

# ユーザーガイド (管理者用)



REVISION: 1.0 DATE: 2022 DEC.

## Table of Contents

Tab	le	of Contents1
1.	A	T.LogOn について2
а	)	AT.LogOn には以下の利用/環境が含まれます2
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。3
С	)	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
1.	: L	ます。
2.	IT	「管理者 – 初期化と登録4
а	)	URLs の定義と注目点
b	)	AT.LogOn.Server の初期設定
С	)	ATKey.Pro を従業員に割り当てる12
d	)	"AT.LogOn for Windows"を従業員の PC にインストールしてください。17
е	)	管理者のユーザーケース17
3.	衏	É業員の Windows ログイン21
а	)	指紋の登録21
b	)	ATKe.Pro を AD アカウントに登録する
C	)	初回ログインと2回目以降のログイン24
d	)	内部ドメインと外部ドメイン
е	)	オンライン/オフライン
f)		ATKey のユーザーケース(従業員向け)
4.	A	T.LogOn Server 管理
а	)	admin の割り当て
b	)	"Hotkey"(ホットキー)と"Recovery code"(リカバリコード)
с	)	登録ユーザーの管理
d	)	API ログ
5.	R	DP – リモートデスクトップ
а	)	ホスト PC、リモート PC、AD の設定基準34
b	)	RDP のユーザーケース
6.	A	T.LogOn.Pass
а	)	Chrome extension(Chrome 拡張機能)
b	)	Chrome whitelist
7.	N	lore from ATKey.Pro

### 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



AT.LogOn for Windows

(credential provider)

Subsection of the

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

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:
    - o 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:
        - ✓ <u>adfs01.domainname,com</u> (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。
    - o 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。



o 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。

لموOn				admin Admin
Overview				
Registered Users API Logs	FIDO2 server adfs01.att.co Domain name adfs01.att.co Please cl Passwor	لا xange your password for the first login in ID/ under user's menu.	Registered User 17 Max User 1000	
	Account	Set now Later	Last login at 2022/12/21 13:49:38	Operations
	att\atest.jensen	2022/11/11 12:03:06	2022/12/22 03:51:23	От ди
ID/Password	×			
Password :				
đ	0			
. New Password :				
£	۲			
Confirm new Password :				
Ê	0			
* The password only allows 8 d numbers and alphabets.	ligits mixed with			
• Allow ID/Password to login On * For security reasons, it is reco	ommended to disable			
* Before turning off, please mail at least 2 keys.	ke sure you register			
Apply	y Cancel			
✔ パスワードの	代わりに ATKey.P	ro をパスワードレスログィ	ン認証機として登録す	けること
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。
- o 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。

n	2022/11/	at #	Last login =	Operations		
"鍵"のアイ	コンをクリック	します(赤丸でハイ	ライト)			
FIDO2 server adfs01.att.cor Domain name adfs01.att.cor	m/10.38.10.26 m	δ Lock key Remaining 17 days	Registe 17 Max Us 1000	ered User ser		
Account	,	Created at 📲	Last login 🔹	Operations		
admin	2	2022/11/09 19:24:35	2022/12/21 13:49:38	( OT )		
"+ Add a new authenticator"(新しい認証機を追加)をクリック						
Account	•	Created at	Last login *	Operation		
admin	2	2022/11/09 19:24:35	2022/12/21 13:49:38	On 🎥		

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)

2022/11/09 19:24:35 Registered at 2022/12/23 17:12:16	2022/12/21 13:49:38	On 💩
Registered at 2022/12/23 17:12:16	<b>D</b>	
変更		
7		

- ✓ 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。
- o 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。
- o "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。

		admin Admin	1
	Admin		
	Hotkey	, <sup>Im</sup>	
egistere	ID/Password	1	
00	About		
	Logout		

"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。

⊗ Ho	tkey	@ Re	covery Code	
Content	Ctrl + Shift + Z + A	Content	12345678	

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。

1210101					
Hotke	ey .				
Hotke Pleas differe	ey is composed e choose 2 fund ent alphabets in	of <b>4 keys</b> ctional but the input	ttons from tox as He	below options an otkey.	d type in two
	🔲 Alt 🔽	Ctrl	Shift	Windows L	ogo
+	Z		+	A	
*Since define	e this hotkey is ed hotkey won't	for Windo be same	ows logon as other s	screen, please ma ystem or applicati	ake sure on defined
Recov	very Code				
123	345678			Random code	generator
*Reco	overy code allov	vs 8 digits	s only		

