ThinC-AUTH

(指紋端末認証 USB)

Powered by

ENSURITY
TECHNOLOGIES

目次

1 はじめに

ThinC-AUTH は、ユーザー認証のための USB ドングル(デバイス)です。このデバイスのハードウエアは、高い安全性を持つ組み込み部品を利用して“セキュリティ”のコアとして設計、開発と実装がされています。ThinC-AUTH は、キー、証明書、トークン、およびユーザー情報の生成や保護をハードウエアをベースとしたセキュアエレメントを使用して行っています。ThinC-AUTH にはセキュリティ層が追加されるため、デバイスに保管される暗号化されたデータのセキュリティレベルが向上しています。

ThinC-AUTH デバイスは、最先端の指紋認証用タッチ/スワイプセンサーを核とした OEM 製品を使用しています。センサーから取得した指紋データは、すべて暗号化されて安全に保管されます。ThinC の指紋認証セキュリティは、登録したユーザーだけがデバイスへアクセスできるように強力に制御しています。このタッチセンサーはたいへん感度の高いものです。ThinC-AUTH は、登録された指紋とデバイスのロックをハードエウアで解除し、FIDO2 / U2F プロトコルにて安全にユーザー認証します。

安全なチップセットと高度なハードウェア技術が、FIDO2 / U2F 認証を迅速に処理します。高速タッチ指紋認証エンジンは、高速に登録指紋との照合を実行し、ThinC のロックを解除し、FIDO2 / U2F 認証します。指紋とデジタル ID はデバイス内に秘密情報として高度な暗号化によって保管されています。ThinC-AUTH は、FIDO (Fast IDentity Online) U2F (Universal Second Factor) / FIDO2 に準拠しているため、認証器の機能は非常に多数の応用に利用できます。

デバイスの管理と指紋登録用に、独立動作のダウンロード可能な管理用ソフト ThinC-Manager が用意されています。このデバイスは堅牢な金属製の筐体でできていて、何回も USB 抜き差し（プラグイン - プラグアウト）をした後でも長く性能が持続するように設計されています。更に、欧米 FCC / CE 商品規格の認定を受けています。

ボード生体認証
（5 指登録可能）

AES-256 ハードウエア暗号（企業向け信頼）

暗号標準
FIPS140-2
レベル 2 準拠

FIDO2/U2F 準拠
（プライバシー設計）

注- ThinC-FIDO2/U2F は、ThinC-AUTH に名前が変わりました。

1.1 ハードウエア仕様

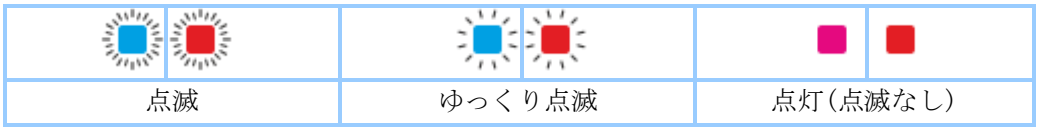
以下の表は ThinC-AUTH デバイスの使用を示しています。.

番号	特徴	仕様/記述
1	接続	• 高速 USB 2.0
2	指紋認証	• タッチ指紋センサー • 最大 5 指登録可能
3	暗号	• 登録指紋の暗号：AES-256 • チップ内ダイナミック暗号/トークン鍵生成 • 暗号基準 FIPS 140-2 Level 2 準拠設計
4	認証標準	• FIDO 2.0 • FIDO 1.2 U2F
5	物理的な強度	• 1 万回抜き差し可能
6	動作環境	• 保存温度: -40° C ~ 85° C • 動作温度: -5° C ~ 55° C • 動作電圧: 4.9V ~ 5.1V
7	指紋登録ソフトウエア	動作ＯＳ: • マイクロソフト® Windows® 7 以上のデスクトップ版 • アップル® Mac OS® 10.12 以上
8	ＥＭＣ試験	• EN 55032:2015 (Class B) • EN 55024:2015 • EN 61000-4-2:2009 (contact: level 2 (±4kV), air: level 3 (±8kV)) • EN 61000-4-3:2006+A2:2010 (80-1000MHz, level 2 (3V/m)) • EN 61000-4-8:2010 (level 2 (3A/m), continuous field) • FCC Part15 subpart B: 2018 (Class B)

1.2 LED 表示

以下の表はデバイスを USB 端子に差し込み電源オンした後の LED 表示を示しています。

機能	意味	LED 表示	説明
電源オン	-		標準, 1-2 秒
自動テスト	-		自動テスト　成功
	-		自動テスト　失敗
指紋認証	待機中		標準タイムアウト - 30 秒.
	認証中		
	成功		標準, 1-2 秒
	失敗		
登録指紋削除	成功		
	失敗		
出荷時初期化	成功		
	失敗		
	リセット後		USB 抜き出した後



2 管理ソフト ThinC Manager

ThinC - Manager は、ThinC 製品群を管理するためのスタンドアロンツールです。
ThinC Manager は以下のリンクからダウンロードできます。インストーラをメールで受け取るには、件名が "Send Tool - Windows"または "Send Tool - Mac"の Microsoft Windows 用および Apple macOS ベースのツールを使用して、*thinc.support@ensurity.com* に電子メールを送信してください。

- https://x.co/tctools
- https://manage-thinc.ensurity.com/download

このマニュアルのこのセクションでは、マイクロソフト®Windows®およびアップル macOS 用の ThinC Manager のインストールプロセスについて説明します。ThinC Manager は、指紋の登録と ThinC-AUTH Secure USB の管理に必要なソフトウェアです。
デバイスを利用するには、2 つのステップで行います。

1) 登録ソフトウエアによるユーザー指紋を ThinC デバイスへ登録
2) 利用するサービスアプリへの ThinC デバイスの登録。

2.1 マイクロソフト® Windows®OS 用

ThinC Manager は、ThinC シリーズのセキュア USB デバイスを管理するためのソフトです。このツールを使用して、デバイスの設定、指紋の管理、さまざまなデバイスの設定/リセットを行うことができます。ThinC Manager のインストーラは、下記の URL または Web リンクからダウンロードするか、「ThinC tool-Windows」という件名で thinc.support@ensurity.com まで連絡ください。管理ソフト ThinC Manager が電子メールで送付されます。

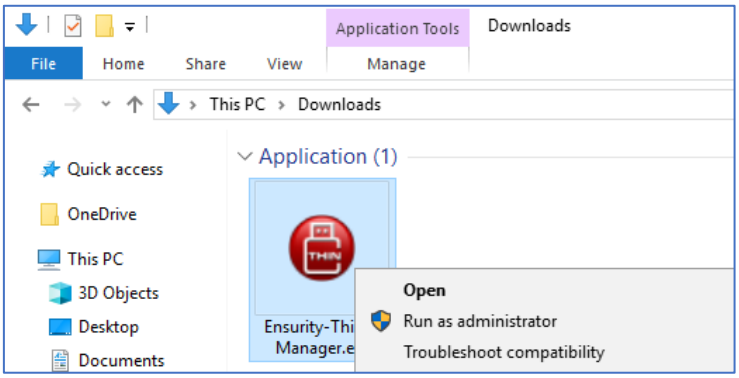
Microsoft®Windows®ＯＳ（オペレーティングシステム）用の ThinC Manager インストーラをダウンロードしてください。

ステップ 1:

ダウンロードファイルを開いて、インストールウイザードを開始してください。

マイクロソフト® Windows® 8 / Windows® 10 またはそれ以上にインストールする途中に、 Microsoft Smart Screen protector により、許可のためのウインドウが現れる場合があります。“実行”またはそれと同等な必要な許可を与えてください

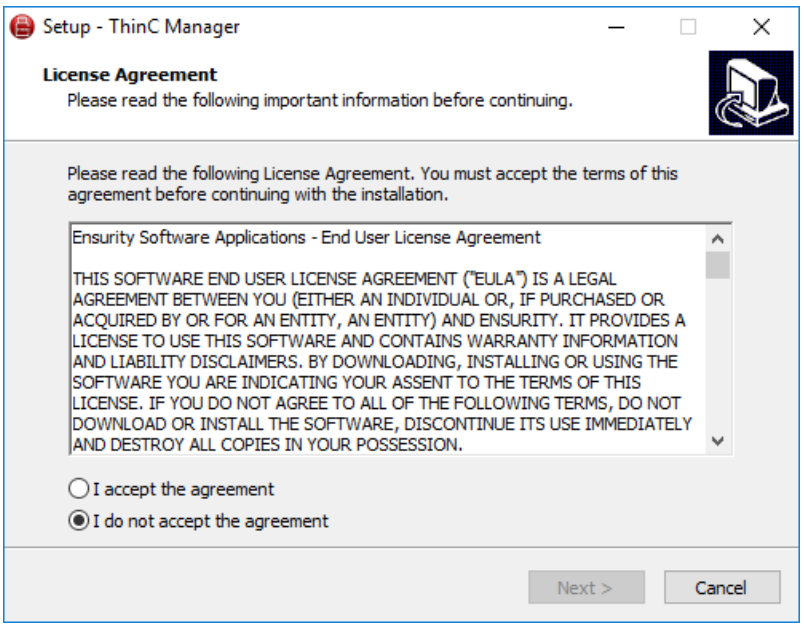
ユーザーアクセス制御/ウイルス対策/ End Point Protector ソフトからインストールを承認するように要求される可能性があります。インストール中に表示される可能性のあるそのような要求を許可することをお勧めします。



ダウンロードされたインストールツールを表示する典型的なウィンドウ

ステップ 2:

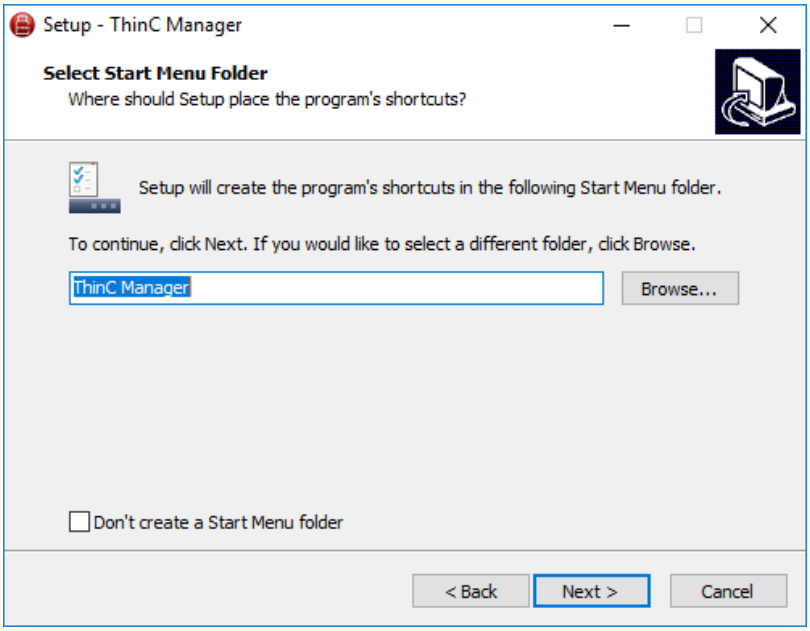
- ThinC Manager インストーラを開いた後、使用許諾契約書のウィンドウが表示されます。 Ensurity ソフトアプリ- エンドユーザー使用許諾契約書をよく読み、[同意する]をクリックして同意することを選択し、[次へ]をクリックしてウィザードを進めてください。インストールプロセス中にキャンセルを選択すると、インストールが中止されます。



ステップ 3:

- [スタート]メニューの[フォルダの選択]ウィンドウには、Windows の[スタート]メニューにショートカットを配置する場所を選択するオプションがあります。デフォルトでは、ツールショートカットはスタートメニューフォルダに作成されます。 「スタートメニューフォルダを作成しない」にチェックを入れると、ショートカットの作成をスキップできます。

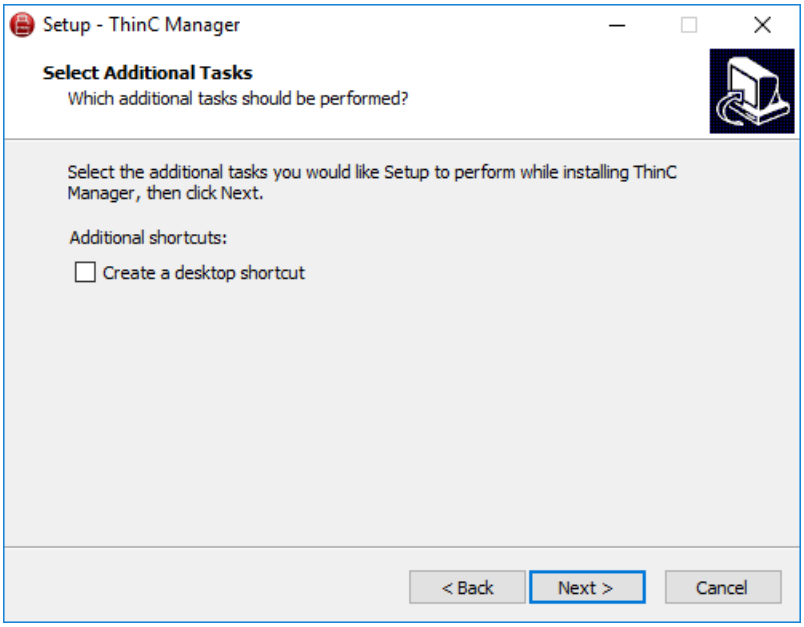
- [次へ]をクリックしてインストールウィザードを続行します。



ステップ 4:

