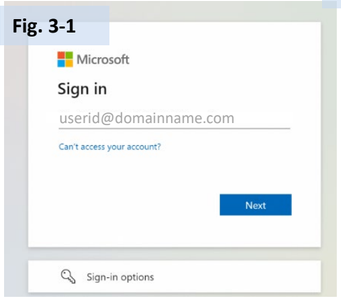


Step 3. [ユーザー] ATKeyをAzure ADアカウントに登録する(b)

b) FIDOキーのみ登録したい場合は、「一時的なアクセス パス」を設定してから、FIDOキーを有効にしてください。

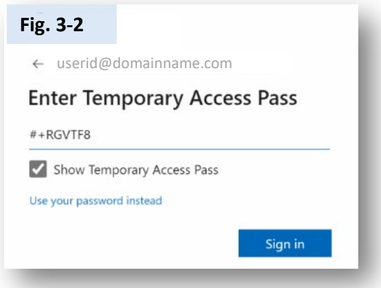
1. ステップ 1. [Admin] Azure ADの設定(b)で「一時アクセス パス」が有効になっている事を確認してください。
2. ログアウトがされている事を確認してから新しいセッションで https://aka.ms/mysecurityinfo.へアクセスしてユーザー名を入力し**「次へ」**をクリックします。**Fig. 3-1**

Fig. 3-1



3. ここで、パスワードの代わりに、Azureポータルに表示されていた、「一時アクセス パス」の入力を求められます。**Fig. 3-2**

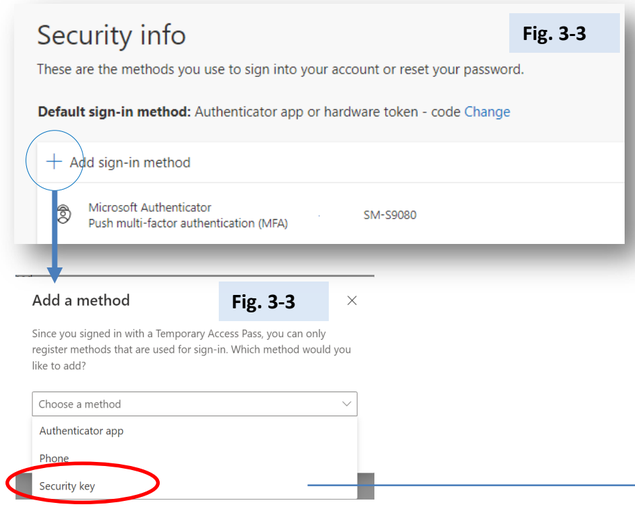
Fig. 3-2

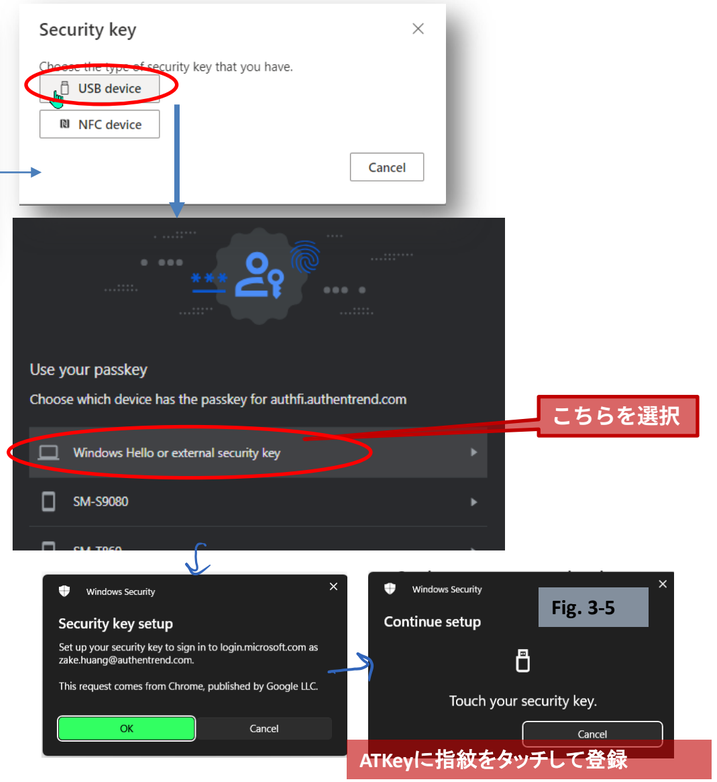


4. サインイン後、**「セキュリティ情報」**を選択し、**「認証方法の追加」**をクリックして、**「方法を追加します」**のプルダウンメニューから**「セキュリティキー」**を選択します。**Fig. 3-3**

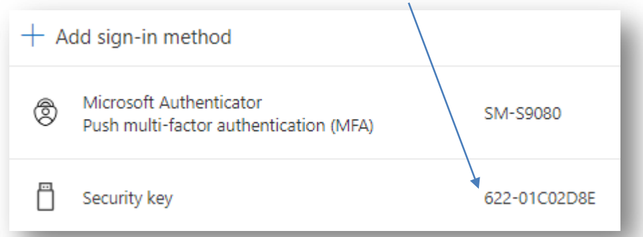
- セキュリティ情報 => “+ サインイン方法の追加”