"Apply"の機能を ON にしてください。

	)			Q
⊗но	tkey	@ Re	covery Code	
Content	Ctrl + Shift + Z + A	Content	12345678	6
Created at:	2022/12/23			Records

- ✓ 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。

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

- o 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。

Welcome
Login
Please have your ATKey ready.
🛉   Login with fide
Login with ID/Password

Use your passkey Choose which device has the passkey for adfs01.att.com	Windows Security ATKey.Pro LED is blue flashing, Malteych registered fingerprint to login Please sign in to adfs01.att.com.	×
the External security key or built-in spesor	This request comes from Chrome, published by Google LLC.	
Select "External security key or"	Ö	
as authenticator	Touch your security key.	
SM-T860	Cancel	
A different device	© Wait for venty	
Manage devices Ca	and the second se	

- o 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。

۵gOn				admin Admin
verview	Account Q	Keycode Q	Created at v 🛅 Start date -	End date C
egistered Users				
	Account	Created at	Last login 🔹	Operations
21 Logs	ATT\atest.nuno	2022/11/14 16:48:14	2022/11/29 16:50:08	On 🙇 🗓
	att/elia1	2022/11/18 10:06:02	2022/11/18 10:06:02	0m 🗸 🗓
	att/elia2	2022/11/18 10:20:30	2022/12/21 14:11:23	On 🎥 🗓
	Att/elia3	2022/11/18 13:53:12	2022/12/23 18:29:11	On 🙇 🗎
	att/user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	0- 1. E
	att/user3.demo	2022/11/21 18:29:47	2022/11/23 14:58:05	On 🌋 🛙
	ATT\nuno1	2022/11/22 11:17:42	2022/12/20 12:30:26	Оп 🙇 🚺
	att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	On 🚴 🗓
	att/elia4	2022/11/23 16:10:07	2022/12/19 14:05:15	On 🔏 🗓
	att\elia5	2022/11/23 16:18:49	2022/12/19 14:33:02	On .

- ✔ 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。

gOnوا				admin Admin
Overview Registered Users API Logs	Comparison of the server adfs01.att.com	δ Lock key Remaining 17 days	Registered User 1 Max User 1000	
	Account	Created at =	Last login 🤌	Operations
	admin	2022/11/09 19:24:35	2022/12/23 18:30:36	On 🎥
	att\atest jensen	2022/11/11 12:03:06	2022/12/23 18:31:59	On 🚴
🗕 🚽 🚽	att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	Оп 🙇
	att\atest.carrine	2022/12/13 12:03:24	2022/12/23 18:05:59	On 💄

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。

	Created at	Last login 👘	Operations
	2022/11/09 19:24:35	2022/12/23 18:30:36	On 🚴
ensen	2022/11/11 12:03:06	2022/12/23 18:31:59	On 🎥
demo	2022/11/21 18:22:13	2022/11/23 13:50:12	-( 2m
arrine	2022/12/13 12:03:24	2022/12/23 18:05:59	On or
	6		
	×		
	ensen demo carrine	Created at #       2022/11/09 19:24:35       ensen     2022/11/11 12:03:06       demo     2022/11/21 18:22:13       carrine     2022/12/13 12:03:24	Created at #         Last login #           2022/11/09 19:24:35         2022/12/23 18:30:36           ensen         2022/11/11 12:03:06         2022/12/23 18:31:59           demo         2022/11/21 18:22:13         2022/11/23 13:50:12           carrine         2022/12/13 12:03:24         2022/12/23 18:05:59

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。

Confirm

att\user1.demo

- ✓ 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
  - o 要求するログの確認または検索(各 API から)