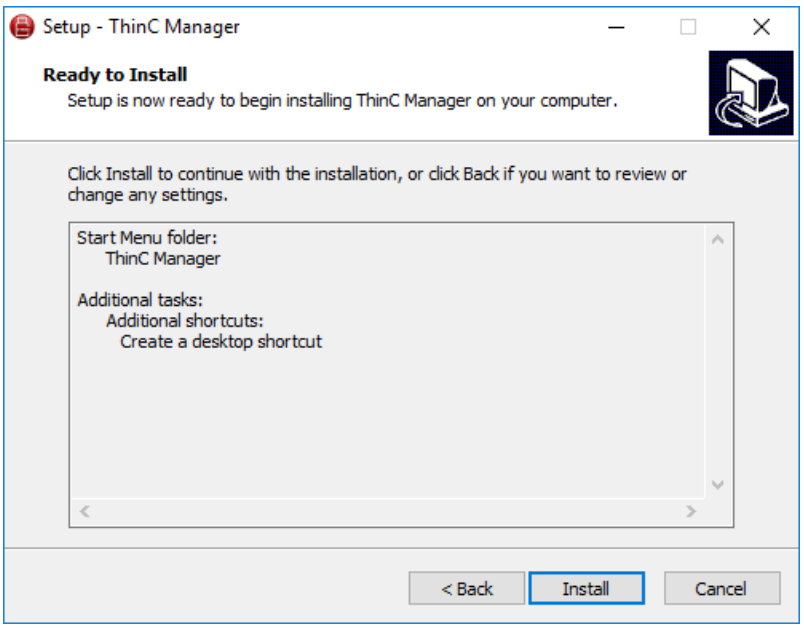
- [追加のタスク]ウィンドウを選択すると、Windows デスクトップにショートカットを配置する場所を選択するオプションが表示されます。デスクトップショートカットが

必要な場合は、[デスクトップショートカットの作成]チェックボックスをクリックしてから、[次へ]をクリックします。



デフォルトでは、このツールは ″C：¥Program Files (x86) ¥ThinC Manager″にインストールされます。 [デスクトップショートカットの作成]チェックボックスをオフにしてデスクトップショートカットの作成をスキップした場合は、デフォルトの場所に移動して ThinC.exe を見つけてアプリケーションにアクセスします。

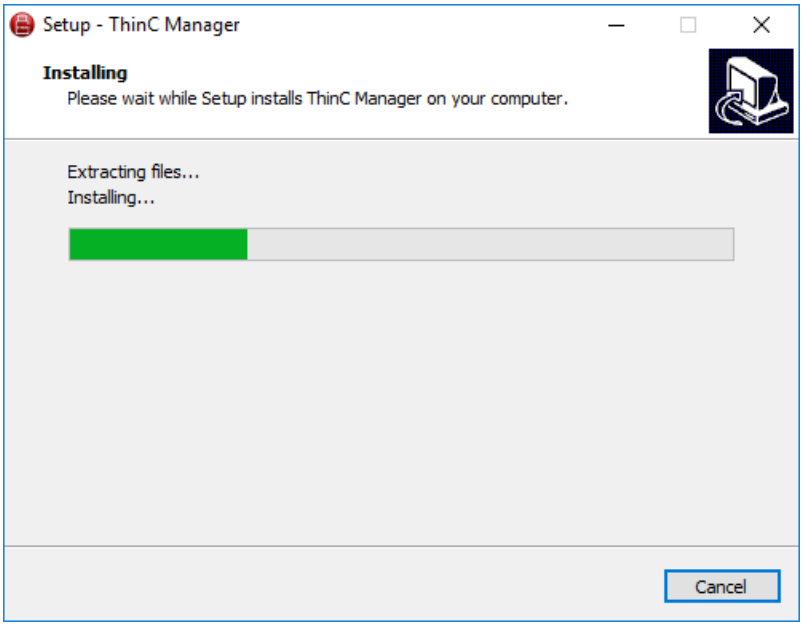
- [インストール準備完了]ウィンドウに、手順 3、4、5 で行った選択の概要が表示されます。変更が必要な場合は、[戻る]をクリックして必要な変更を行います。 [インストール]をクリックして、コンピュータに ThinC Manager のインストールを開始します。



ステップ 5:

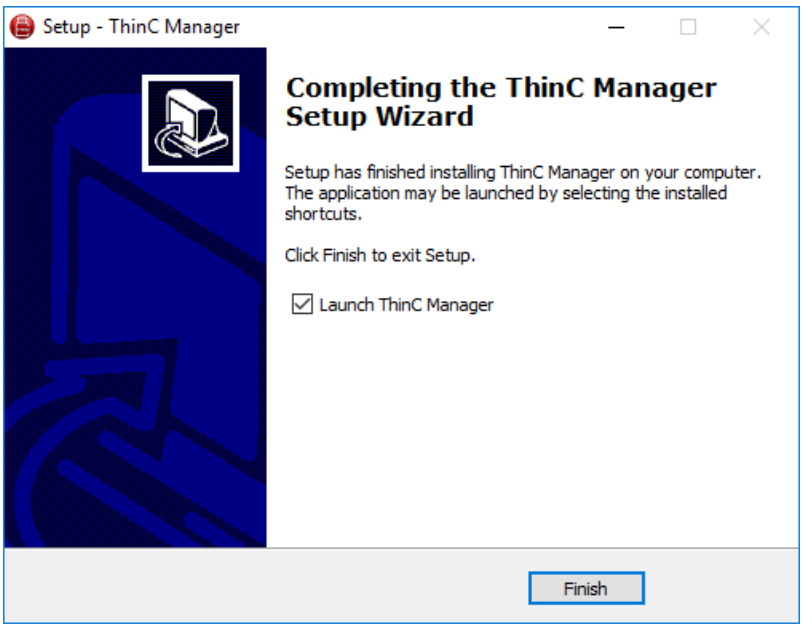
- [インストール]ウィンドウにインストールの進行状況が表示されます。キャンセルをクリックすると、このプロセスを中止することができます。

インストールが停止または中止された場合、ツールはインストールされません。



ステップ 6:

- インストールが正常に完了したら、[完了]をクリックします。



[完了]をクリックしてインストールを完了し、すぐにツールを起動します。 [Launch ThinC Manager]の選択を解除し、[完了]をクリックして後でツールを開いて使用します。

デスクトップショートカット/スタートメニューのショートカットを使用して/ ThinC Manager を開くためのインストールパスに移動します。

インストール中に問題やエラーが発生した場合は、*thinc.support@ensurity.com* にサポートに連絡するか、thinc.ensurity.com のテクニカルサポートにお問い合わせください。

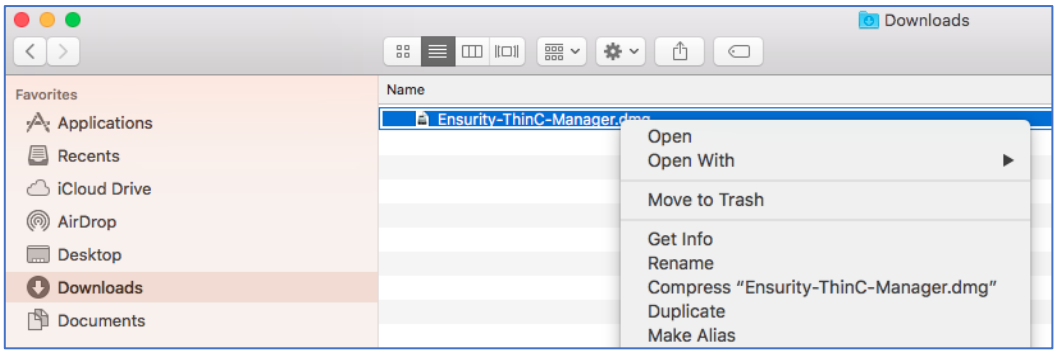
2.2 アップル® Mac®用

ThinC Manager は、ThinC シリーズのセキュア USB デバイスを管理するために提供されるソフトです。このツールを使用して、ユーザーはデバイスの設定、指紋の管理、さまざまなデバイスの設定/リセットを行うことができます。 ThinC Manager のインストーラは、下記の URL / Web リンクからダウンロードするか、 "ThinC tool - Mac"という件名で *thinc.support@ensurity.com* までご連絡ください。管理ソフト ThinC Manager が電子メールで送付されます。

Apple®Mac®ＯＳ（オペレーティングシステム）用の ThinC Manager インストーラをダウンロードしてください。

ステップ 1:

- ダウンロードした ThinC-Manager.dmg ファイルを開いてインストールウィザードを開始します。 DMG ファイルを開いて ThinC Manager のインストールを開始します。

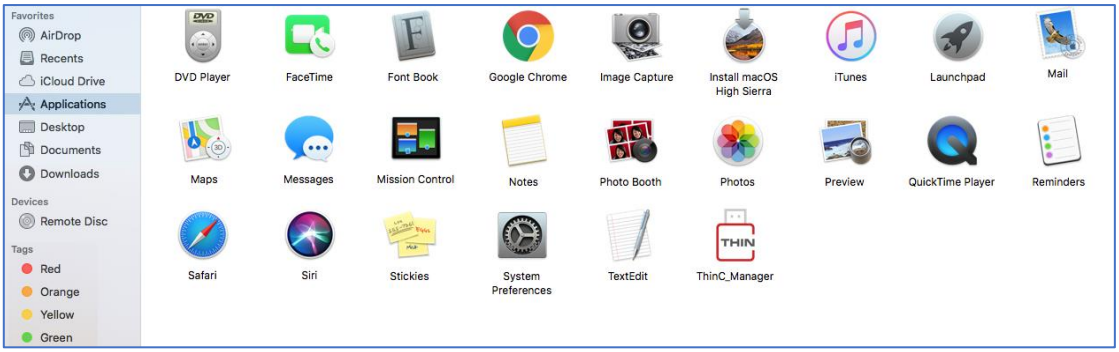


ステップ 2:

- ThinC ツールウィンドウで、ThinC ファイルをドラッグして Application フォルダにドロップすることを選択します。アプリケーションフォルダに移動し、「ThinC」を確認します（そうでない場合はプロセスを繰り返します）。

ステップ 3:

- [アプリケーション]フォルダに移動するか、[ThinC]を検索して[ThinC]を実行し、ThinC Manager を起動します。



2.3 アンインストール

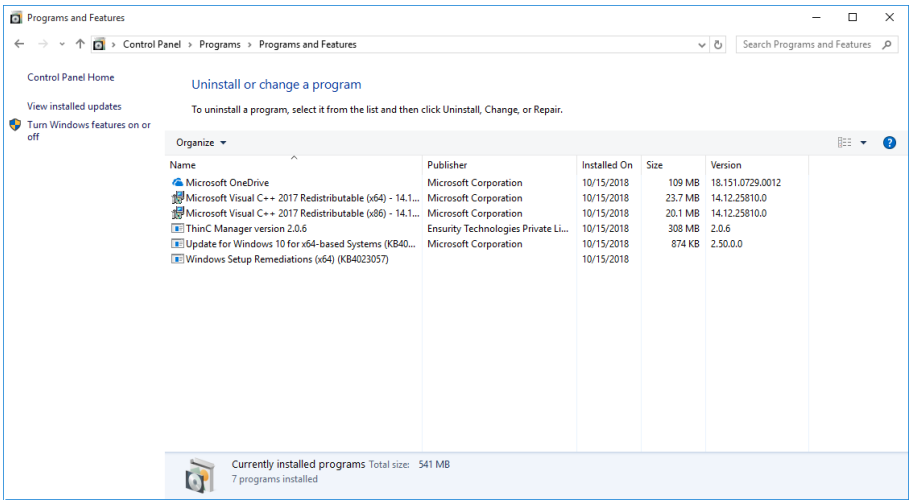
この文書では、Windows とMacOS から管理ソフト ThinC-Manager をアンインストールする方法について説明します。

