ThinC-COMPUTE

(パーソナル端末 USB)

Powered by

ENSURITY
TECHNOLOGIES

目次

1 はじめに

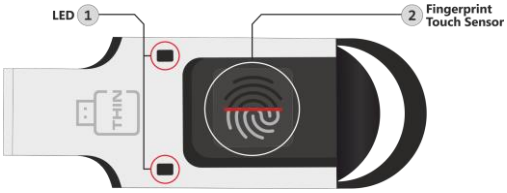
ThinC-Compute は、オンボードでカスタマイズされた Go 言語ＯＳ（オペレーティングシステム）、アクセス制御用の指紋認証、および安全な/暗号化されたストレージを備えた安全な USB ベースのデバイスです。

ThinC-Compute 上の OS は修正された Debian Linux であり、セキュリティとプライバシーを強化するために再パッケージ化されています。 OS と一緒にパッケージ化されているデフォルトのアプリには、ThinC Manager Linux 版と Secure Browser が含まれます。ブラウザの URL リストは、外部サーバー（ゲートウェイサーバー）によって管理されます。 URL のリストは、ThinC-Compute ブラウザがアクセスできる所定のサイトで更新されます。

ThinC-Compute Go 言語ＯＳ〈オペレーティングシステム〉は、ハードウェアリソース、すなわち CPU、RAM、および I/O インターフェイス（イーサネットおよび Wi-Fi）を利用して USB 外部のホストパソコン（x86 ベース）で起動します。

ThinC-Compute は、ハードウェアベースの 256 ビット AES 暗号化で保存データとＯＳ（オペレーティングシステム）を保護します。暗号化のための鍵は生成され、そのセキュアエレメント（ＳＥ）内に保存されます。 ThinC-Compute は、デバイスに保存されている暗号化データの保護レベルを高めながら、セキュリティを強化するためのセキュアエレメントを使用しています。事前にパッケージ化されたスタンドアロン管理ツールは、デバイスの管理と指紋登録のために各デバイスで利用できます。

ThinC は、指紋ベースの生体認証セキュリティを使用してデバイスへのアクセス制御を確立します。 ThinC-Compute は、ウイルス、マルウェア、トロイの木馬などの潜在的な感染を抑制しながら、読み取り専用モードで OS を操作するように設定されています。



On-board Biometric Authentication (Supports upto 5 Biometric registrations)

AES-256 Hardware Encryption (Build-Your-Own-Trust for Enterprises)

Designed in compliance with FIPS140-2 level 2 standards

1.1 ハードウエア仕様

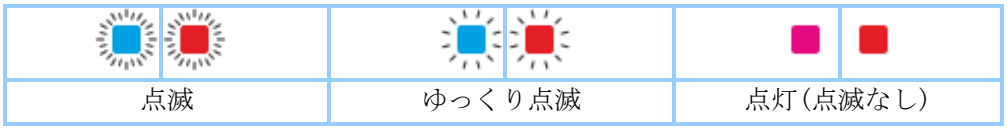
以下の表は ThinC-AUTH デバイスの簡易仕様です。

番号	特徴	仕様/記述
1	接続	• 高速 USB 2.0
2	メモリ容量	• 16 GB / 32 GB
3	指紋認証	• 容量型指紋タッチセンサー • 最大 3 指紋登録可能 • 最大 3 ユーザー
4	暗号	• 指紋およびデータの暗号 AES-256 • 動的チップ内鍵生成 • 暗号基準 FIPS 140-2 Level 2 準拠 • メモリ個人パーティション毎に個別鍵で暗号化
5	商品認可	• FCC(米国) • CE(ヨーロッパ)
6	耐久性	• 耐久性——1 万回抜き差し回数 • 5 MB /s 標準読み・書き動作
7	動作環境	• データ保存温度 -40℃ - 85℃ • 動作温度 -5℃ - 55℃ • 動作電圧 4.9V - 5.1V
8	指紋登録	• 内蔵ソフトウエア

1.2 LED 指示

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 ThinC Compute の機能

ThinC-Compute は、TextEditor、SecureBrowser、ThinC Manager（Finger_Enroll）などの基本的なアプリとともに、起動可能なセキュア OS を備えています。

2.1 ThinC-Compute のブート（起動）

ブート（起動）プロセス

ThinC-Compute は、USB からブート（起動）可能な Intel x86 ハードウェアからなるホストパソコンで利用できます。ThinC-Compute をホストパソコン（x86 ベースのラップトップ/ PC）の USB ポートに接続し、ホストパソコンの電源を入れます。ホストパソコンの BIOS 設定に進み、最初の起動デバイスが USB（ThinC-Compute）になるようにブート（起動）優先順位を変更します。

2.1.1 BIOS ブート（起動）優先順位の設定

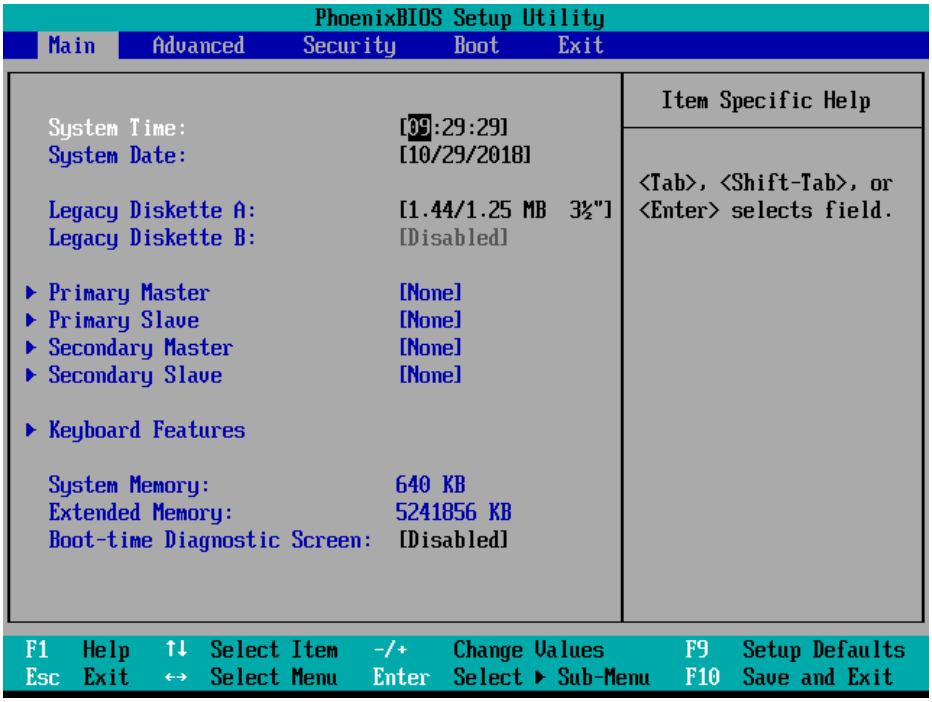
IBM 互換システム（Windows または Linux で稼働）の場合、システムは USB で起動するように設定する必要があります。BIOS をチェックして USB ブート（起動）できるようにします。適切なブート（起動）が可能になるよう優先順位設定については、パソコンの製造元のユーザーガイドを参照してください。ホストパソコンの初期起動画面で起動設定キーを押して BIOS 設定/マネジャーに入ります。