logOn						<b>a</b> A
werview	Account ~ Search	Created at	Start date +	End date: Q		
egistered Users						-
	Type API Name	Account	IP Address	Created at description		Result
PI Logs	POST http://127.0.0.1.8080/assertion/authOnly	Attelia3	10.38.10.104	2022/12/23 18 48 32	2	Success
	POST http://127.0.0.1.8080/assertion/challengOn	ły	10 38 10 104	2022/12/23 18:48:31		Success
	PATCH http://127.0.0.1.8080/adminimanagement/ 1G4HCjKW9IWFWdUXLb6f5bk-L7MXaW5	yroLqM4J6U M	10.38.10.108	2022/12/23 18:47:54		Success
	POST http://127.0.0.1.8080/assertion/authOnly	Attielia3	10.38.10.104	2022/12/23 18:42:44		Success
	POST http://127.0.0.1.8080/assertion/challengOn	ly .	10.38.10.104	2022/12/23 18:42:43		Success
	PATCH Mtp://127.0.0.1.8080/admin/management/ 1G4HCjKW9NWFWdUXLb8f5bk-L7MXaW9	yroLqM4J6U attiuser1.demo SM	10 38 10 108	2022/12/23 18:39:14		Success
	POST http://127.0.0.1.8080/assertion/authOnly	Attielia3	10.38.10.104	2022/12/23 18:36:56		Success
	POST http://127.0.0.1.8080/assertion/challengOn	ły	10.38.10.104	2022/12/23 18:36 55		Success
	POST http://127.0.0.1.8080/assertion/authOnly	Attielia3	10.38.10.104	2022/12/23 18:35:01		Succesa
	POST http://127.0.0.1.8080/assertion/challengOn	ly .	10.38.10.104	2022/12/23 18:35:00		Success

- o 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)
  - o 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。



- Check keycode for production record customer service and warranty
- 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。
  - o 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バシー) ※Windows を除く
    - Standalone enrollment: https://youtu.be/NnNqXbrf7vA (AuthenTrend 特許技術)
  - o 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
  - o 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。

login demo/5@atloosndemo.com	5
	5
login	

 のめて 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



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

。 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

- 0 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:

URL: (mandatory)	AD + :	FS の URL(管理者様がローカルパー ナーと事前に設定したもの)
API KEY:	•	AuthenTrend がローカルパートナー、 管理者に定義し、割り当てたもの (AT.LogOn,Server 毎に固有のキーをお
SID SEC:		(いたの) ちます)

- TARGET\_URL="adfs01.domainname.com"
- API\_KEY= "D/rgZVIVB4LvF3nnoBX5VuvG+0qDX9Is6fu5i46gGmk="
- SID\_SEC= "GluQTZkKRC/sgYfaXpcdt2bSpXmfo8Rn3/an/U/B+nM="

geetlocal enableextensions Ged /d "%~dp0"	
.\ATLogOnForWindows.exe /quiet TARGET_URL="adfs01.att.com" API_KEY="D/ngZVIVB4LvF3nnoBX5VuvG+0qDX9Is6fu5146gGmk=" 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。
  - o 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: <u>account@domain.com</u> 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。

Characteristic de la constante	
Change password	
someone@example.com	
Old pursword	
new password	
	Change password someone@example.com Old password new password

o 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)
  - o 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。

- **AUTHENTREND**  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
  - o 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: <u>https://youtu.be/NnNqXbrf7vA</u>
  - 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

You are not logged in, log in to this website
login
© 2018 Microsoft

b. ユーザーの AD の AD/Password でサインインします。

login	
demo05@atlogondemo.com	5
	5
login	

- 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。



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



		For security reasons, we verify your account
	Windows Security	× sert ATKey and
	Security key setup Set up your security key to sign in to adfs.att.com	as att
	This request comes from Chrome, published by G	.0.0.4 cogle LLC.
	OK Cano	ы
1.1		Please insert ATKey
•	Windows Security	×
Cor	ntinue setup	
	Ē	4
	Touch your security ke	у.
	Ca	incel
of the		

- 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
  - o 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

- o 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. <u>https://adfs01.domainname.com/dashboard/</u>)

<b>LogOn</b> Welcome
Login
Please have your ATKey ready.
<b>†</b>   Login with <b>fido</b>
Login with ID/Password

- "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。

وما				admin Admin
Overview	Account	Keycode Q	Created at V 🖄 Start date	- End date Q
Registered Users				
	Account	Created at	Last login 🔹	Operations
API Logs	ATT\atest.nuno	2022/11/14 16:48:14	2022/11/29 16:50:08	on 🙇 🗓
	att\elia1	2022/11/18 10:06:02	2022/11/18 10:06:02	0m 📠 🗓
	att\elia2	2022/11/18 10:20:30	2022/12/21 14:11:23	On 🙇 🔟
	Att\elia3	2022/11/18 13:53:12	2022/12/23 18:29:11	0n 🚴 🖽
	att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	~ <b>.</b> 1
	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	On 🚴 🗓
	att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	0n 🚴 🖽
	att\elia4	2022/11/23 16:10:07	2022/12/19 14:05:15	on 🚴 🗒
	att\elia5	2022/11/23 16:18:49	2022/12/19 14:33:02	On 🐁 🔟