2.4 マイクロソフト® Windows®OSからのアンインストール

以下の手順が、WindowsOS から ThinC Manager をアンインストールする方法です。

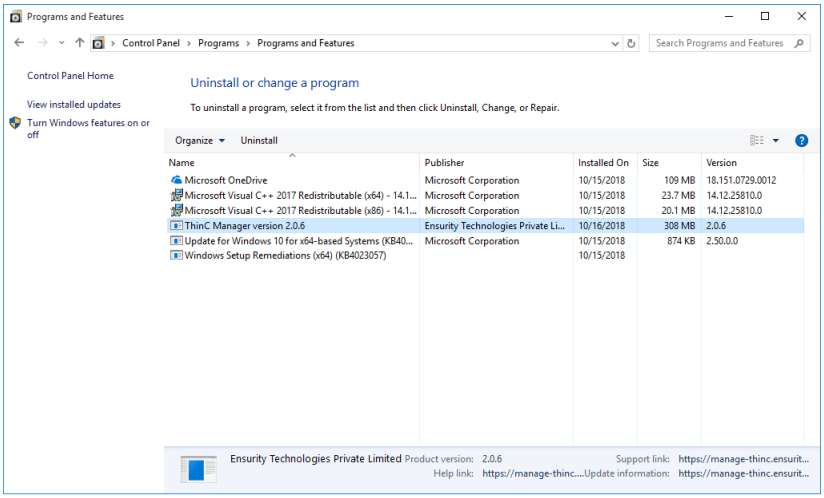
ステップ 1:

- Windows の[コントロールパネル]> [プログラムと機能]に移動します。またはコントロールパネル>プログラムをアンインストールします。



ステップ 2:

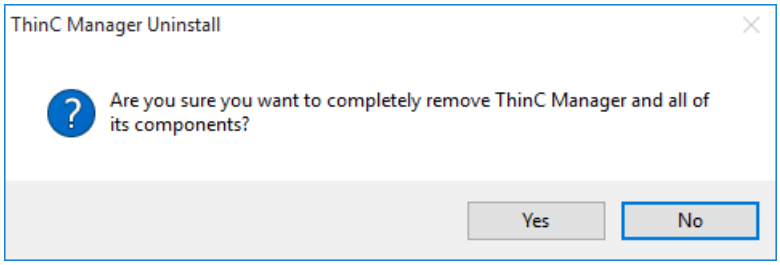
- [ThinC Manager version x.y.z]を選択し、[アンインストール]または[アンインストールと変更]をクリックします。



Microsoft でのアンインストールが始まる前に、Windows は管理ソフト ThinC Manager をアンインストールする許可を要求します。同意する場合は、[はい]をクリックすると、アンインストールが続行します。

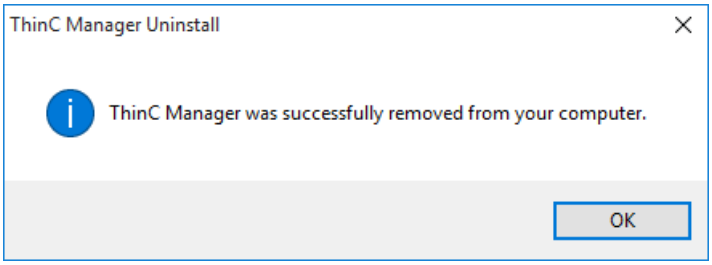
ステップ 3:

- 管理ソフト ThinC Manager のアンインストールのウィンドウで、アンインストールを本当に行うのか再確認されます。続行するには、はいを、中止するには、いいえを選択します。



ステップ 4:

- インストーラは、インストールされたディレクトリから ThinC Manager のインストール済みファイルを削除または削除します。アンインストールが終わり、「ThinC Manager はコンピュータから正常に削除されました」と表示されたら、Ok を押してアンインストールを完了します。アンインストール中に問題が発生した場合は、件名が"Uninstall-Windows"として *thinc.support@ensurity.com* にご連絡ください。

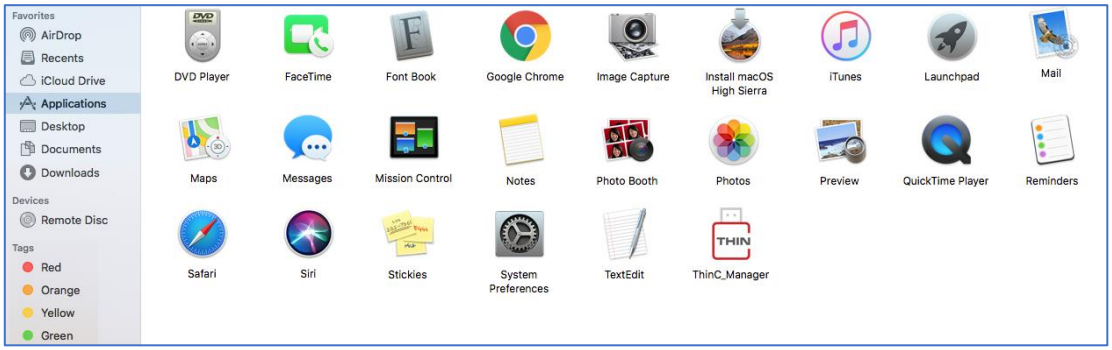


2.5 アップル® macOS からのアンインストール

MacOS 用 ThinC Manager をアンインストールには以下のステップで行ってください。

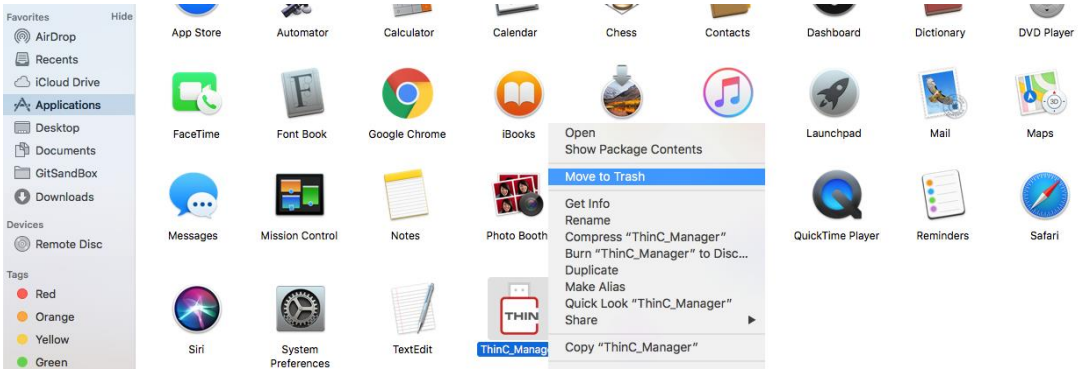
ステップ 1:

· [アプリケーション]フォルダに移動して[ThinC Manager]を選択します。



ステップ 2:

- 右クリックして[ゴミ箱に入れる]を選択します。ツールを完全に削除するには、ゴミ箱を空にしてください。アンインストール中に問題が発生した場合は、件名 "Uninstall-Mac"にして *thinc.support@ensurity.com* にご連絡ください。



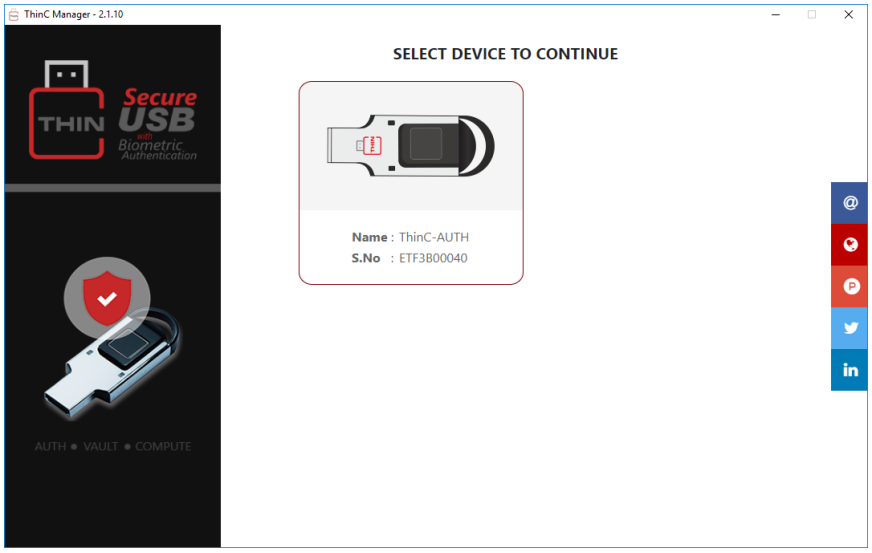
3　管理ソフト ThinC Manager の機能

Manage ThinC-AUTH USB

ThinC Manager は、ThinC-AUTH USB デバイスを管理するために必要なソフトウェアユーティリティです。管理ツールは３つのサブウィンドウ、すなわち１）指紋２）設定３）ＦＡＱおよび切断ボタンを有する。ThinC Manager ツールを使用してユーザーをデバイスに登録した後、デバイスを FIDO / U2F サービスの認証器デバイスとして使用できます。それ以降のプロセスに進む前に、ツールが必要なコンピュータに以前の指示に従ってインストールされていることを確認してください。ThinC-AUTH の管理を開始するには、コンピュータの USB ポートへの接続して、デバイスの電源を入れて初期化し、指紋の読み取りまたは指紋の登録を行います。

デバイスのさまざまな状態を理解するには、LED 表示の表を参照してください。
デバイスの初期化中は、指紋センサーに指を触れないでください。

- ThinC Manager アプリを開き、管理する必要があるデバイスをクリックします。アプリは、接続されている ThinC デバイスを自動的に検索、認識、および一覧表示します。



- デバイスが正しく接続されていないか、コンピュータで動作しない場合は、次の画面が表示され、ユーザーにデバイスの再接続を促します。それでも認識されない場合は、thinc.support@ensurity.com にお問い合わせください。

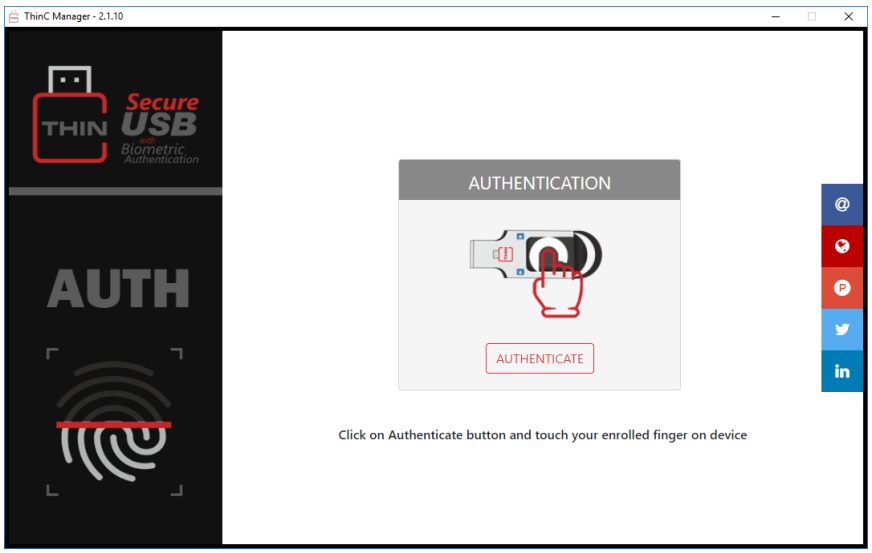
ThinC-AUTH デバイスは、最大の登録指紋数は 5 です。

3.1 指紋管理

ThinC Manager には、フレッシュ/リセット/未登録のデバイスと指紋登録済みのデバイスを自動的に区別する機能があります。指紋登録されたデバイスの場合は、登録ユーザーが ThinC Manager の管理を開始する前に指紋認証が必要です。以下のステップ 1 は、指紋が登録されたデバイスの管理機能にアクセスするためのプロセスを提供します。フレッシュ/リセットデバイス/初回登録についてはステップ 2 を参照してください。

ステップ 1:

- ［認証］をクリックして、既に登録されている指を置きます。認証が成功すると、指紋管理ウィンドウへアクセスできます。フレッシュ/リセット/未登録のデバイスですと、このステップは自動的にスキップされます。