注：BIOS 設定画面は BIOS OEM メーカーによって異なります。

次のプロセスは典型的な BIOS 起動の設定を記述したものです。

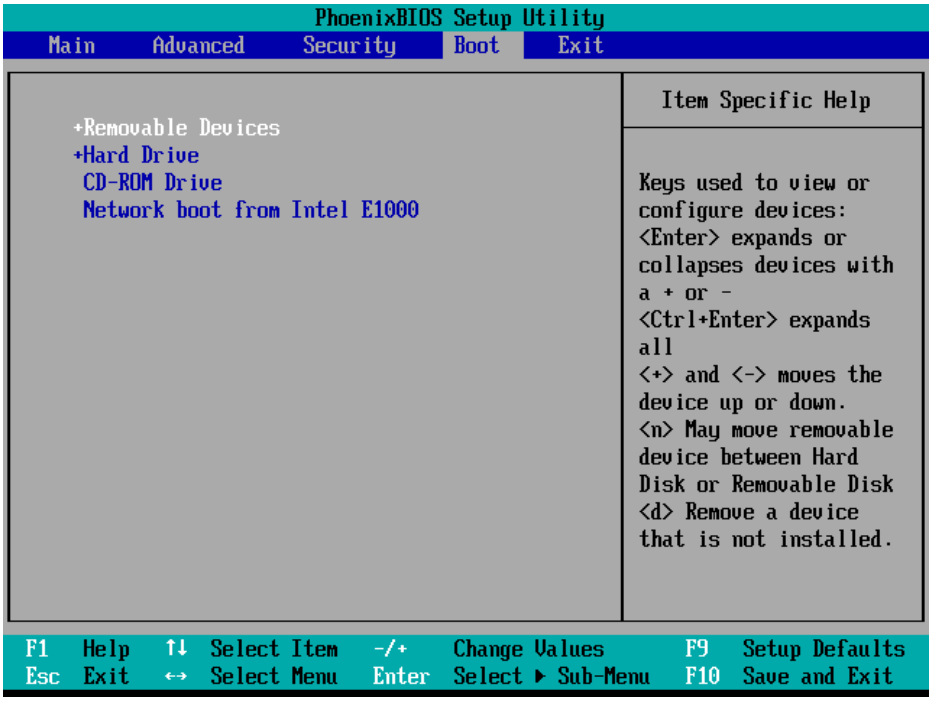
ステップ 1：

- BIOS 設定へ（通常、起動直後に Del キーを押します。BIOS 設定画面に入るために押すキーはパソコンによって違います）。



BIOS 設定ユーティリティ

- 矢印キーを使って[ブート]タブを選択します。ThinC USB デバイスをハードドライブのリストの一番上に移動します。

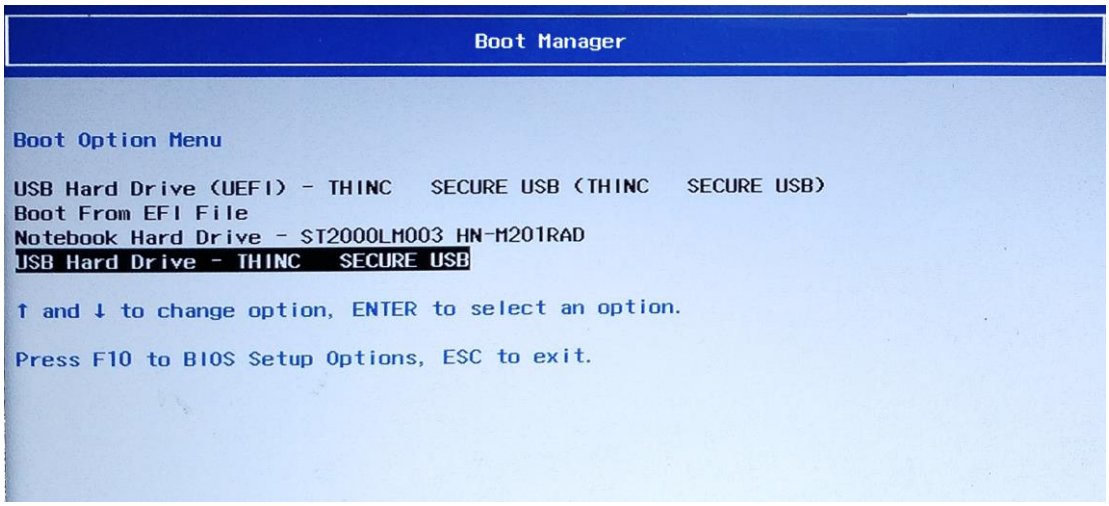


ステップ 2:

- BIOS 設定ユーティリティを保存して終了します。変更した設定でパソコンを再起動します。

2.1.2 ブートマネジャーを利用する場合

BIOS の設定の代わりに、パソコンがブートマネージャをサポートしている場合は、ブートマネージャー（通常のブート設定キー ″F12″、 ″F10″、 ″F11″、 ″Del″）に移動し、USB（ThinC-Compute / Secure USB）を選択します。起動デバイスとして USB）。



ブートマネジャー

上記の画面は典型的なブートマネジャー画面を表示しています。ブートマネジャー設定のオプションは、パソコンによって異なります。

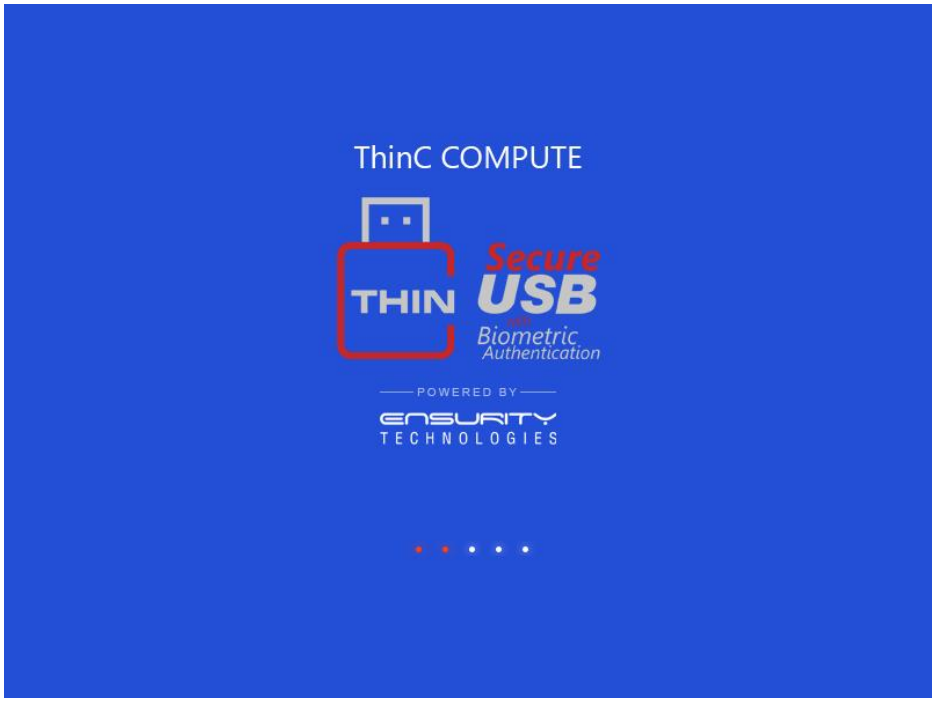
2.2 OS ブート（起動）

ThinC-Compute には 2 種類の起動プロセスがあります。

a. 初期状態起動モード
b. 指紋認証起動モード

2.2.1 初期状態起動モード

- ThinC-Compute OS を起動するには、[USB ハードドライブ ThinC Secure USB]（または同等のシステムに表示されているもの）を選択します。

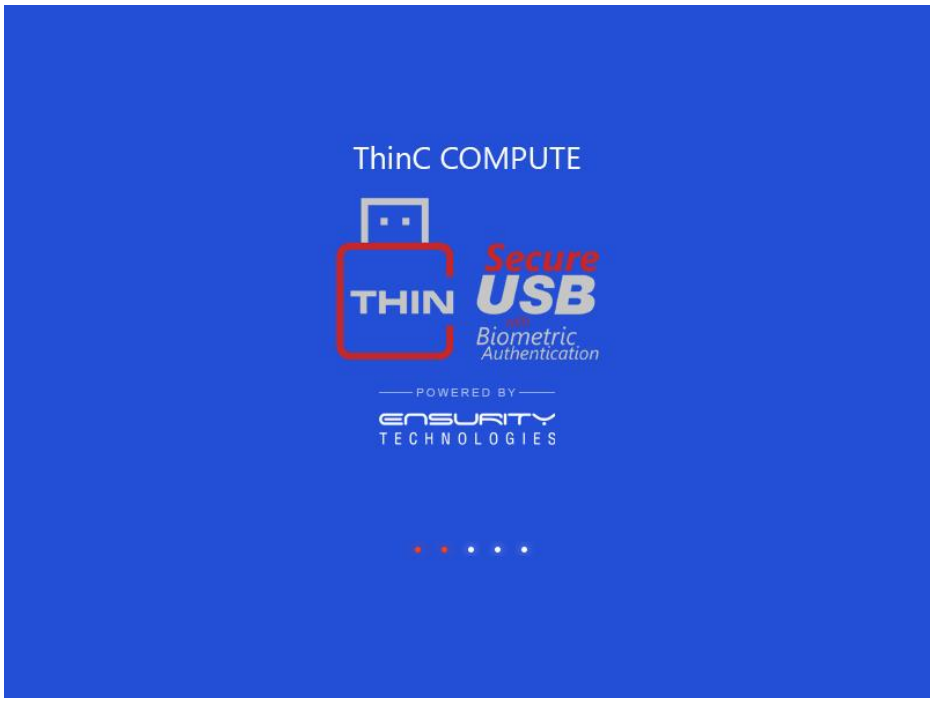


- 起動が成功すると、パソコンに OS ウィンドウが表示されます（以下の図を参照）。 このウィンドウを使用すると、OS、TextEditor、SecureBrowser、ThinC Manager（Finger_Enroll）アプリにアクセスできます。

- ThinC-Compute の指紋認証アクセスを設定するには、ThinC Compute のセクションを参照してください。

2.2.2 指紋認証起動モード

- ThinC-Compute OS を起動するには、[USB ハードドライブ ThinC Secure USB]（または同等のシステムに表示されているもの）を選択します。
- 初期起動画面の後、デバイスは[ThinC-Compute は待機状態（ピンクの LED が点灯）] で登録済みの指紋認証を要求します。
- 登録した指をタッチして認証します。 ThinC-Compute は指紋を検証して、認証が成功した後に、ホストパソコンに OS をロードします。



.

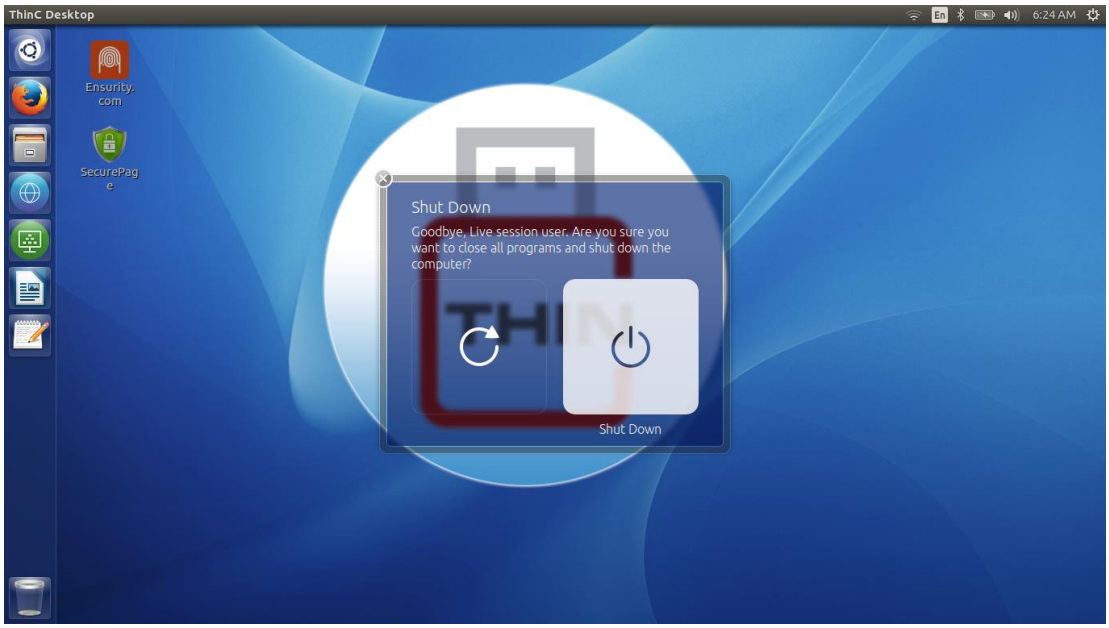
- 正常に起動すると、パソコン画面に OS ウィンドウが表示されます（以下の図を参照）。 このウィンドウから、OS、TextEditor、SecureBrowser、ThinC Manager（Finger_Enroll）アプリにアクセスできます。