- 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。

Acco				×	gin a	
ATT	Assign this specific user a	s administrator	role?	11	1/29 16:50:08	
att/eli				11	1/18 10:06:02	
attleli	att/user1.d	lemo		13	2/21 14:11:23	
Att\el				13	2/23 18:29:11	
att\us		Confirm	Cancel		1/23 13:50:12	
att\us					1/23 14:58:05	

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

gOnوما				admin Admin
Overview		F		
Registered Users	FIDO2 server adfs01.att.com/10.38.10.26 Domain name adfs01 att.com	O Lock key Remaining 17 days	Registered User 17 Max User 1000	
API Logs	unsertaktoon		1000	
	Account	Created at	Last login 🔹	Operations
	admin	2022/11/09 19:24:35	2022/12/23 18:30:36	Om 🎥
	att\atest.jensen	2022/11/11 12:03:06	2022/12/23 18:31:59	On 🐊
	att\user1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	On 2.
	att\atest carrine	2022/12/13 12:03:24	2022/12/23 18:05:59	On &

• 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。

				AUTFENTREND
				2×
⊗но	tkey	@ Re	covery Code	•
Content	Ctrl + Shift + Z + A	Content	12345678	đ
Created at:	2022/12/23			Records

THEATOCH

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。

lotkey & Reco	very Code		×
у			
y is composed of 4 e choose 2 function ent alphabets in the	<b>keys</b> nal buttons from input box as He	below options a otkey.	and type in two
📄 Alt 🔽 Ctr	I 🔽 Shift	Windows	s Logo
Z	+	А	
this hotkey is for t d hotkey won't be very Code	Windows logon same as other s	screen, please i system or applic	make sure ation defined
845678		Random cod	le generator
very code allows 8	digits only		
		(	
	Hotkey & Record         y         y is composed of 4         is choose 2 function         nt alphabets in the         Alt       Ctr         Z         e this hotkey is for V         d hotkey won't be a         rery Code         145678         wery code allows 8	Hotkey & Recovery Code         y         y is composed of 4 keys         e choose 2 functional buttons from         nt alphabets in the input box as He         Alt       Ctrl         Alt       Ctrl         Alt       Ctrl         It is hotkey is for Windows logon         d hotkey won't be same as other s         rery Code         Hotker         Wery code allows 8 digits only	Hotkey & Recovery Code         y         y is composed of 4 keys         s choose 2 functional buttons from below options and alphabets in the input box as Hotkey.         Alt       Ctrl         Alt       Ctrl         Shift       Windows         Z       +         A       A         Random code       Keys         Keys       Random code         Wery code allows 8 digits only       Keys

• 必ず"Apply"ボタンを押して機能を有効にしてください。

⊗но	tkey	@ Re	covery Code	
Content	Ctrl + Shift + Z + A	Content	12345678	

- 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。



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) 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 (<u>https://fs.domainname.com/adfs/ls/idpinitiatedsignon</u>)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。

logOn				admin Admin i
verview	Account	Q Keycode	Q Created at v 📰 Start date	- End date Q
gistered Users				
	Account	Created at	Last login 🦉	Operations
API Logs	att\atest.jensen	2022/11/11 12:03:06	2022/12/27 21:17:27	0n 🚠 🔟
	att'elia2	2022/11/18 10:20:30	2022/12/26 15:54:01	on 🔔 🗇
	Attielia3	2022/11/18 13:53:12	2022/12/28 11:26:28	0= 🏨 🔟
	attiuser1.demo	2022/11/21 18:22:13	2022/11/23 13:50:12	or 🚠 🔟
	ATT\nuno1	2022/11/22 11:17:42	2022/12/27 18:18:28	o= 🔔 🔟
	att\atest.elia	2022/11/23 14:55:16	2022/12/21 17:19:24	0m 🧸 🔟
	att\elia5	2022/11/23 16:18:49	2022/12/26 17:53:14	0= 1. D
	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	On 🛵 🔟
	attizakenew	2022/12/16 15:57:49	2022/12/16 16:30:54	on 1. 🗇
			Registered A managemen	TKey.Pro Delete the u does not exi inactive, ren
				Assign this specific user as administrator role for

- ◆ 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

Ac	count	Created at	La	ast login ⊥⊧	Operations
att\	atest.jensen	2022/11/11 12:03:06	20	022/12/27 21:17:27	Оп 🙇 🗓
	δ [keycode]j2	Registered at 2022/12/27 21:16:13	Ē		
	+ Add a new authenticator				