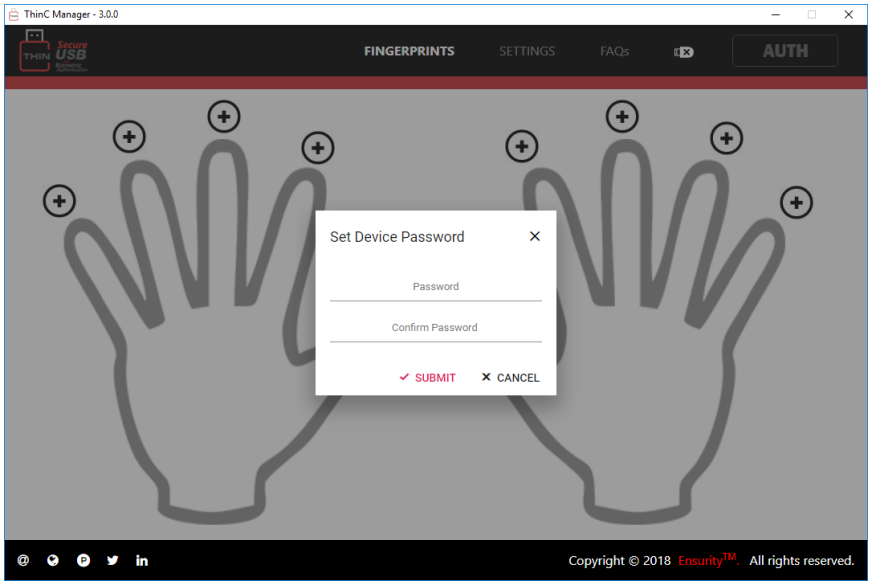


ツールは自動的にステップ２に進み、新しいフレッシュ/リセット/未登録のデバイスの初期認証プロセスを開始します。

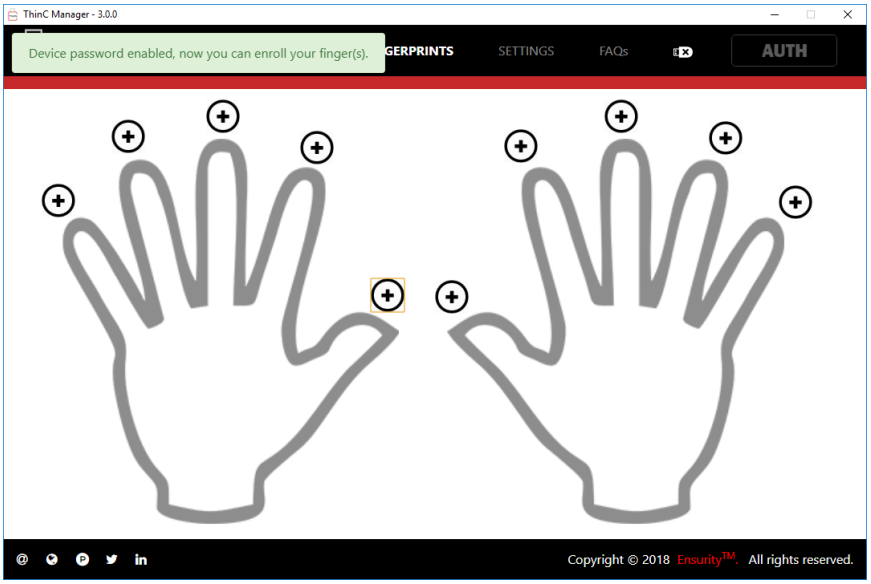
ステップ 2:

- パスワードも利用するには、指紋管理ウィンドウでプラス/追加アイコンをクリックすると、ポップアップのメニューが現れ、デバイスパスワードを設定します。パスワードを入力して、更に同じパスワードを再度入力で確認し、送信をクリックします。

詳細についてはパスワード管理のセクションを参照してください。



- 「デバイスパスワードが有効になりました。今すぐ指紋を登録できます」というポップアップが表示されます。

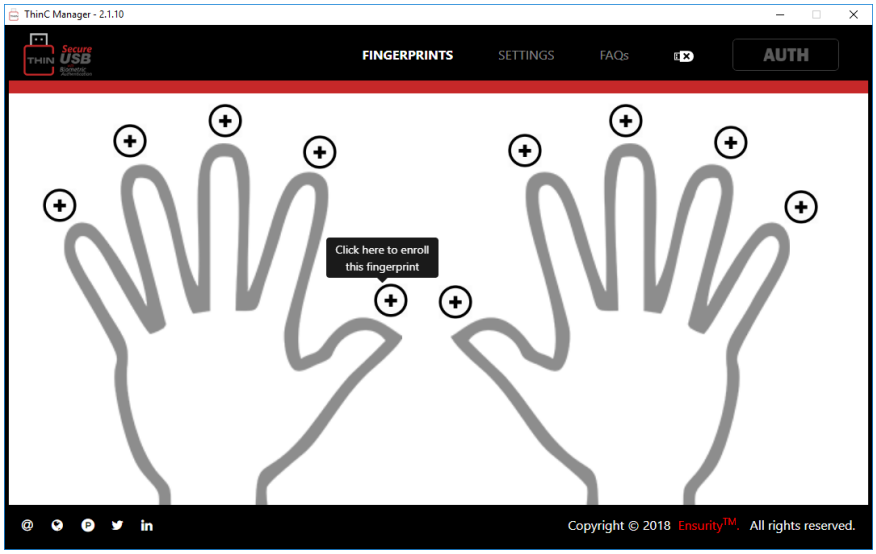


3.1.1 指紋登録

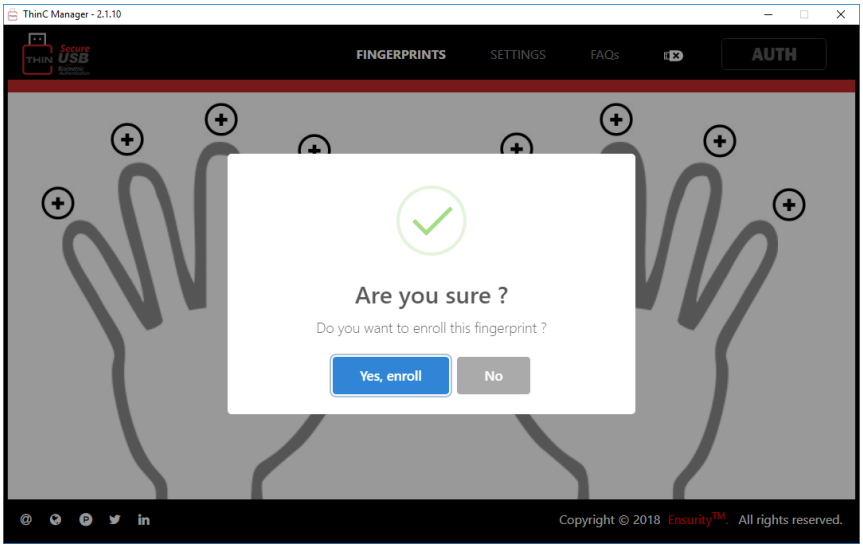
ステップ 3:

- 指紋管理ウィンドウは指の登録のために選択する 10 指分のスロットを提供します。

  指紋を登録するには、プラス/追加アイコン⊕をクリックして、好みの指スロットを選択します。



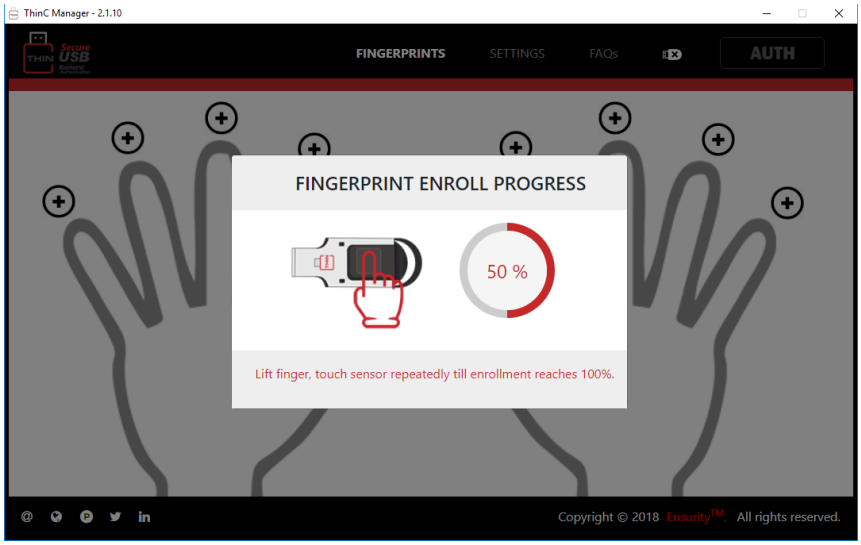
- 登録プロセスを開始するには、[はい登録]をクリックします。[いいえ]をクリックして登録プロセスを中止します。



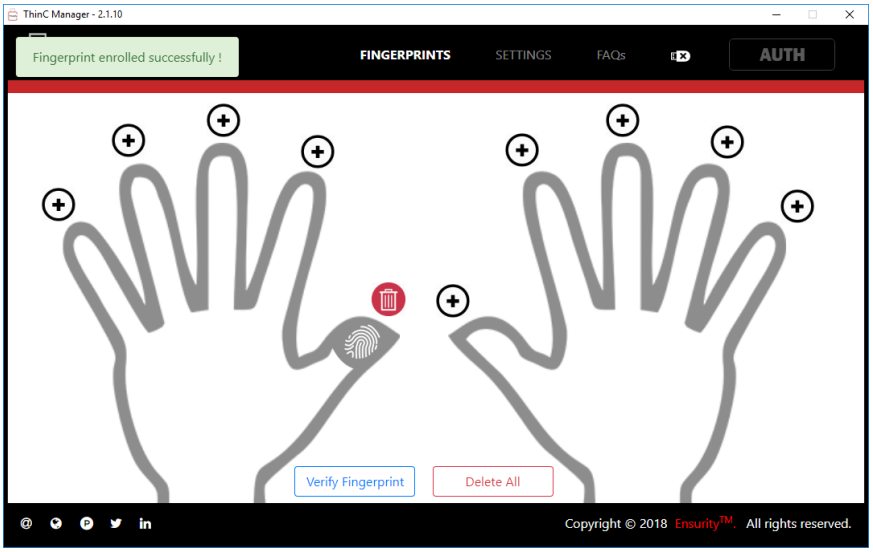
後で混乱を最小限に抑えるために、指定された指紋スロットに別の指を使用しないでください。登録されているすべての指紋は、ThinC-Auth デバイスに安全に保存されています。

指紋やデバイスアクセス情報は管理ツールに保存されません

- 選択した指を指紋センサーに置いて登録プロセスを繰り変えします。登録プロセスが100%に達するまで指を指紋センサーに複数回置く必要があります。指をすばやく登録するための最良の方法は、毎回わずかに異なる角度で指を配置します。



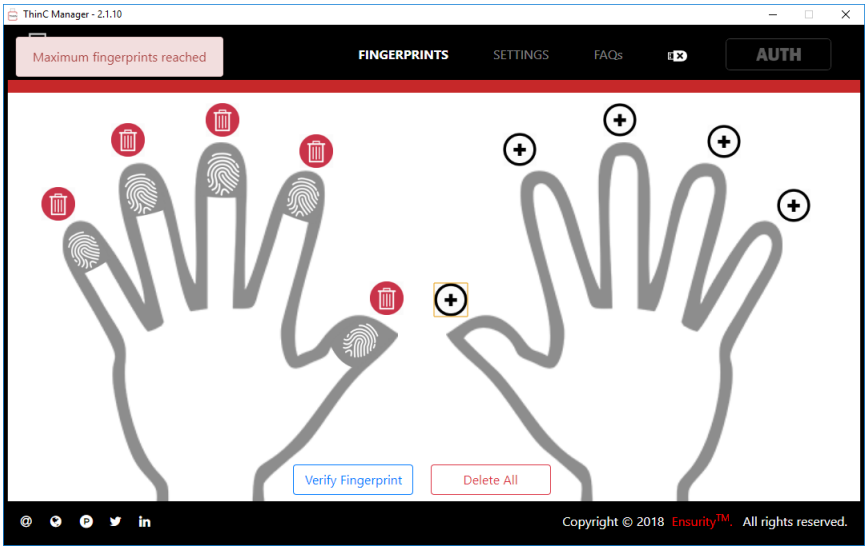
- 指紋登録が正常に完了した後、「指が正常に登録されました」というメッセージを表示し、画面が更新されます。