2.3 OS シャットダウン

ThinC-ComputeOS は、必ず決められた手順に従ってシャットダウンする必要があります。突然シャットダウンした場合、OS が破損する可能性があります。以下は、ThinC-Compute OS をシャットダウンするプロセスです。

- 安全な OS を安全にシャットダウンするには、タスクバーの右上隅にあるシャットダウンボタンをクリックしてください。

- [シャットダウン]ボタンをクリックして、ThinC-ComputeOS の電源を切ります。



- ThinC-ComputeOS をシャットダウンした後、ThinC-Compute デバイスを取り外し、必要に応じてデスクトップ/ラップトップの元の OS でパソコンを起動してください。

パソコン時刻が変更された場合は、時刻を現在の現地時間に同期させるか、手動で変更してください。

2.4 ThinC-Compute の機能

ThinC-Compute は、ThinC Manager (Finger-Enroll) アプリを実装しています。このアプリは、以下の目的のためのものです。

1. 指紋登録.
2. 指紋認証
3. 登録指紋削除
4. Wi-Fi 接続
5. WI-FI 接続情報の保存
6. すべての認証情報の削除

ThinC-Compute には、フレッシュ/リセット/未登録のデバイスと指紋登録/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。デバイスに指紋が登録されていない場合は、ThinC-OS が直接ホストパソコンを起動します。デバイスのモードを指紋認証モード

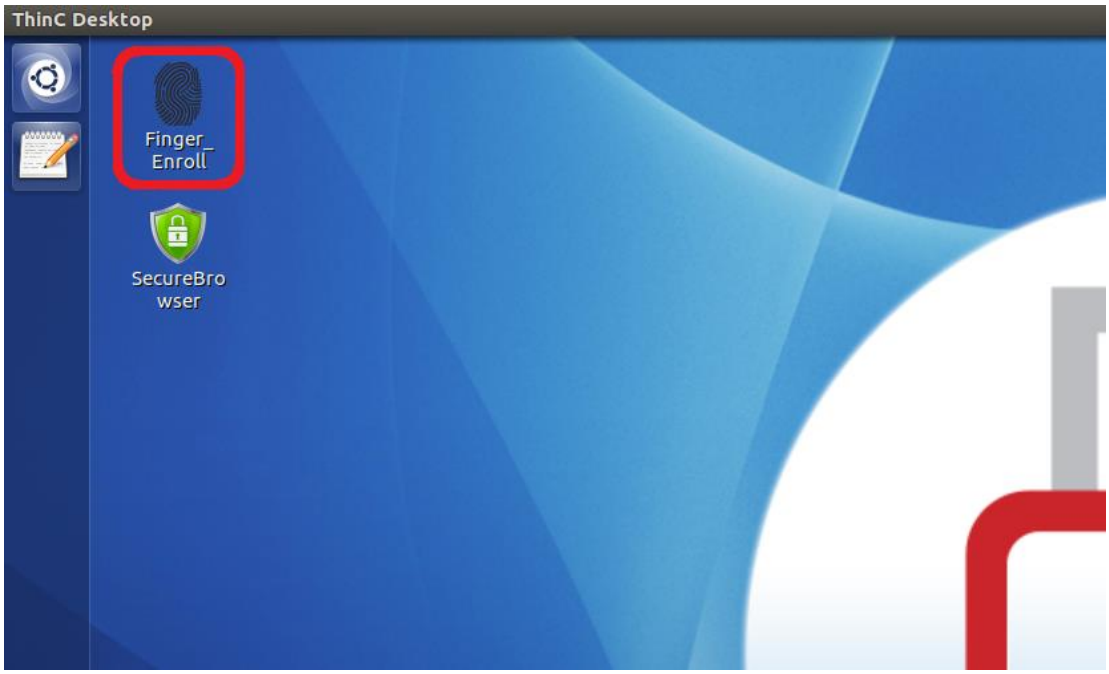
（すなわち、指紋認証ベースのセキュア OS 起動モード）に変更するには、ユーザが少なくとも 1 つの指紋をデバイスに登録することが必要です。

2.4.1 指紋登録

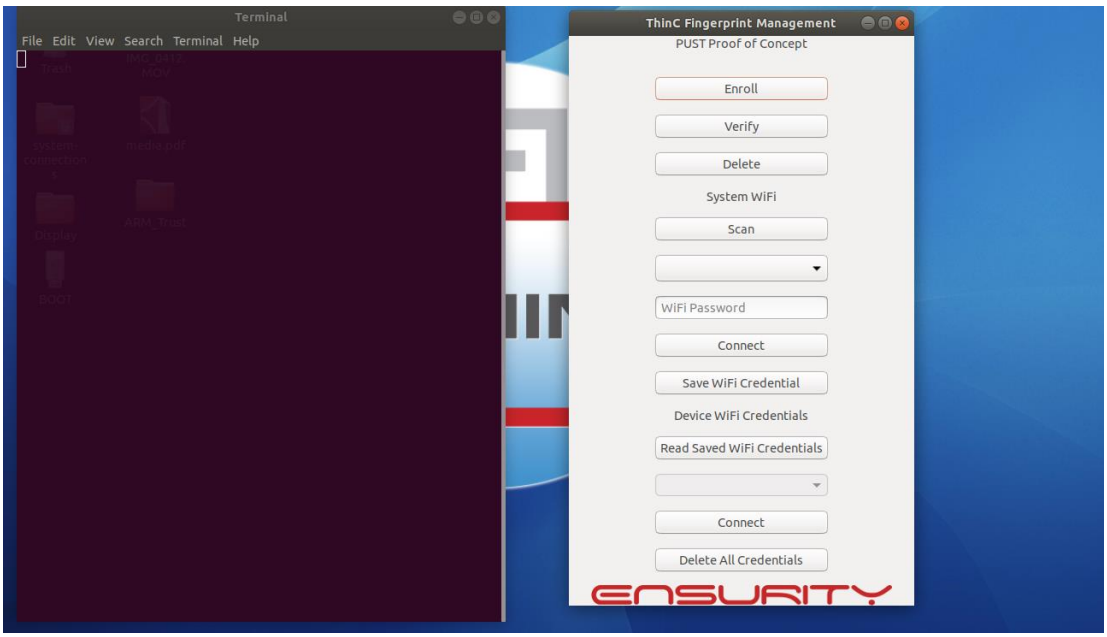
ステップ 1:

- ThinC-Compute の決められた起動プロセスを使って、フレッシュ/リセット/未登録のデバイスを起動します。
- ThinC Manager（Finger_Enroll）アプリを実行します。

.

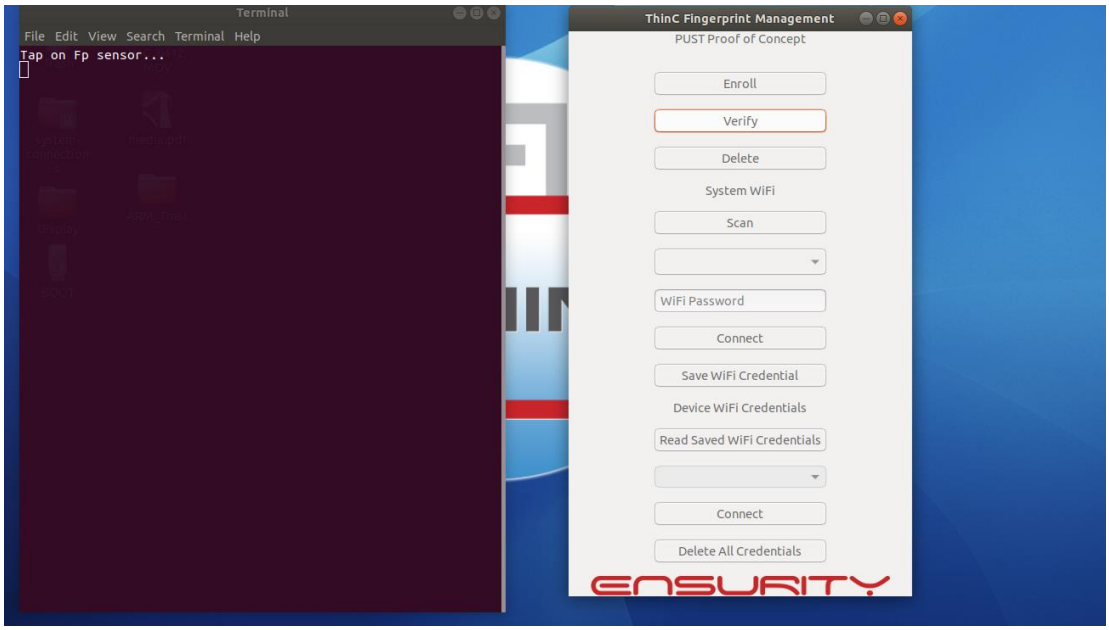


- このツールには指紋登録の管理機能があります（現在の ThinC-Compute では最大 3 本の指を登録できます）。登録ボタンをクリックして登録プロセスを開始します。
- 指紋登録機能の準備が完了すると、デバイスはピンクの LED を点滅させます。
- 指紋センサーに繰り返し指を置いて登録プロセスを続行し、デバイスが青色の LED を点灯するまで続けます。
- これまでの経験によると、すばやく指を登録するには、毎回指をわずかに異なる角度で繰り返し配置することをお勧めします。