AT.LogOn.Server

 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。

Account	Created at	Last login #	Operations
att\atest.j	2022/11/11 12:03:06	2022/12/27 21:17:27	On 🚴 🗐
δ 01C01F5E	Registered at 2022/12/27 21:16:13	۵	
	A		

<= 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。

	×	Last
e]12	Are you sure to delete this key ?	2022
w au	[keycode] 12345678	
	Confirm Cancel	2022 2022

- [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。

att\user1.demo	Q	
Keycode (キーコード): 万ヵ	バー紛失	したん

 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。

01C	01F5E			Q

▶ 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。

		2022	Decer	mhar					201	2 Ton	0177		5 5
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3	25	26	27	28	29	30	31
4	5	6	7	8	9	10	1	2	3	4	5	6	7
11	12	13	14	15	16	17	8	9	10	11	12	13	14
18	19	20	21	22	23	24	15	16	17	18	19	20	21
25	26	27	28	29	30	31	22	23	24	25	26	27	28
1	2	3	4	5	б	7	29	30	31	1	2	3	4

#### 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)

Account	Search Search	Q	Created at	Start date •	End date Q
Туре	API Name	Account	IP Address	Created at d	escription Result
PATCH	http://127.0.0.1.8080/admin/managem ent/5iku02vhyz7qQo9YOIGiGIRg5Zr My002RnAQR4qnXD0/credential/w7F JOR8jWT23WJRfj1MSVe07iF2TOAAy op-yGI0XAD8	att\atest.jensen	10.38.10.108	2022/12/28 12:47.40	Succes
PATCH	http://127.0.0.1.8080/admin/managem ent/5ikuQ2vhyz1qQo9YOIGiGIRgSZr My0O2RnAQR4qnXD0/credential/w7F JOR8jWT23WJRj1MSVe07iF2TOAAy op-yGI0XAD8	att\atest jensen	10 38 10 108	2022/12/28 12:47:12	Succes
POST	http://127.0.0.1.8080/assertion/authOn ly	att\elia4	10.38 10 113	2022/12/28 12:19:42	Success
POST	http://127.0.0.1:8080/assertion/challen gOnly		10.38.10.113	2022/12/28 12:19:39	Succes
POST	http://127.0.0.1:8080/assertion/challen gOnly		10.38.10.113	2022/12/28 12.18.55	Succes
POST	http://127.0.0.1.8080/assertion/authOn ly	attlelia4	10.38.10.115	2022/12/28 12:18:25	Succes
POST	http://127.0.0.1.8080/assertion/challen gOnly		10 38 10 115	2022/12/28 12:18:22	Succes
POST	http://127.0.0.1:8080/assertion/challen gOnly		10.38.10.115	2022/12/28 12:18:19	Succes
POST	http://127.0.0.1.8080/assertion/challen gOnly		10 38 10 115	2022/12/28 12:18:16	Succes
POST	http://127.0.0.1.8080/assertion/challen gOnly		10 38 10 115	2022/12/28 12:18:14	Success

### AUTHEOTREND

10/page ~ < 1 2 3 4 5 6 ... 40237 >

- ◆ 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。

AT.LogOn for Windows

がインストールされてい

AD クライアント参加

るか

### 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)



• 各役割の基準は下記の通りとなります。

Active Directory

クライアント PC と ATKey.Pro 側	client with PC1 ATKey.Pro	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	<b>管理者権限のアカウント</b> でなければならないか? 必須です。	<b>管理者とし</b> デスクトッ mstsc)した か? 管理者とし 又は直接実 す。	て実行(リモート プクライアント- なけ r ばならない って実行する(推奨) 2行どちらも可能で	<b>その他</b> 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	PC 2 Remote Host	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。	<b>AD で RDP が許可さ たアカウントが必要</b> 必須です。 AD admin アカウン も OK です。	*れ か? トで	その他 ATKey.Pro をこのリモ ATKey.Pro をリモート あります。 しかし、リモート PC 必要なので、リモート トの後であれば「ホッ	ニートホストアカウントに登録し、 ・ホストにリダイレクトする必要が は「ログインセッション」の準備が PC がクールブートやウォームブー トキー+リカバリコード↓ →「ID/
		NLA が AD 有効にす る必要があるか? 必須です。				・ スワード」でログイ ッションが準備されて クトはログインセッシ となります。	ンできますが、その後はログインセ いるので、ATKey.Pro のリダイレ ョンが整っているため、動作が可能