⊕シンボルのついている指が登録可能な可能な指紋スロットを表示しています。

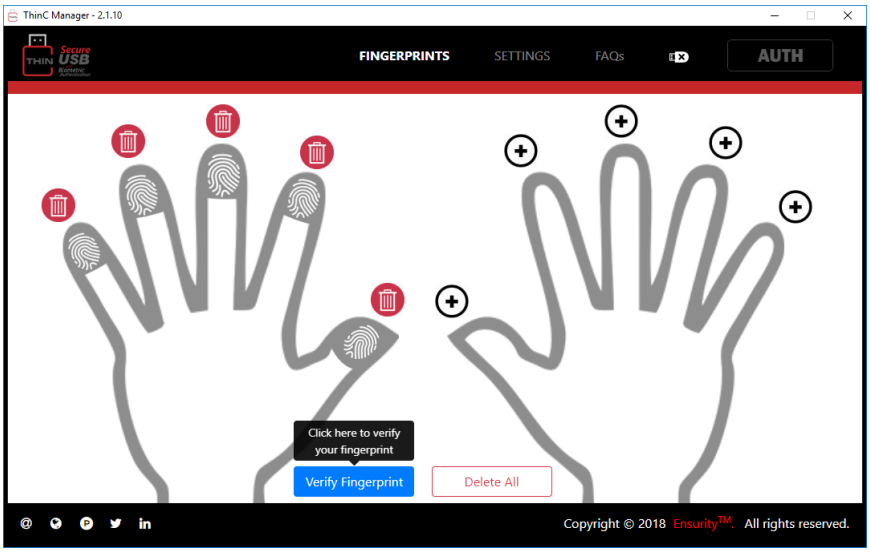
すでに登録されている指紋スロットは、  か  のアイコンで管理ツールの指の画像に表示されます。

指の登録には最大5スロットが利用可能です。これらのスロット数を超えていると、登録終了時の「Finger Successfully Enrolled」の代わりに、「Number of slots exceeded」を通知します。

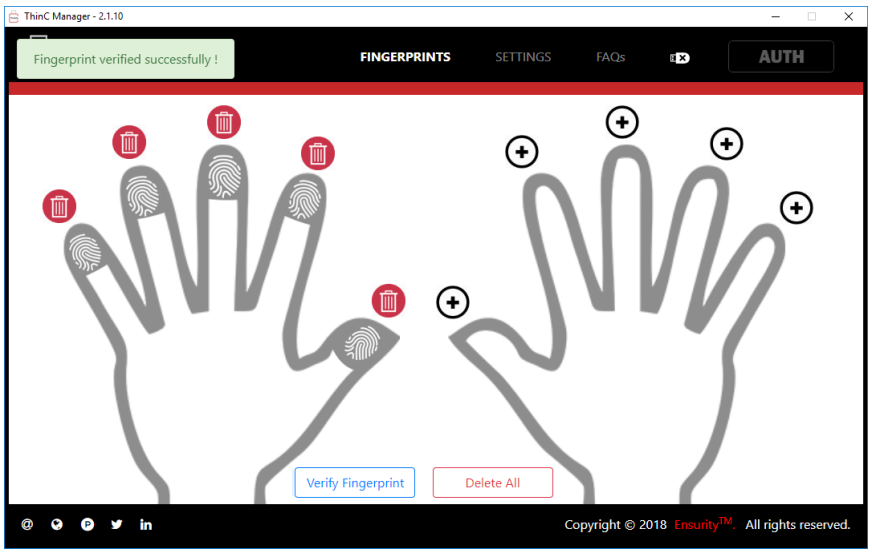


ステップ 4:

- 指の認証は、通常の方法で[指の認証]オプションを使用して登録された指紋を認証することを選択してください。指紋管理ウィンドウで、指の確認をクリックして指をセンサーに置きます。



- 指紋が登録された指と一致する場合は「認証に成功しました」、一致しない場合は「認証に失敗しました」と通知することでツールは自動的に検証を開始し、結果を提供します。

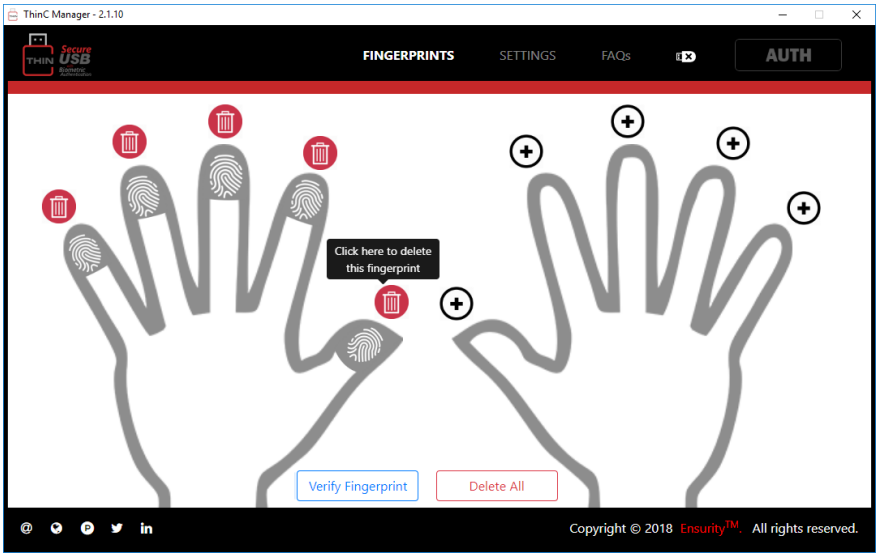


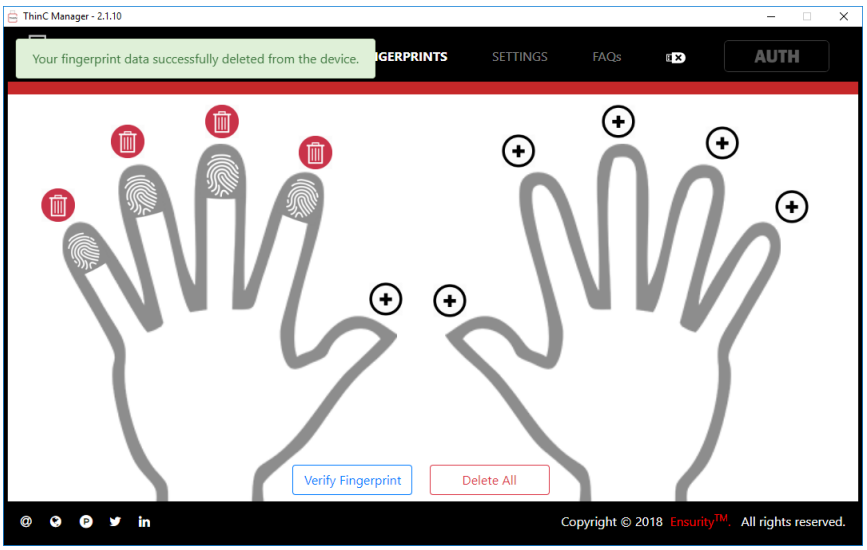
3.1.2 指紋の削除/ 登録解除:

指紋管理は、個々の指紋の削除/登録解除、またはすべての削除を可能にします。

個人指紋の登録解除

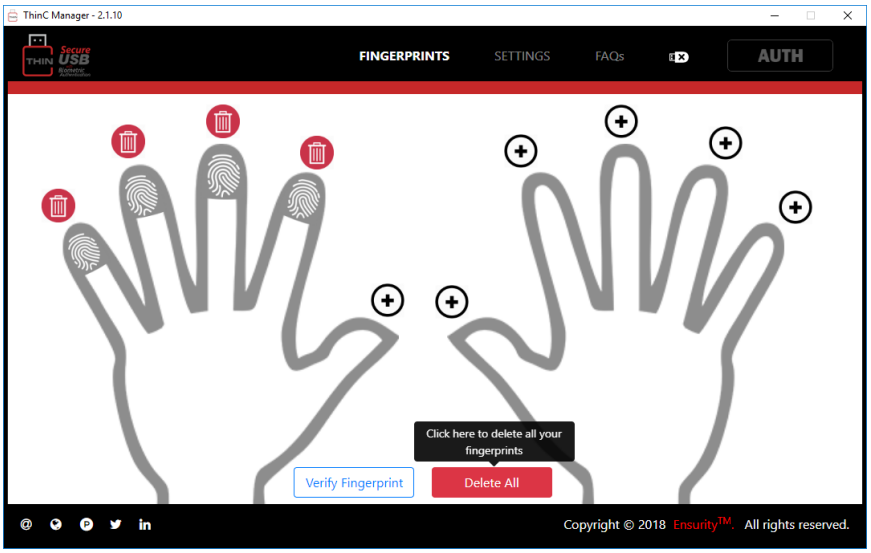
- 指紋管理ウィンドウで指紋を削除/登録解除するには、指定されたスロットの[削除/ゴミ箱アイコン]をクリックします。指紋の削除に成功すると、「あなたの指紋データはデバイスから正常に削除されました」という通知が表示されます。

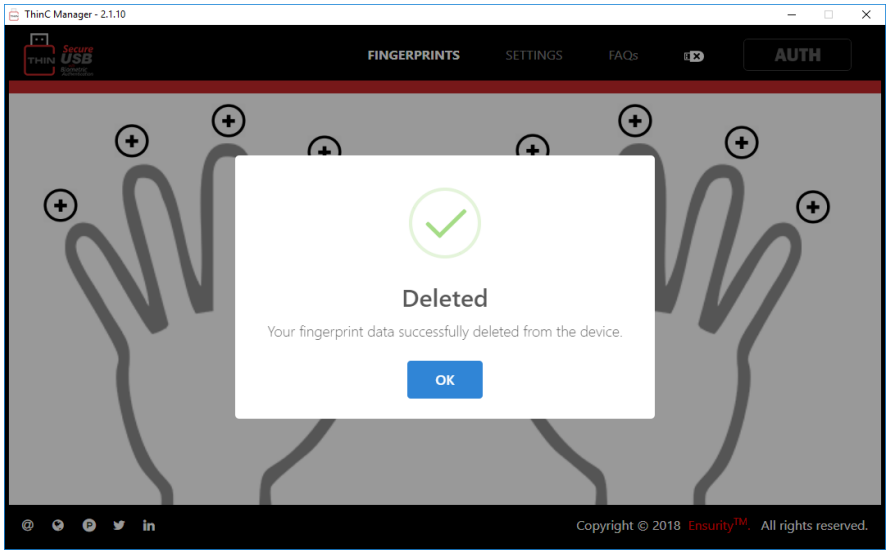




すべての登録指紋の削除

- すべての指紋を削除するには、画面の下部にある[すべて削除]ボタンを選択します。このオプションを使用すると、登録されているすべての指紋をデバイスから完全に削除できます。すべての指紋が正常に削除された後、「あなたの指紋データはデバイスから正常に削除されました」というポップアップウィンドウがツールによって表示されます。





⚠ *警告：FIDO サービスアプリから登録を解除せずにデバイスから指紋を削除すると、アクセスできない状況が発生する可能性があります。*

3.2 パスワード管理

ThinC Manager 管理ソフトは、ThinC-AUTH デバイスとの間の通信により、デバイスに保存されている指紋を管理する指紋管理機能を備えています。この管理機能には、指紋の登録、削除、空き/占有の指紋登録領域の一覧表示、登録指紋のチェックなどがあります。

指紋は、偶発的な損傷（例えば、指を切る）や、特定の病気のため指紋の損傷を引き起こす可能性のあることは良く知られています。それは、本人の意図でなく認証を試みたり、湿度の高い環境で操作したり（デバイス上の高湿度/結露）、わざと検知されないような試みであったり、手の指紋の色褪せなどの職業上の問題（例：建築工事）などの可能性もあります。これらの条件は、認証やデバイス操作のために指紋が利用できないような状況を生み出してる可能性があります。このような状況をバックアップするために、ThinC-AUTH はデバイスを管理するためのパスワードを利用した認証を提供しています。