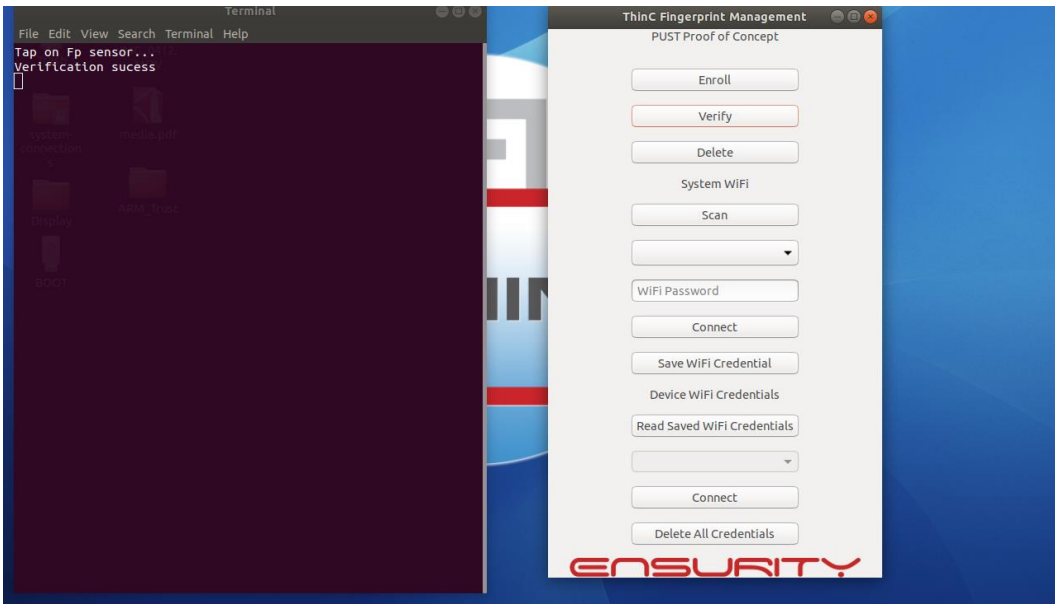


ステップ 2:

- 指の認証確認は、ThinC-Compute を使用するために必ずしも必要ではありませんが、これまでの経験から、登録されている指紋の認証を確認することをお勧めします。
- この手順は、登録済みの指紋を確認するためのものです。 ThinC Manager（Finger_Enroll）の、[認証]ボタンをクリックしてから、登録済みの指をセンサーに置きます。



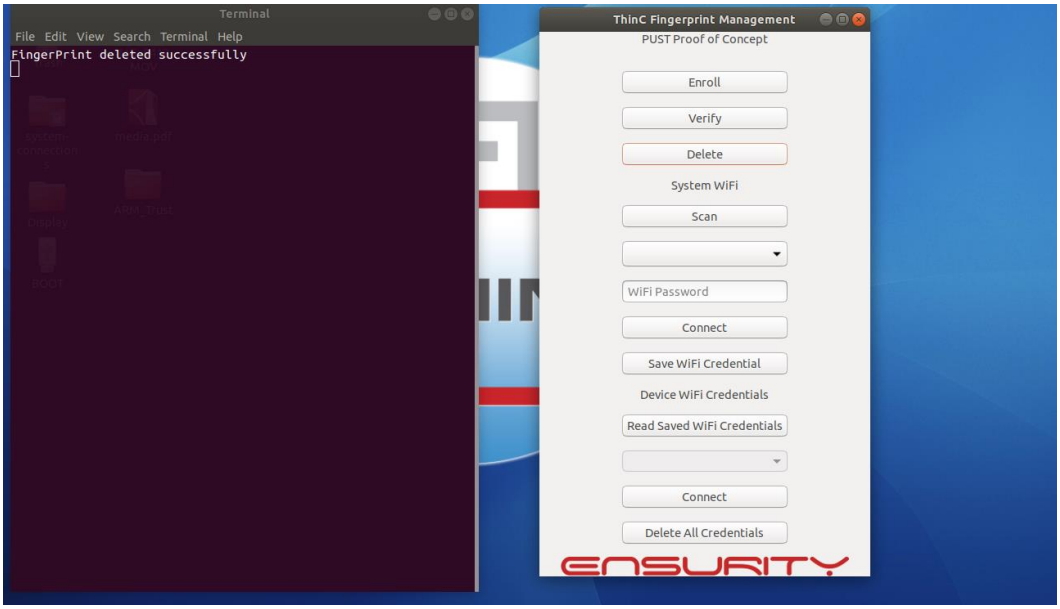
- ツールは自動的に認証プロセスを開始し、入力指紋が登録済みの指と一致したら「成功」を通知します。



2.4.2 登録解除／登録指紋の削除

ツールには、保存されている指紋を削除するオプションもあります。デバイス上の指紋は登録順序と逆順序で削除されます。つまり、最後に登録された指紋が最初に削除されます。

- ThinC 指紋管理ウィンドウで、指紋を削除/登録解除するには[削除]をクリックします。
- 指紋の削除に成功すると、「FingerPrint deleted successfully」という通知が端末に表示されます。



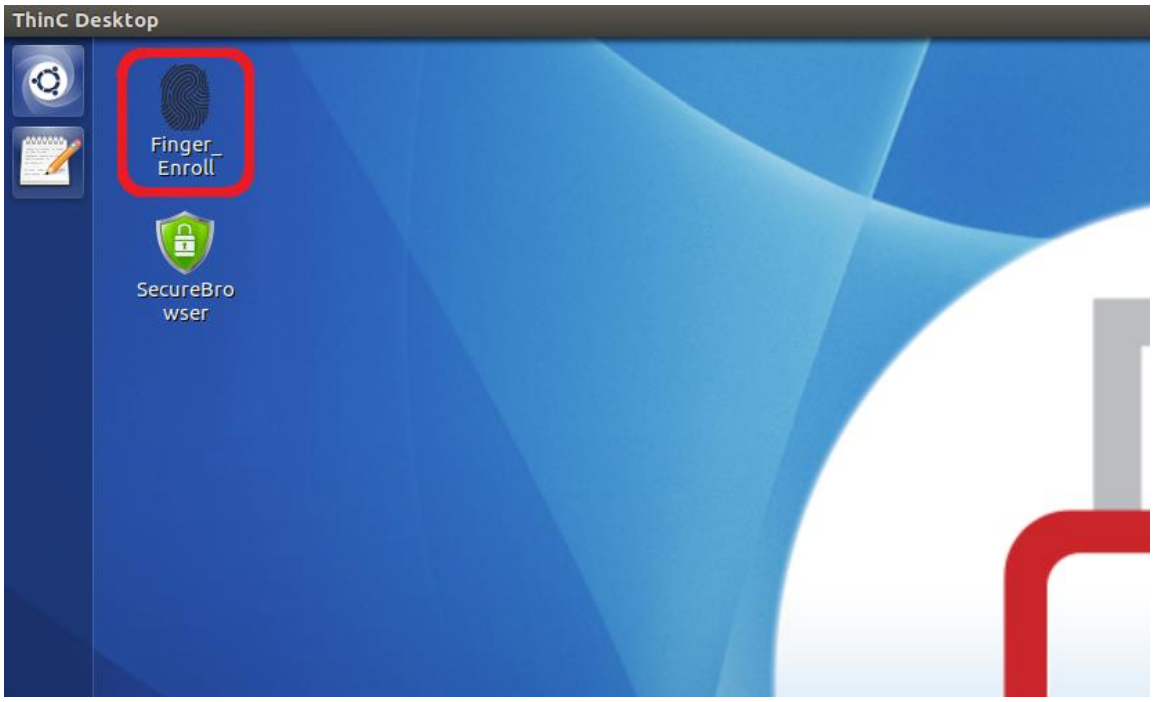
2.4.3 Wi-Fi ネットワーク接続

ThinC Manager ツール（finger_enroll）は、スキャン、接続、保存、Wi-Fi ネットワークの読み取り、および関連する資格情報を管理する機能を提供します。

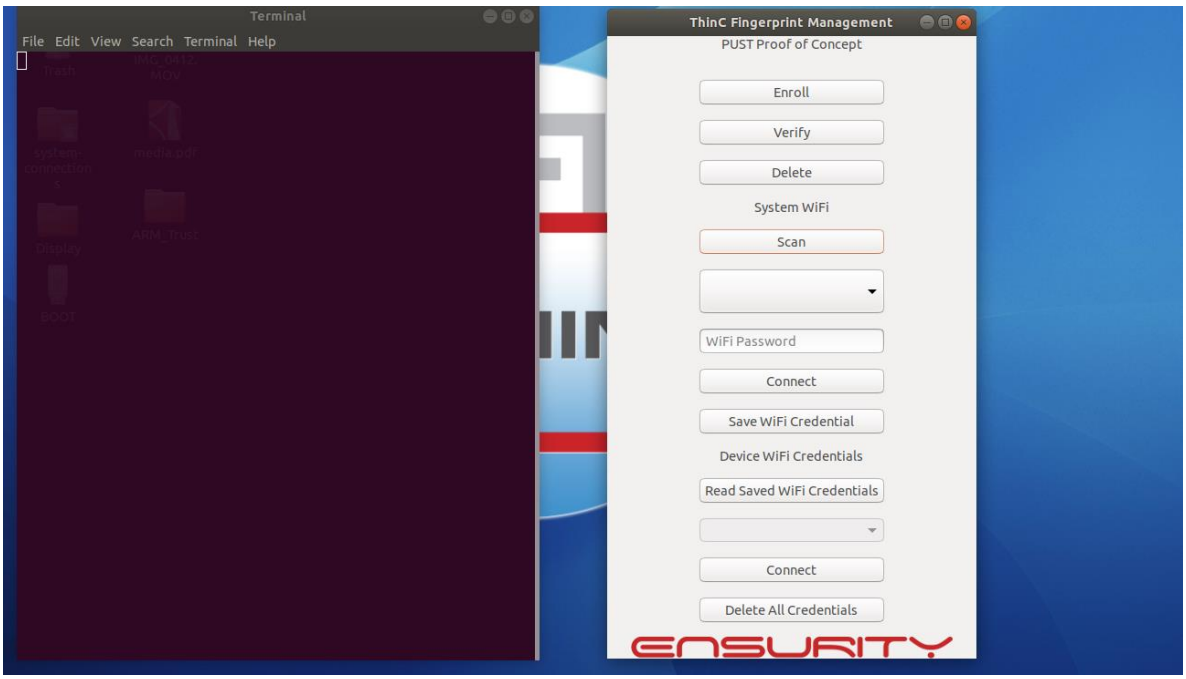
注：必要な Wi-Fi ネットワークがスイッチオンモードになっていることを確認してください。ホストコンピュータに Wi-Fi をオン/オフするための専用ハードウェアボタンがある場合。次に先に進む前に適切に電源を入れてください。
以下はその手順です： -