Fig. 3-3





キーの名前を付ける



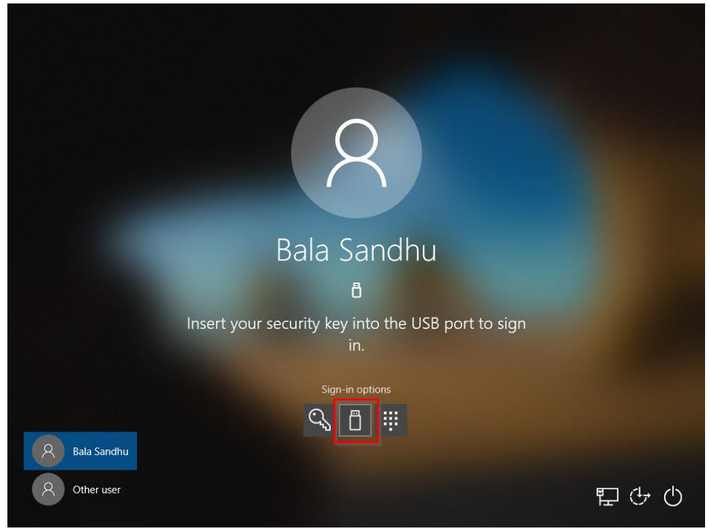
Step 4 [ユーザー] ATKeyでログインする

a) 「AzureADに参加」したWindows PCにパスワードレスでログイン

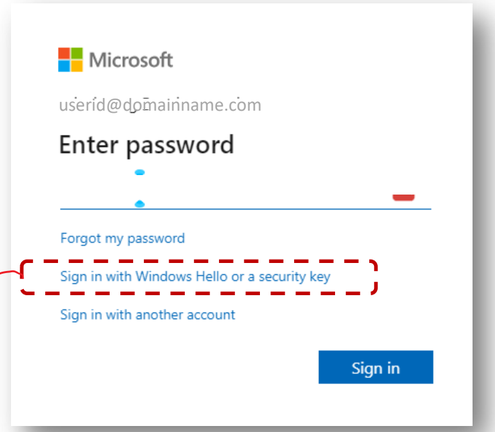
“Bala Sandhu ”という名前の下記のユーザーは、前のページの「パスワードレスを有効にしてセキュリティキーでサインインする」の手順を使用して、すでに FIDO2 セキュリティキーをプロビジョニングしています。

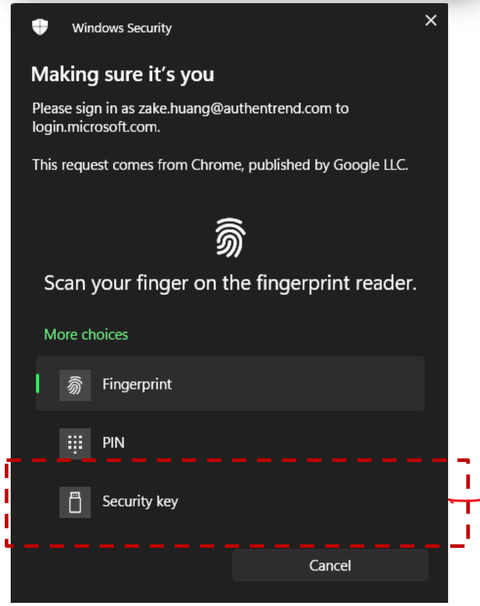
ハイブリッド Azure AD に参加しているデバイスの場合、「パスワードレスを有効にしてオンプレミス環境にセキュリティキーでサインインする」も有効にしていることを確認してください。

上記設定により“Bala ”は、Windows 10のロック画面からセキュリティキー・クレデンシャル・プロバイダを選択し、セキュリティキーをUSBポートに挿入してWindowsにサインインすることができます。(Windows10ビルド1903+、Windows11)

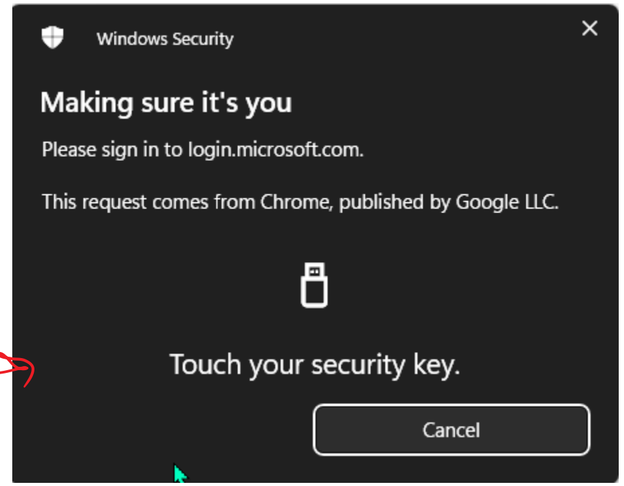


b) Microsoftサービス（Azure AD、Microsoft 365、OneDrive、Teams、.....）へのログイン





“セキュリティキー”を選択してください



ATKeyに指紋をタッチして照合

ATKeyのLEDが青く点滅したら、指紋をタッチして照合すること要求している事を意味します。

ATKey.ProのLED

What the LEDs mean

Blue LED ON	電源がONの状態
Green LED ON	指紋照合に成功した状態
Red LED ON	指紋照合に失敗/指紋の削除中/キーのリセット中の状態
Cyan LED ON	OSがキーを認識していない状態
Blue LED flashes	指紋の照合を求めている状態
Cyan LED flashes	タッチのみが必要な状態
White LED flashes	スタンドアローン登録(段々早く点滅する)
Green LED flashes	指紋登録がある状態でスタンドアローン登録前に指紋の照合を求めている状態

ATKEY.Pro

AUTHENTREND

あなたの会社で
パスワードレスを始めましょう。


www.AuthenTrend.com


contact@authentrend.com


AuthenTrend


AuthenTrend technology inc.