3.2.1 パスワード設定

指紋を登録する前に、デバイスは認証バックアップ用のパスワードの設定ができます。

パスワードの最小および最大長は 4 から 32 文字です。

ℹ *認証に 3 回失敗した後でデバイスを使用するには、一度デバイスをコンピュータから切り離して、再度接続する必要があります。*

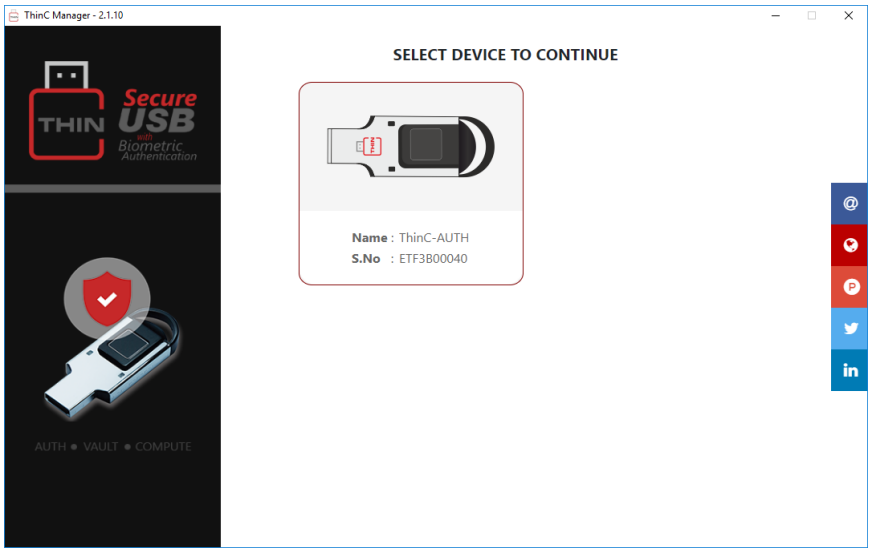
次の表は、デバイスのロックを有効にするシナリオを示しています。

番号	指紋認証失敗	起きるロック状態	ロック解除方法	**ロック状態での利用できない機能**
1	ThinC-Manager ツールのログインプロセス中に 3 回連続して失敗した場合	ThinC-AUTH ファームウェアは、デバイスの設定変更をロック/制限します。ThinC-Manager のユーザー設定パスワードを使用して、デバイスのロックを解除する必要があります。	1. ロックされた ThinC-AUTH をパソコンに接続 2. ThinC-Manager 起動 3. 本ドキュメントのデバイスのロック解除操作に従う。	1. デバイスの設定と管理 2. 指紋の管理
2	FIDO / U2F Web サービスのログインプロセス中に 5 回連続して失敗した場合	ThinC-AUTH は、登録済みの FIDO / U2F /認証サービスにデバイスの使用をロックします。ThinC-Manager のユーザー設定パスワードを使用してデバイスのロックを解除する必要があります。	1. ロックされた ThinC-AUTH をパソコンに接続 2. ThinC-Manager 起動 3. 本ドキュメントのデバイスのロック解除操作に従う。	1. FIDO /U2F の Web アプリ 2. 指紋の管理 3. 工場出荷時リセット
3	ThinC-Manager ツールのログインプロセス中に 8 回連続して失敗した場合	ThinC-AUTH のファームウェアは、デバイスの設定変更を恒久的にロック/制限します。デバイスがこの状態になった場合は、デバイスの出荷時設定へのリセットを実行する必要があります。	1. ロックされた ThinC-AUTH をパソコンに接続 2. ThinC-Manager 起動 3. 指紋の利用を続けるにはデバイスをリセットしてください。	1. デバイスの設定と管理 2. 指紋の管理

3.2.2 フレッシュ/リセットデバイス用のパスワードの設定:

ステップ 1:

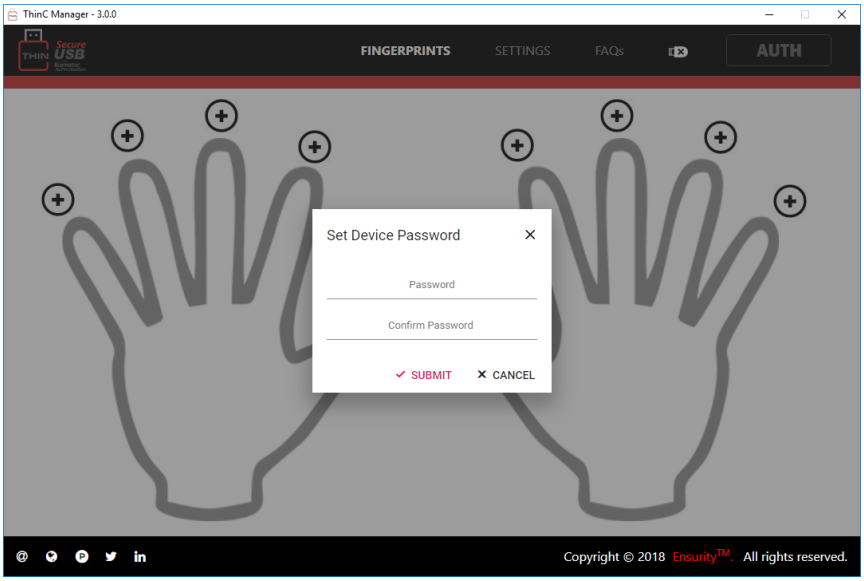
- 設定するデバイスをクリックします。



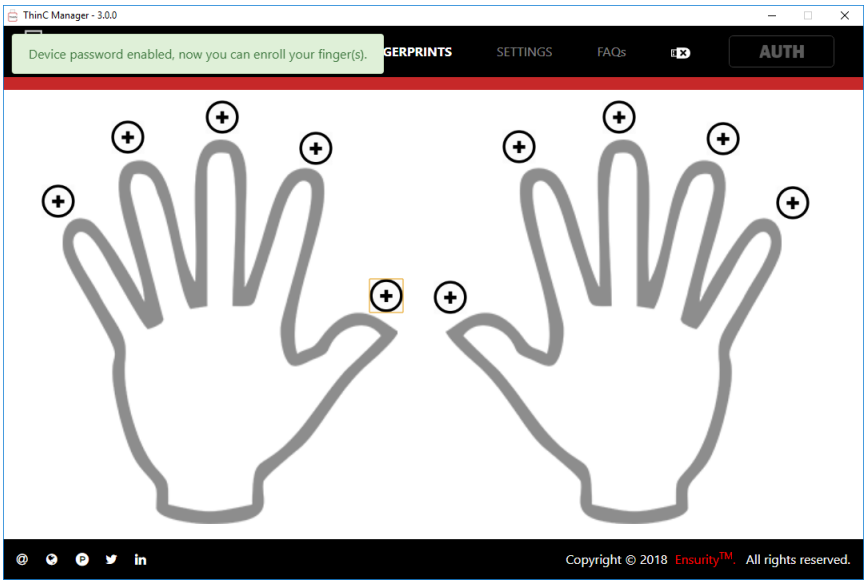
ツールは自動的にステップ 2 に進み、新しいフレッシュ/リセット/未登録のデバイスのために初期認証プロセスを開始します。

ステップ 2:

- パスワードを有効にするには、指紋管理ウィンドウでプラス/追加アイコン⊕をクリックすると、ツールがポップアップを表示してデバイスパスワードを設定します。パスワードを入力してパスワードを確認し、送信をクリックします。



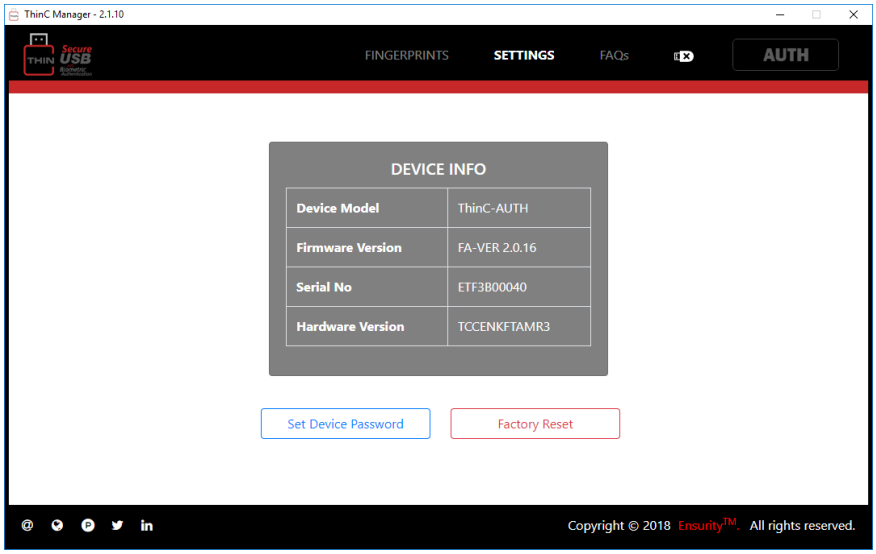
- 「デバイスパスワードが有効になりました。今すぐ指紋を登録できます」というポップアップが表示されます。



パスワードの設定後は、指紋を登録することをお勧めします。

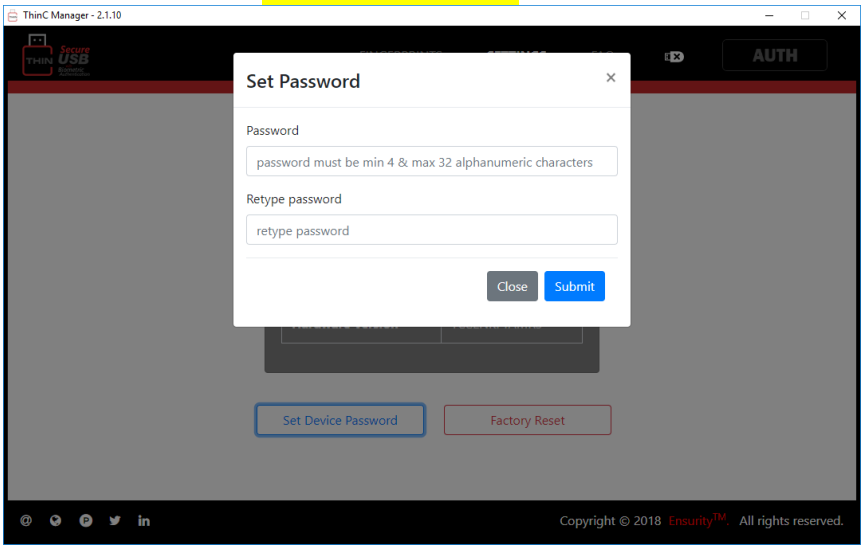
3.2.3 その他のパスワード設定方法

設定タブからパスワード設定

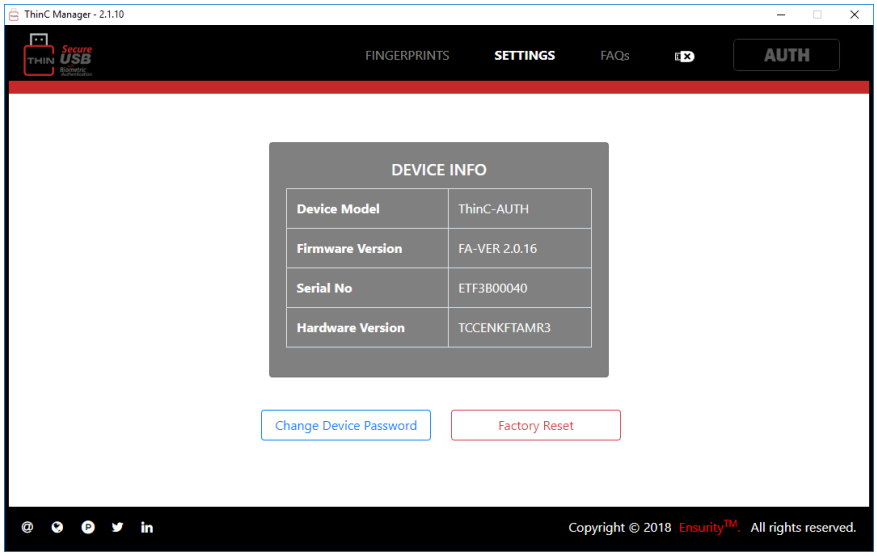


- デバイスパスワードは、ThinC Manager の[設定]タブからも設定できます。デバイスパスワードを設定するには、[設定]をクリックして[パスワードの設定]を表示し、[パスワードの設定]をクリックして同じパスワードを入力し、パスワードを再入力してパスワードを再入力して確認します。