Wi-Fi Network をスキャン

- ThinC Manager（Finger_Enroll）アプリを実行します。

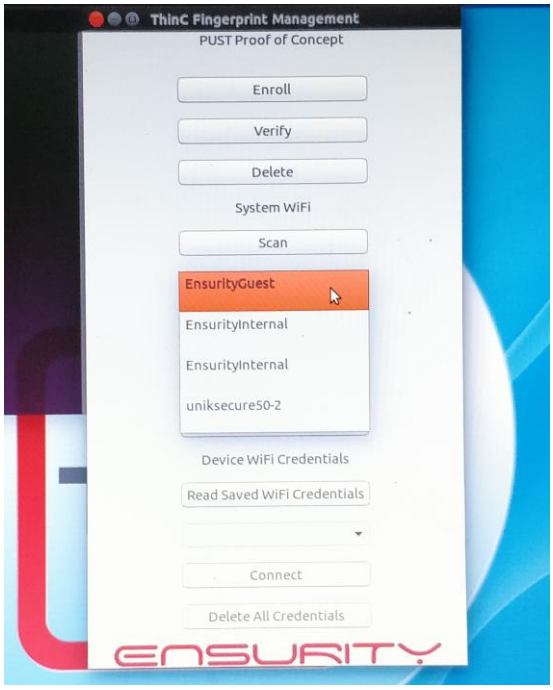


- [スキャン]をクリックし、約 10〜25 秒待ってから Wi-Fi スキャンを完了します（これは、周囲の Wi-Fi ネットワークの数によってはさらに時間がかかる場合があります）。
- スキャン処理が完了すると、スキャンボタンの下にあるドロップダウンボックスに Wi-Fi ネットワークの名前（SSID）が表示されます。



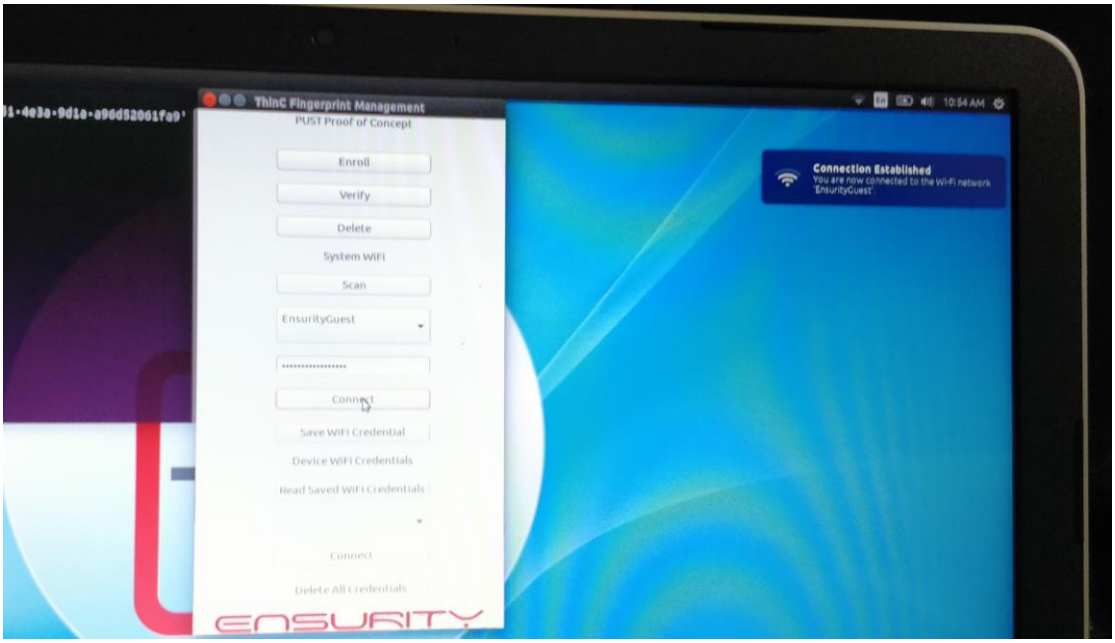
Wi-Fi ネットワークへの接続

- ドロップダウンリストから接続する Wi-Fi ネットワークの名前 SSID を選択し、Wi-Fi パスワードボックスに Wi-Fi パスワードを入力します。
- [接続]ボタンをクリックして、それぞれの Wi-Fi ネットワークに接続します（[Wi-Fi 認証情報の保存]ボタンの上にある[接続]ボタン）。



- 参考として、上のスクリーンショットは利用可能な Wi-Fi ネットワークのサンプルリストを示しています。 Wi-Fi ネットワークリストは場所によって異なります。Wi-Fi ネットワークリストは場所によって異なります。

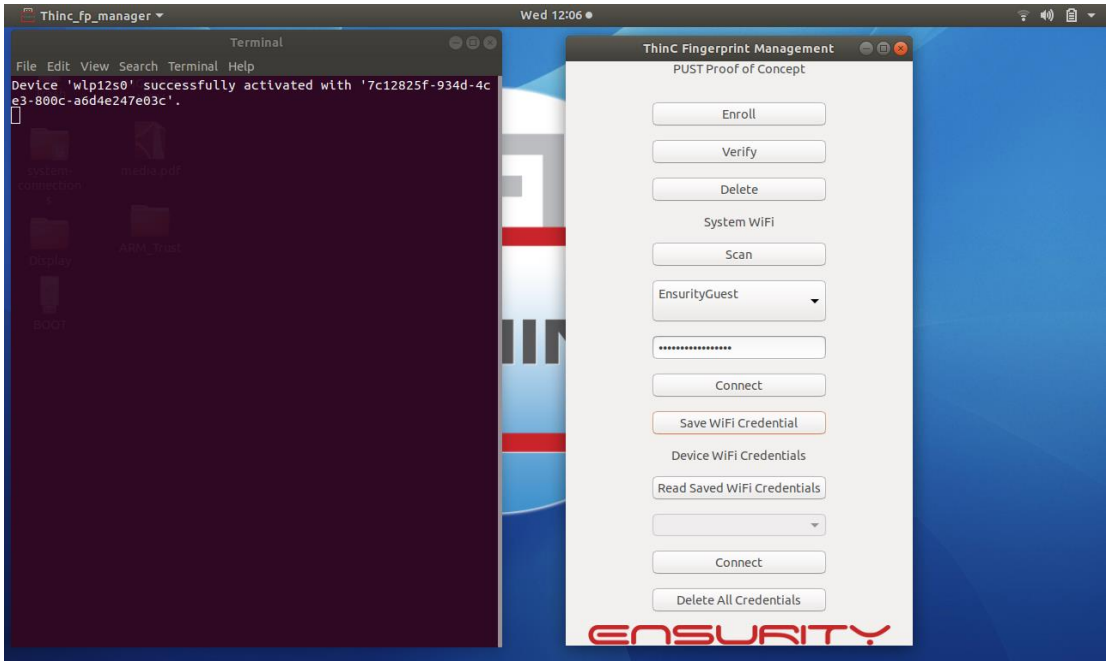
- 接続が成功した場合、OS は接続の確立に関して「connection established」という通知を送信します。ユーザーが接続を確立できない場合は、上記の手順（1 と 2）を繰り返します。



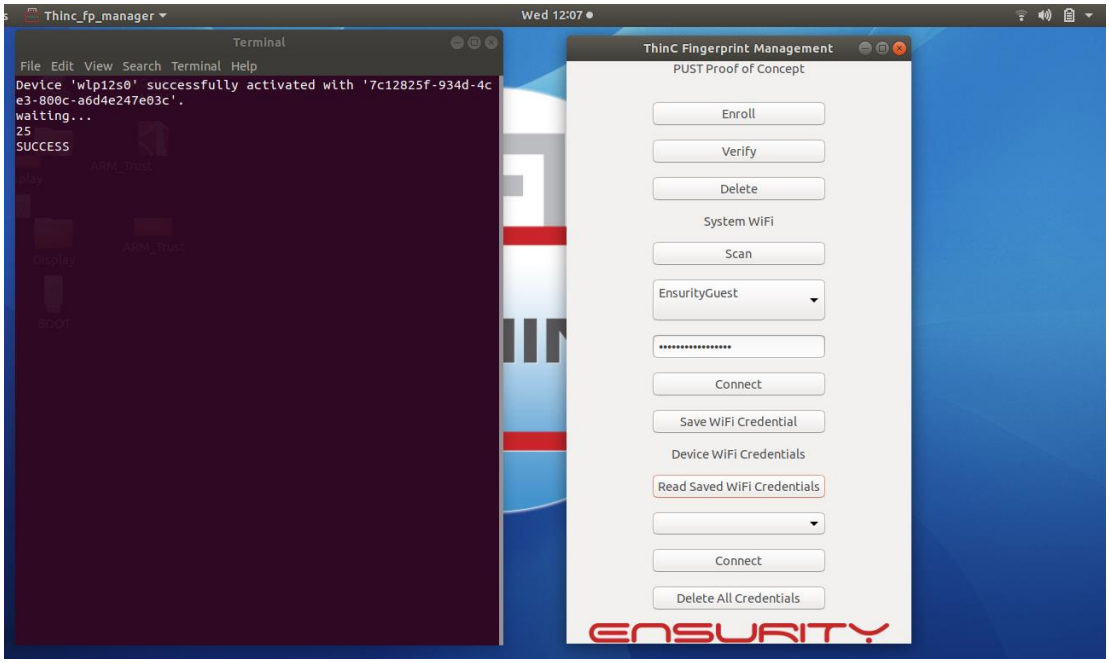
Wi-Fi 情報の保存

ThinC-Compute は、次の再起動まで Wi-Fi 認証情報を一時的に保存するリードオンリーのオペレーティングシステム（OS）を利用しています。Wi-FI 認証情報は、Wi-Fi 保存機能を使用して恒久的に保存することができます。この機能を使用して保存された Wi-Fi 認証情報は、認証情報がユーザーによって削除または変更されるまで、次回の起動時に使用可能になります。