AD 側

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。

File Action View Help	ps (Local)/Groups)	General	nte Desktop Users		
Local Users and Groups (Local)	Name Access Control J Administrators Backup Operato Cryptographic C Cryptographic C Device Owners Distributed CON Event Log Reade Guests My Devr-V Admin	Description: Members:	Members in this group are granted t remotely in Admins Users	the right to logon	
	IIS_IUSRS     Network Config     Performance Lo     Performance Mo     Power Users	Add	Changes to a user's are not effective un user logs on. OK Cancel App	s group membersh still the next time dy He	hip the
	Remote Desktop Remote Manage Replicator System Manage Users	u Users ement Users d Accounts Group	Members in this group are Members of this group can Supports file replication in a Members of this group are Users are prevented from m	grante acces a dom mana naking	

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

Windows Security       Run As Admin       X         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.         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.       AT.LogOn for Windows         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.       Or windows         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.       Or windows         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.       Or windows         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified. Please enter new credentials.       Or within 596 sec, scan or input "NWLI-6QX1" into the APP.         Image: Comparison of the remote computer 192.168.139.137 because its identity is not fully verified.       Description of the remote comparison of the	Windows Security       NOT Run As Admin       ×         Enter your credentials           These credentials will be used to connect to 192.168.139.137.           Image: Art.LogOn for Windows            Confirm password             Please enter password for current user within 25 sec.
REFRESH	Remember me
OK Cancel	OK Cancel

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
  - o ATKey.Pro#2 がアカウント#B に登録されている。

- o 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。
  - o 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。
  - o 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。
  - の 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。

### 

Windows	Security		×
Enter	your credentials		
These o	redentials will be used to co	nnect to 192.168.139.137.	
( 🍆	AT.LogOn for Windows		
V	Confirm password		
1.	Enter the current user's pa	assword.	
	Remember me	<b>-</b> 2.	
	ОК	Cancel	1

 (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。



*	Name	Date modified	Туре	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			
I	🚞 pages	12/27/2021 4:33 PM	File folder			
_	🚞 рорир	12/27/2021 4:33 PM	File folder			
	🚞 views	12/27/2021 4:33 PM	File folder			
C:)						
Folder:	dist-chrome					
				Select	older	Cancel .::

o 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。

$\equiv$ 🧿 Extensions			٩	Search extensi
Load unpacked Pack extension	Update			
	6	AT.LogOn.Pass 0.9.5 A secure hardware passy your devices.	word manager	for all of
		ID: ngdcddmicfialbbdme Inspect views <u>backgrour</u>	bdkmkddkphe 1 <u>d.html</u>	dek
	Details	Remove	C	e

• ATKey.Pro のバインディングを開始します。

*	Extens	iona			×	🙆 chrome-extension//ngdcddmichali X +
4	$\rightarrow$	с	* A	LogOn.Pa	ass	chrome-extension://ngdcddmicfialbbdmebdkmkddkphedek/selup.html
M	Gmail	۰	YouTube	🛃 Maps		
						🖻 LogOn #45
						Welcome to AT.LogOn.Pass
						Gives you an additional layer of security while protecting your passwords!
						Bind an ATKey to access your password vault.
						Bind ATKey

 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。

	"AT.LogOn.Pass" wants to connect to a H	ID device
	ATKey.Pro-01C01F5E - Paired	
A LogOn. PASS		
Welcome to AT.LogOn.Pass		
Gives you an additional layer of security while protecting your passwords Bind an ATKey to access your password vault.		
Bind ATKey	0	

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

"AT.LogOn.F	AT.LogOn.Pass" wants to connect to a HID device						
ATKey.Pro-0	IC01F5E - Paired						
?			Connect				

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: <u>https://www.youtube.com/watch?v=7g3gjnb5mPA</u> (Github のアカウントでデモを行なっています)

- AT.LogOn.Pass の管理
  - o 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。

Vault       Settings         Q. Search vault       Image: Comparison of the support of the supor		B	* 0
Q. Search vault         ALL       1         Image: passwords       Image: Passwords	Vault	<b>Č</b> Settings	
ALL 1 every github.com customer.support@authentrend.com	<b>Q</b> Search vault		
€ github.com customer.support@authentrend.com	ALL		1
Manage Passwords	<b>github.com</b> customer.support@authentrend.com		Ċ
Manage Passwords			
	Manage Passwords		

- o 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"

Q. Search vault			3 🕂 🕲
😋 github.com 😁	customer.support@authentrend.com ·····	• 7 ×	*

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: <a href="https://authentrend.com/atkey-pro/">https://authentrend.com/atkey-pro/</a>