- パスワードを設定するには、[送信]をクリックします。

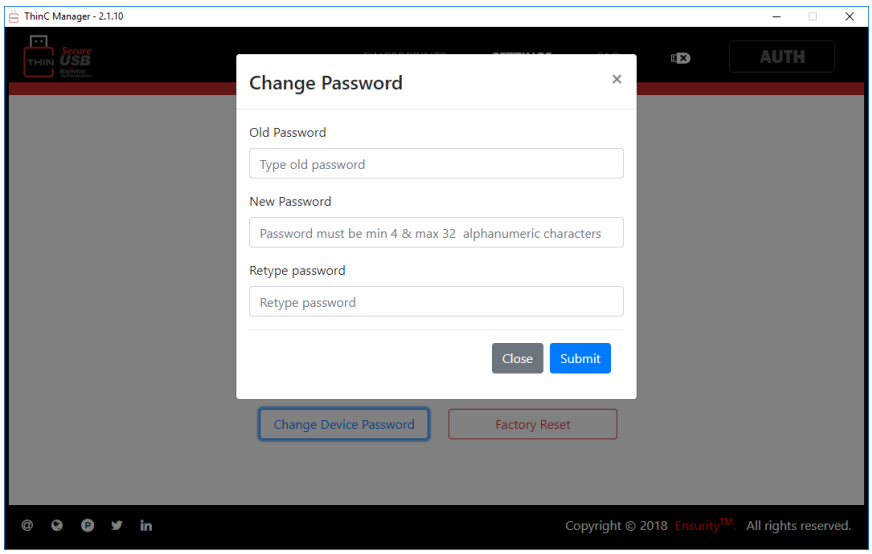


- [設定]をクリックして[パスワードの設定]を表示し、[パスワードの設定]をクリックしてパスワードを入力し、パスワードを再入力して確認します。



3.2.4 パスワードの変更

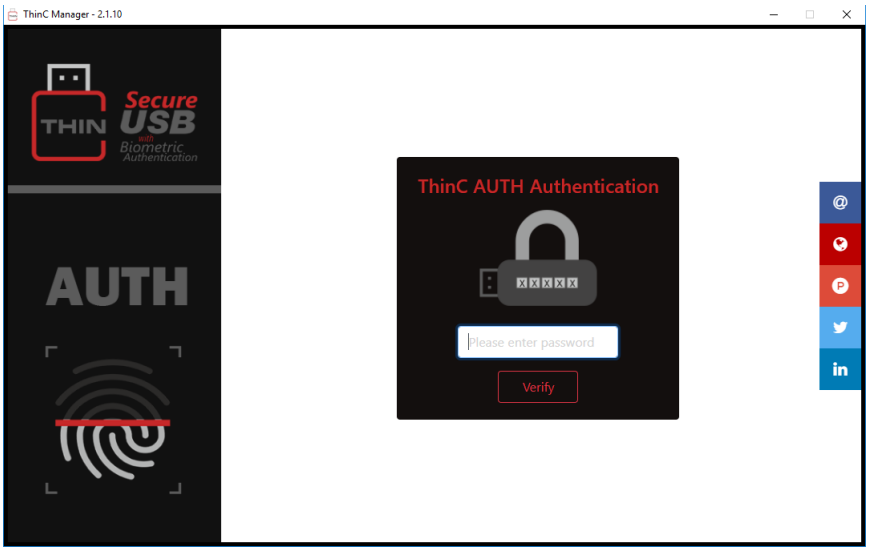
- デバイスパスワードを設定したら、ユーザーは[設定]タブからパスワードを更新できます。 [設定]をクリックして[パスワードの変更]を表示し、[パスワードの変更]をクリックして古いパスワードと新しいパスワードを入力し、確認のために新しいパスワードを再入力します。



3.2.5 デバイスロック解除の方法

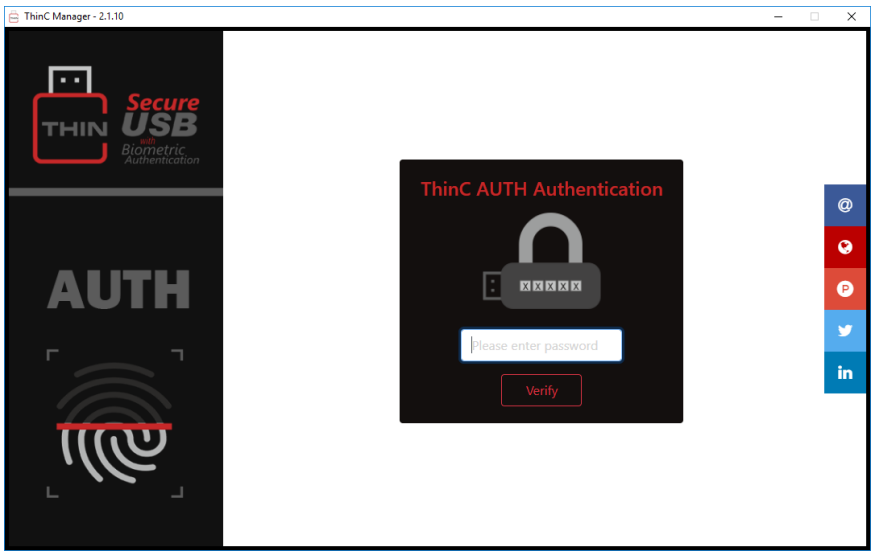
パスワードだけで指紋なしの場合

- ユーザーが指紋を登録せずにデバイスパスワードを設定した場合、ツールはユーザーにデバイスパスワードを使用してログインするように指示します。その際は、デバイスにログインするためのパスワードを入力してください。



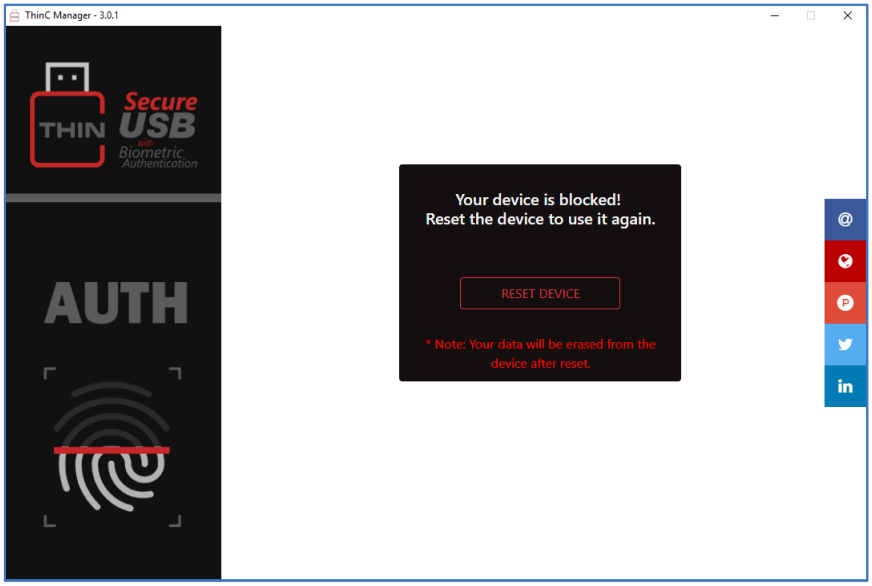
一時的ロックのデバイスのロック解除

- デバイスが一時的にロックされている場合、ツールはユーザーにデバイスパスワードを使用してツールにログインするように指示します。デバイスのロックを解除するためのパスワードを入力してください。



ロックされたデバイスのリセット

- ThinC-Manager ツールのログインプロセス中に 8 回連続して失敗すると（表のシナリオ 3 を参照）、デバイスがロックされ、再接続時にツールによってユーザーにデバイスの出荷時設定へのリセットが求められます。デバイスのリセットをクリックしてすべての設定を消去し、デバイスを工場出荷時の状態にリセットします。



3.3 設定

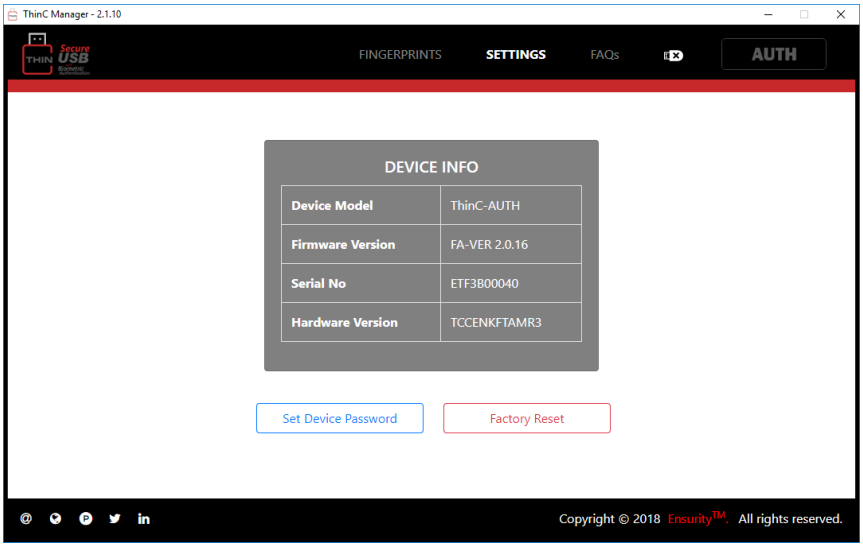
設定ウィンドウは、デバイス情報へのアクセス、デバイスのパスワード設定、および工場出荷時設定へのリセットを提供します。それは、デバイスの完全な詳細データ、すなわちデバイス構成要素のバージョンおよびシリアル番号を表示し、パスワードはデバイ

スのバックアップ認証を設定するために使用され、工場リセットはデバイスを工場出荷時設定にリセットするために使用されています。

サポートとの連絡の際に役立ちますので、デバイス情報を書き留めておくことをお勧めします。

3.3.1 デバイス情報:

- [設定]タブをクリックしてデバイス情報を表示します。表示される情報は、ファームウェアバージョン、ソフトウェアバージョン、シリアル番号、ハードウェアバージョン、FP ファームウェアバージョンで構成されています。この情報は技術サポートを受ける時に必要です。



機器情報に表示されるコンテンツの値は、接続されている機器ごとに異なる場合があります。

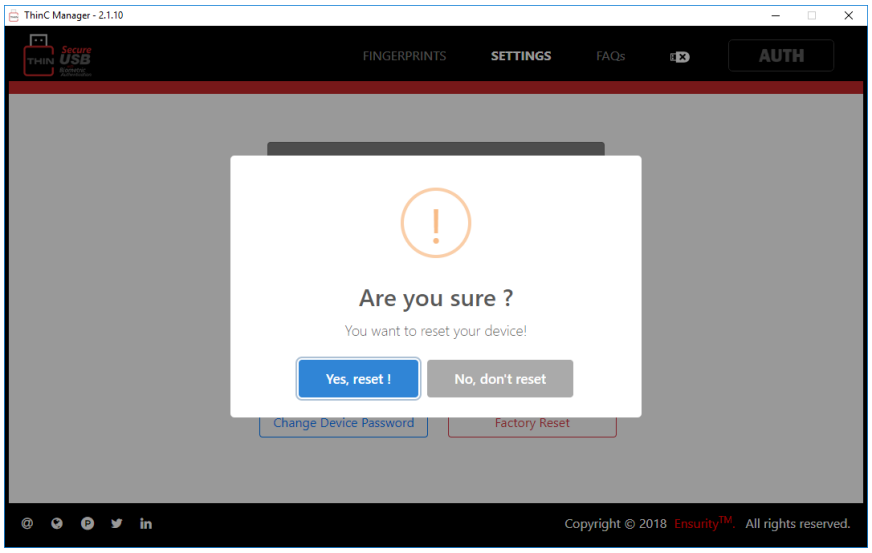
3.3.2 工場出荷時リセット:

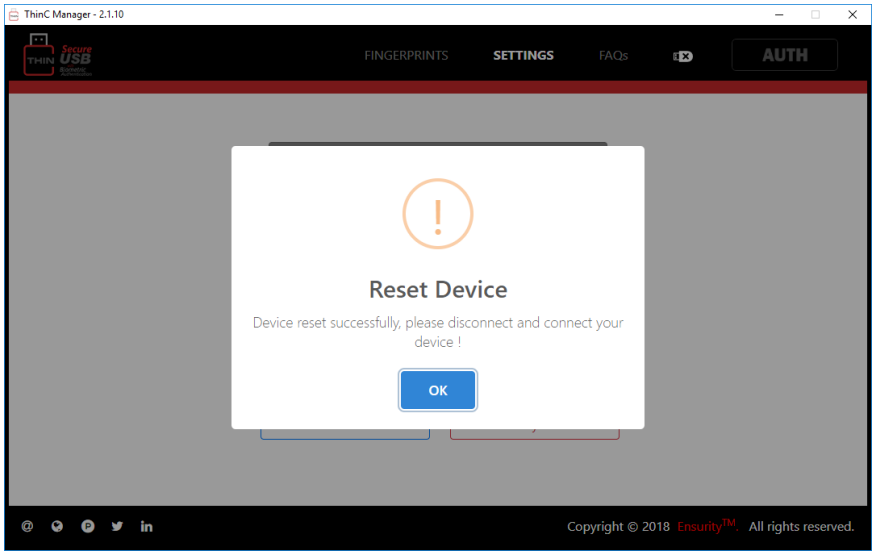
デバイスを工場出荷時のデフォルト設定に設定するには、[Factory Reset]をクリックします。続行するための許可を要求するポップアップ警告ウィンドウが表示されます。「はい、リセットします」を選択します。中止するには「いいえ、リセットしないでください」をクリックします。「はい、リセットしてください。」選択されたツールは認証を要求します。認証をクリックして、すでに登録済みの指を指紋センサーに置き、工場出荷時設定へのリセットプロセスを開始します。