- Wi-Fi 管理セクションの 1 と 2 の手順に従います。
- 特定の Wi-Fi ネットワークへの接続に成功したら、Save Wi-Fi Credentials をクリックします。



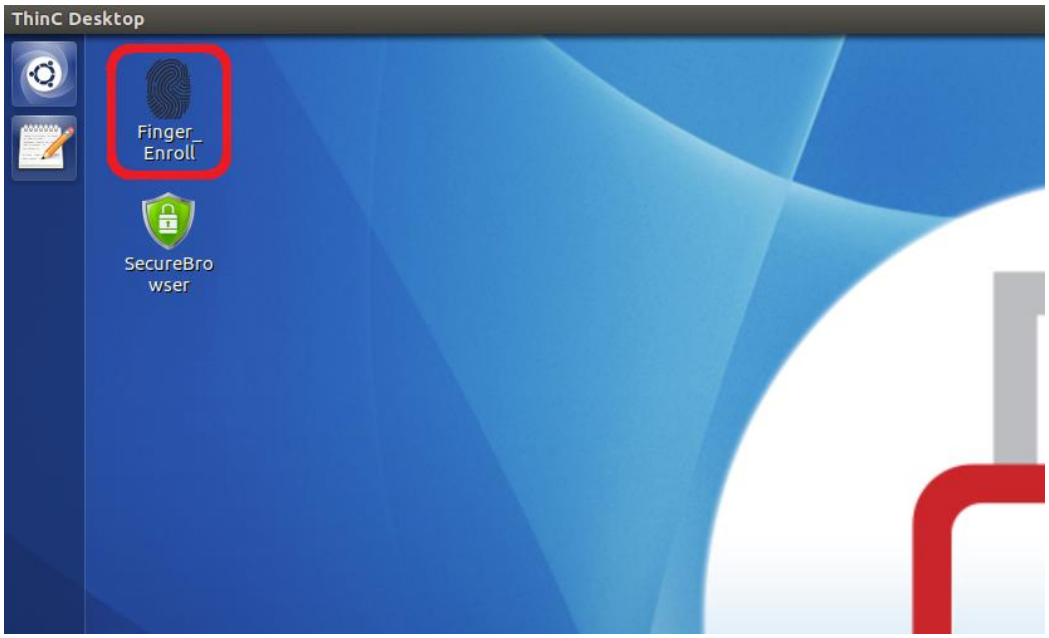
認証情報をデバイスに保存した後、端末には「成功」が表示されます。



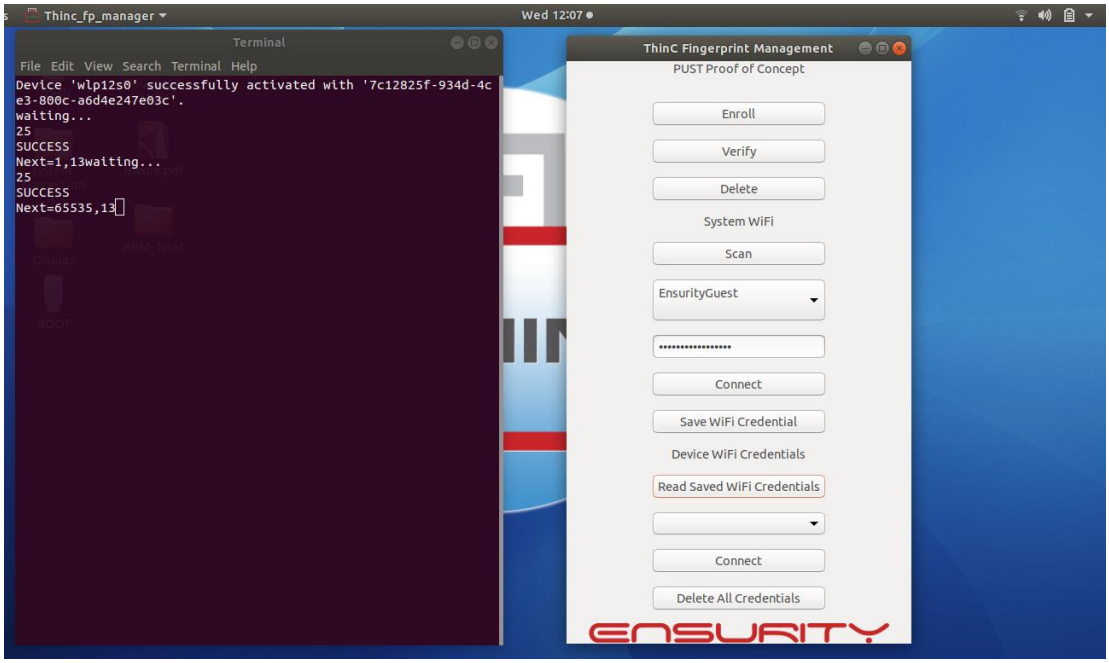
保存されたWi-Fi への接続

アプリは、保存された Wi-Fi ネットワークと関連する認証情報を読み取ることができます。

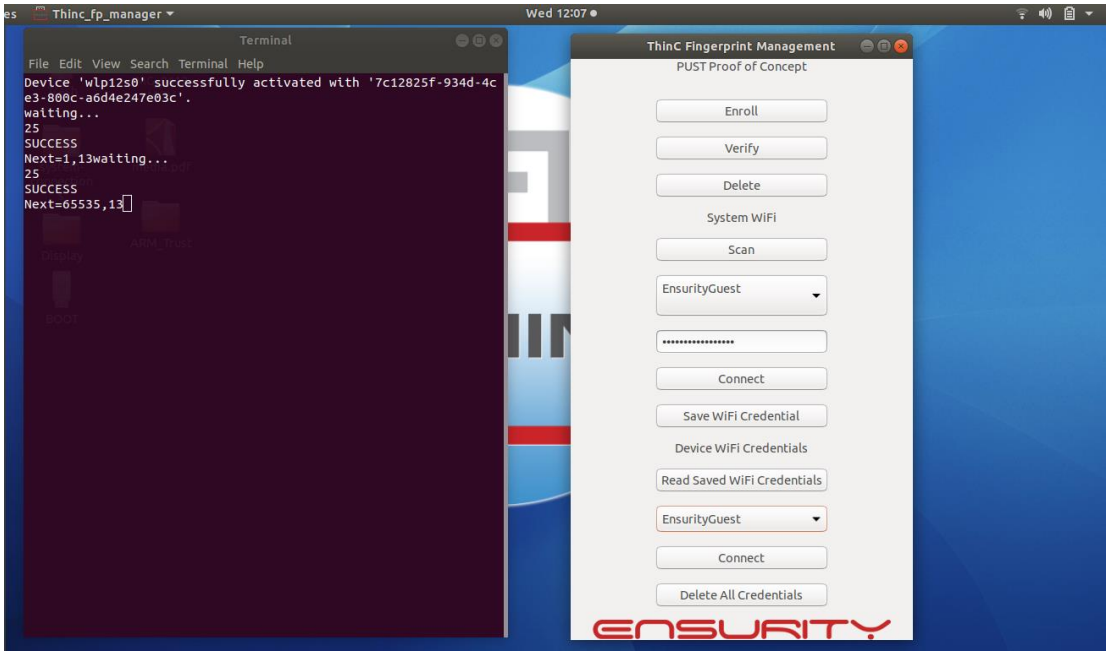
- ThinC Manager（Finger_Enroll）アプリを実行します。



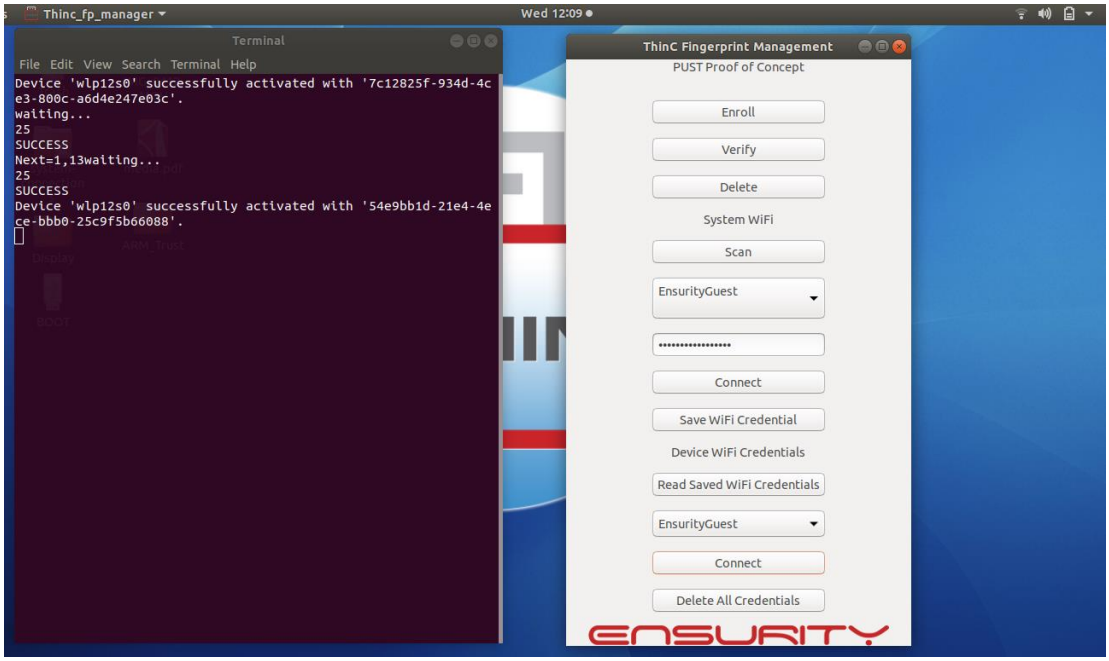
- 保存された Wi-Fi 情報の読み込みのクリック



- デバイスから保存された認証情報に正常にアクセスした後、端末に「成功」が表示されます。
- このツールは、以前に保存した Wi-Fi ネットワークの名前 SSID をボックスに表示されます。
- 接続する Wi-Fi ネットワークの名前 SSID を選択し、ボックスの下にある[接続]ボタンをクリックします。