正常にツールをリセットした後

工場出荷時の状態にリセットする前に、デバイスを登録または登録したサービスアプリからデバイスの登録を解除することをお勧めします。

出荷時設定にリセットすると、指紋を含むすべての保存データが消去され、デバイスが出荷時のデフォルト設定にリセットされます。



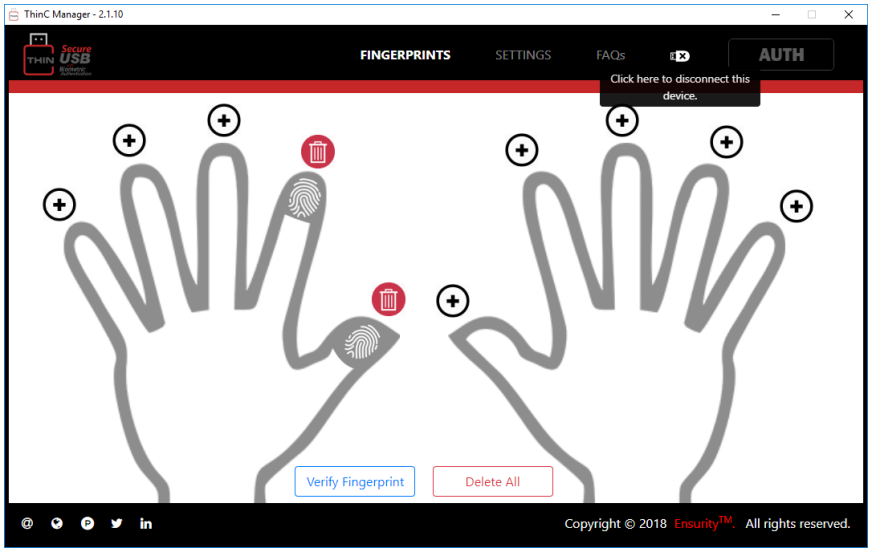


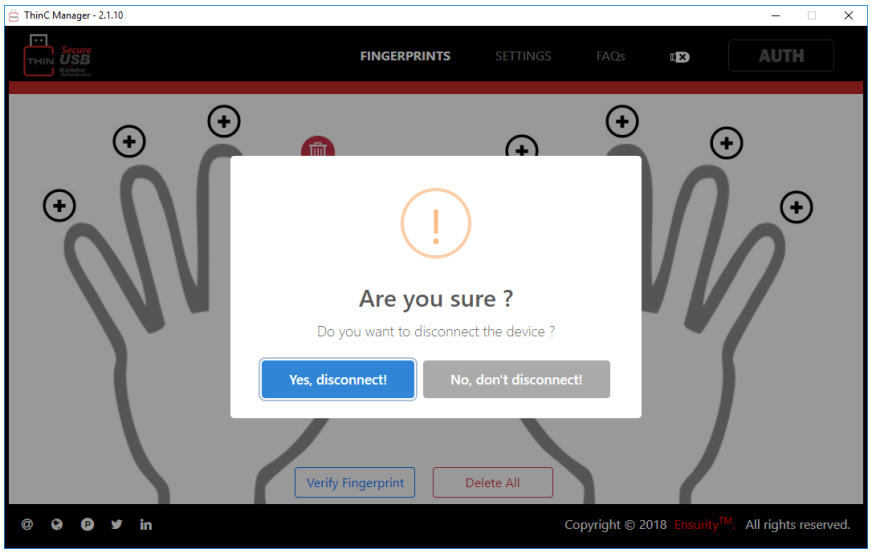
3.4 その他

切断

切断は、デバイスの切断と管理ソフトからのログアウトに使用されます。マークをクリックして切断するには、[よろしいですか]というウィンドウが表示されますので、[はい、切断します]を選択すると、管理ソフトからデバイスを切断します。「いいえ、切断

しないでください」を選択すると、デバイス管理に戻ります。一度切断されると、管理ソフトを再度動作させるには再認証が必要になります。

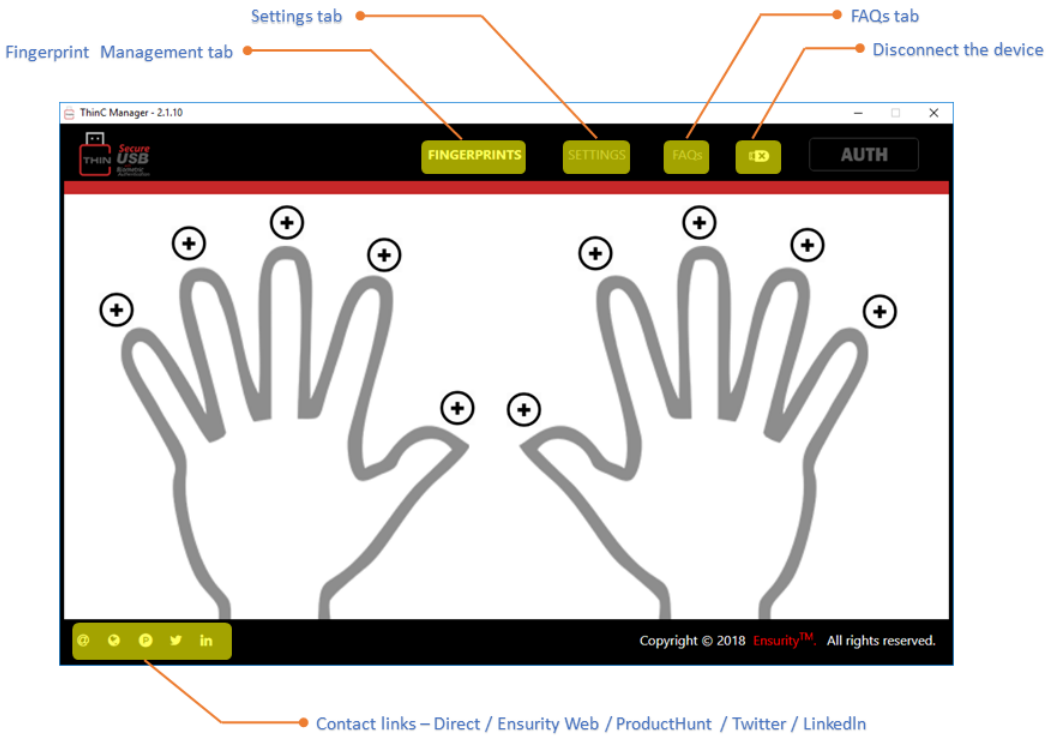




技術サポート

技術サポートは、 thinc.support@ensurity.com にご連絡下さい。

Please note that support services will be extended during the weekdays (Monday to Friday) between 10:00 AM and 7:00 PM IST.



3.5 よくある質問

ユーザー生体認証なしで、ThinC-Auth を FIDO サービスに使用できますか？

• いいえ. デバイスへのユーザーの生体認証が成功した後にのみ、デバイスにアクセスできるようになります。オプションで、ユーザーは生体認証に加えてデバイスの PIN／パスワードを利用することができます。

デバイスに登録できる指紋の数は？

•現在、ThinC-Auth は最大 5 つの指紋をサポートしています。これは、5 人の異なるユーザー（指紋）がデバイスにアクセスできることを意味し、FIDO 対応サービスで認証されます。

ユーザーがデバイスを紛失した場合、ユーザーはどのように FIDO 対応サービスを認証することができますか？

• ユーザーは、FIDO 対応サービスから 2 段階認証を無効にし、新しい ThinC-Auth デバイスで 2FA サービスを有効にする必要があります。 2FA の無効にするプロセスは、複数の FIDO サービスプロバイダによって異なります。

ユーザーは ThinC-Auth から FIDO サービス登録のバックアップを取ることができますか？

• Ensurity 間もなく ’アドオン’サービスを提供する予定です。

FIDO サービスに対する認証に制限はありますか？

• U2F サービスの場合、デバイスは無制限の登録をサポートしています。

• FIDO2 サービスの場合、デバイスは非居住者キーと 30 人の居住者キーによる無制限の登録をサポートします。

4 FIDO について(FIDO Alliance サイトから引用)

4.1 FIDO2: パスワードなし世界へ

FIDO は、“Fast Identity Online”という業界団体で指紋認証を中心とした認証規格の策定と普及推進を進めています。最新の FIDO2 プロジェクトは、Web 用の FIDO 認証標準を共同で作成し、FIDO エコシステムを大幅な拡張を目指して活動しています。FIDO2 は、W3C（業界団体WWWコンソーシアム）の Web 認証仕様（WebAuthn）と FIDO の対応する Client-to-Authenticator Protocol（CTAP）で構成されており、モバイル環境とデスクトップ環境の両方で、共通のデバイスを利用してオンライン認証を簡単に行えます。

WebAuthn は、オンラインサービスで FIDO 認証を利用するために、ブラウザやその関連する Web プラットフォームに組み込める標準 Web API を定義しています。 CTAP を WebAuthn と連携して使用すると、携帯電話や FIDO セキュリティキーなどの外部デバイスを、デスクトップ応用ソフトや Web サービスの認証器として動作させることができます。

Chrome、Firefox、および Microsoft Edge を含む複数の主要 Web ブラウザが WebAuthn 標準を実装しています。 Android、Windows 10、および関連する Microsoft テクノロジも、WebAuthn（FIDO 認証）をサポートしています。

FIDO2 の標準化への取り組みが完了し、主要なブラウザベンダがその実装にコミットしてますので、インターネットを利用するすべての人にとって、ハードウェアに支えられたユビキタス認証の新しい時代の幕開けが訪れています。

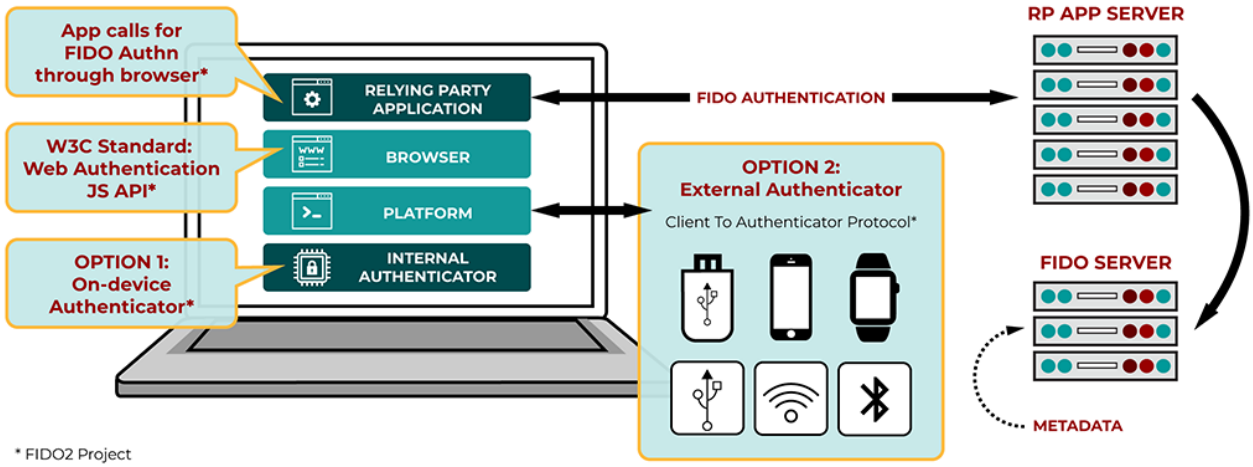
フィッシング、中間者攻撃、盗まれたパスワード情報を使用した攻撃など、パスワードに関連する危険から、社内や顧客を保護しようとしている企業やオンラインサービス会社は、ブラウザを通じて動作する標準的な強力な認証を今すぐにでも導入できます。FIDO 認証を利用すると、携帯電話やセキュリティキーのように毎日使用している装置の相互運用可能なエコシステムからオンラインサービスがユーザーに選択肢を提供できるようになります。

新しい仕様は、既存のパスワード不要の FIDO UAF および第 2 段階認証の FIDO U2F のユースケースと仕様を補完し、FIDO 認証の利用範囲を拡張します。 FIDO U2F セキュリティキーなどの外部の FIDO 準拠デバイスを現在使用しているユーザーは、WebAuthn をサポートする Web 応用で引き続きこれらのデバイスを使用できます。既存の FIDO UAF デバイスは、既存のサービスおよび FIDO UAF プロトコルに基づく新しいサービス提供としても利用できます。

FIDO Alliance は、FIDO2 仕様に準拠しているサーバー、クライアント、および認証器の相互運用性テストおよび認証を開始しました。さらに、Alliance は、すべての FIDO 認証

器タイプ（FIDO UAF、FIDO U2F、WebAuthn、CTAP）と相互運用するサーバー用の新しい“万能サーバー“認定を導入しました。最善策として、FIDO Alliance はオンラインサービスを推奨し、企業はすべての FIDO 認定認証器を確実にサポートするために“万能サーバー“を配備します。

4.2 Web Authn + CTAP のフロー



上記の図は FIDO Alliance が著作権を持っています。