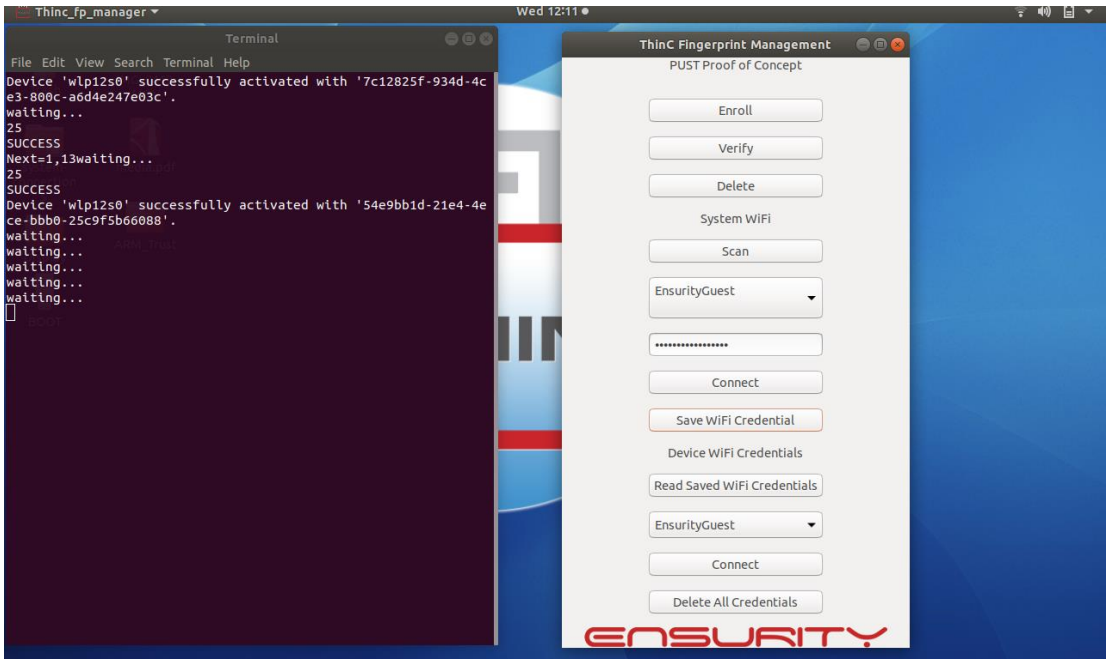


保存された Wi-Fi 認証情報を読んで接続するスクリーンショット。



全認証情報の削除

- この機能は、保存されているすべての Wi-Fi ネットワークと関連する認証情報を削除します。デバイスに保存されているすべての Wi-Fi 認証情報を消去するには、[Delete All Credentials]をクリックします。



ネットワーク接続の設定

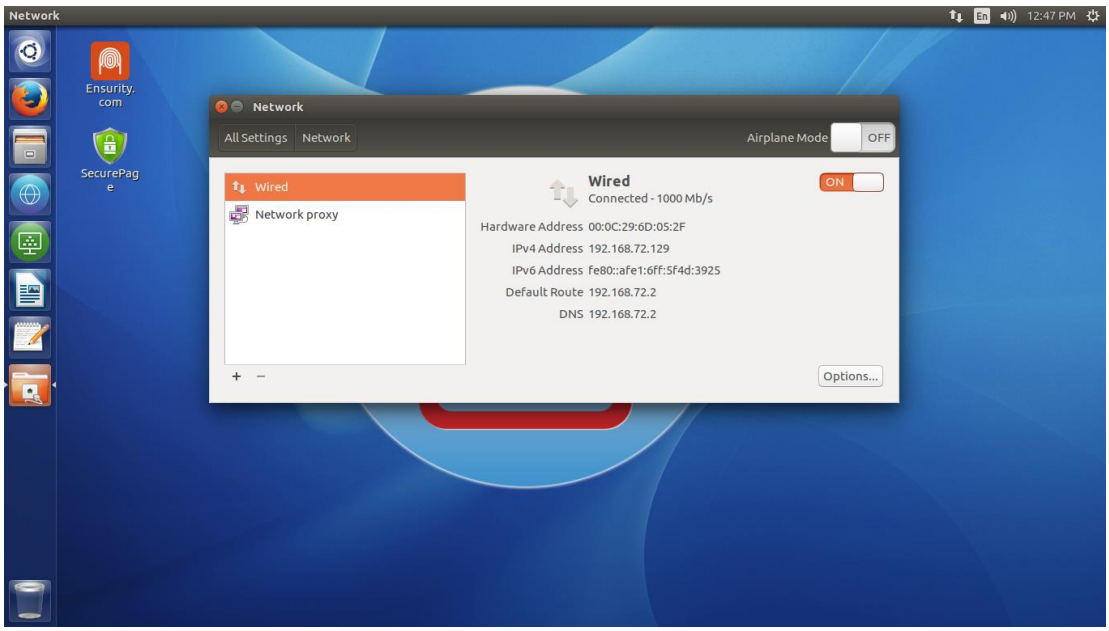
ホストパソコンに応じて、ネットワーク接続オプションは異なります。

ホストパソコンを有線ネットワークに接続するための手順に従ってください。ホストパソコンが有線ネットワークに物理的に接続されていることを確認してください。

ステップ 1 ： OS ウィンドウで[ネットワークマネージャ]を選択するか、ステップ 2 を実行します。

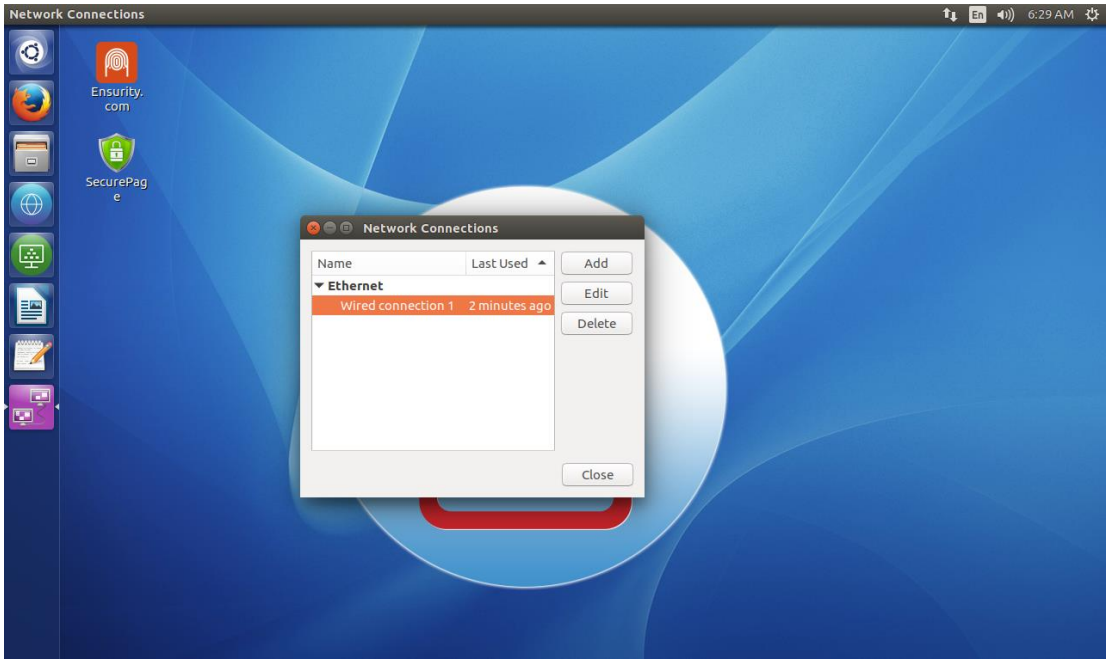
ステップ 2 : ネットワーク  をクリックして検索するか、システム設定に移動してネットワークをクリックします。

- 有線ネットワークで、オプションをクリックします。

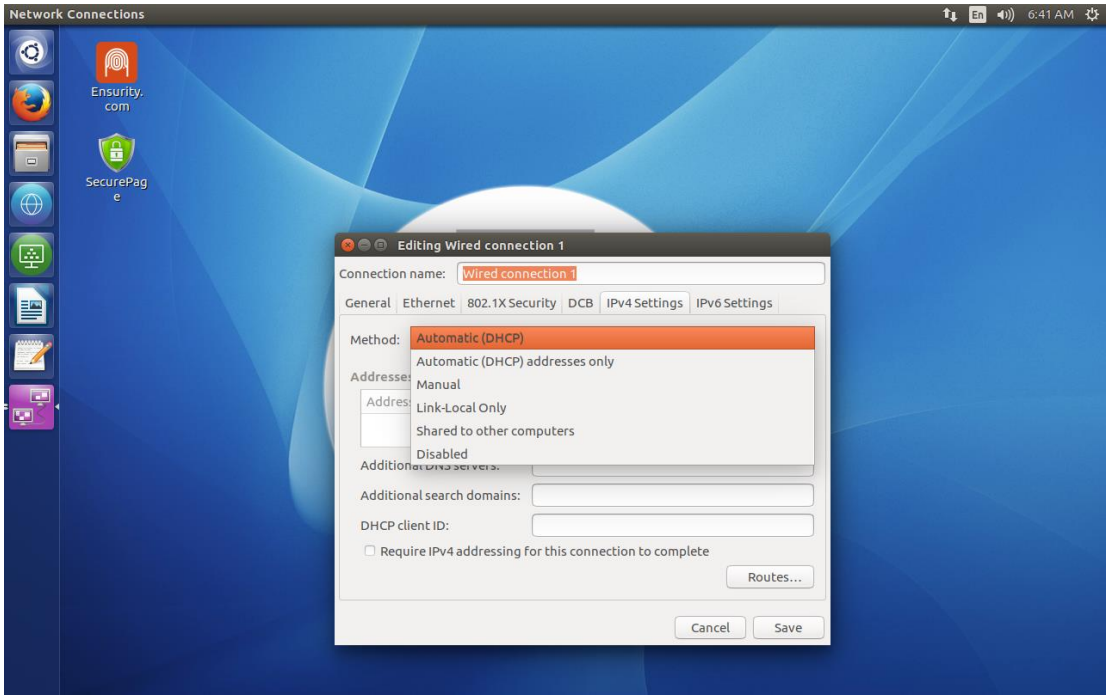


- ネットワーク接続が利用可能な場合は、代わりにネットワーク接続アイコンをクリックして接続の編集を選択します。

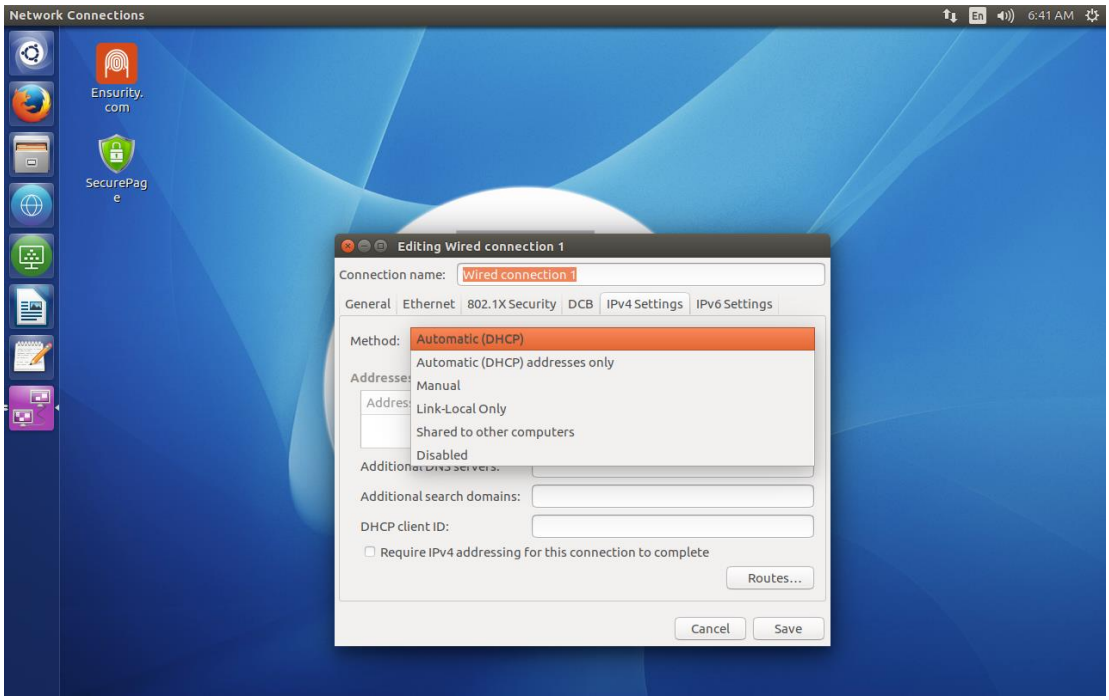
- 利用可能な有線接続を選択して、必要なインターフェースを編集します。



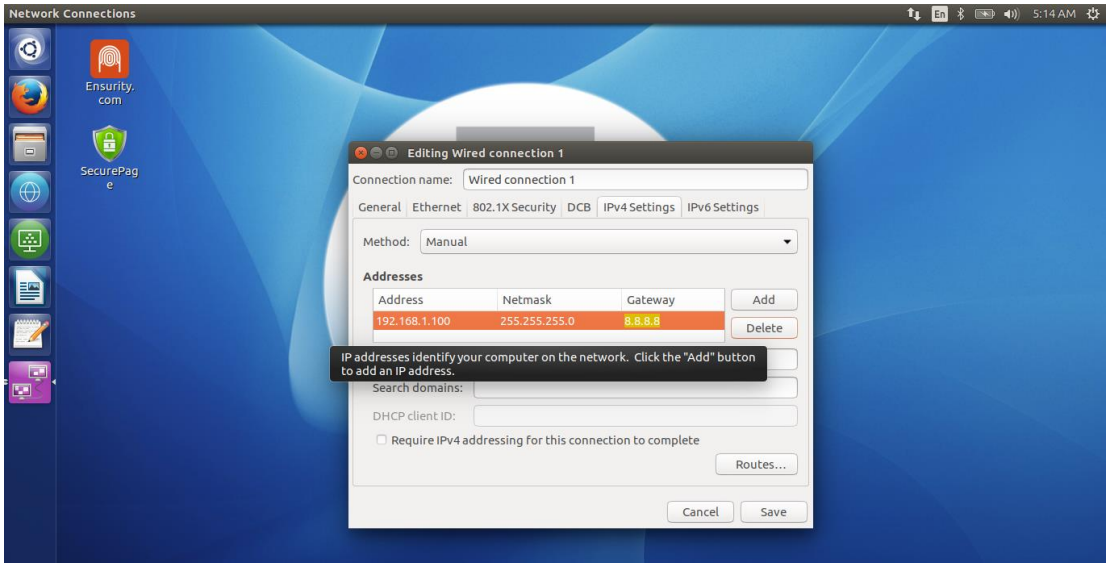
- DHCP ベースのネットワークアドレス割り当て - IPV4 設定に移動し、[自動 DHCP 方式]を選択して[保存]をクリックします。



- 静的 IP 手動アドレス割り当ての場合 - IPV4 設定に移動し、手動方式を選択します。



- [アドレス]セクションで、[追加]ボタンをクリックします。目的の IP アドレス、ネットマスク、DNS、およびゲートウェイを入力し、[保存]をクリックして接続に加えられた変更を保存します。



ネットワークインターフェースの設定後、リストに掲載されている Web ページ/ URL およびアプリにアクセスするために、インターネットまたは必要なネットワークへの接続を確認してください。

2.5 ThinC-Compute SecureBrowser

ThinC-Compute には、ユーザーがホワイトリストに登録された Web サイトのみにアクセスすることを制限できる SecureBrowser があります。この SecureBrowser は、指定されたゲートウェイサーバーと連携して動作します。両方ともまとめてブラウザサブシステムと呼ばれます。このブラウザサブシステムには、コンテンツフィルタリング用に 2 つのコンポーネント（Web サイト/ URL のホワイトリスト）があります。

1. サーバーサブシステム（ゲートウェイサーバー） - コンテンツフィルタリング/ウェブサイトホワイトリストのルールを追加する。
2. クライアントサブシステム - コンテンツフィルタリング/ Web サイトホワイトリストサイトを強化するため

2.5.1 サーバーシステム

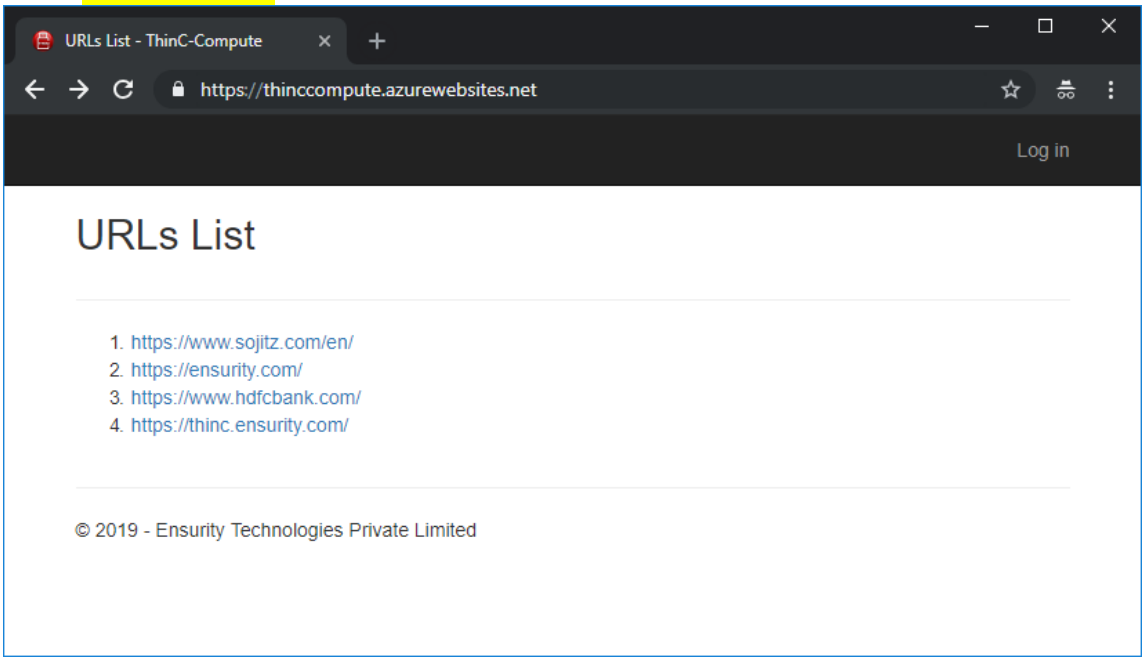
このサーバーサブシステムは、URL https://thinccompute.azurewebsites.net からアクセスできます。管理者はサーバーにログインして、クライアントサブシステム/ SercureBrowser のホワイトリストに登録されたサイトを変更、追加、削除することができます。 Web サイトにアクセスするための認証情報は、「ログイン認証情報 ThinC-Compute Gateway サーバー」という件名で顧客の詳細とともに hello@ensurity.com に電子メールを送信することによって取得できます。サポートチームは顧客の詳細を確認し、アクセスに必要な認証情報を共有します。

Steps to Manage websites

以下は、ThinC-Compute のホワイトリスト Web サイトを管理するためのプロセスです。

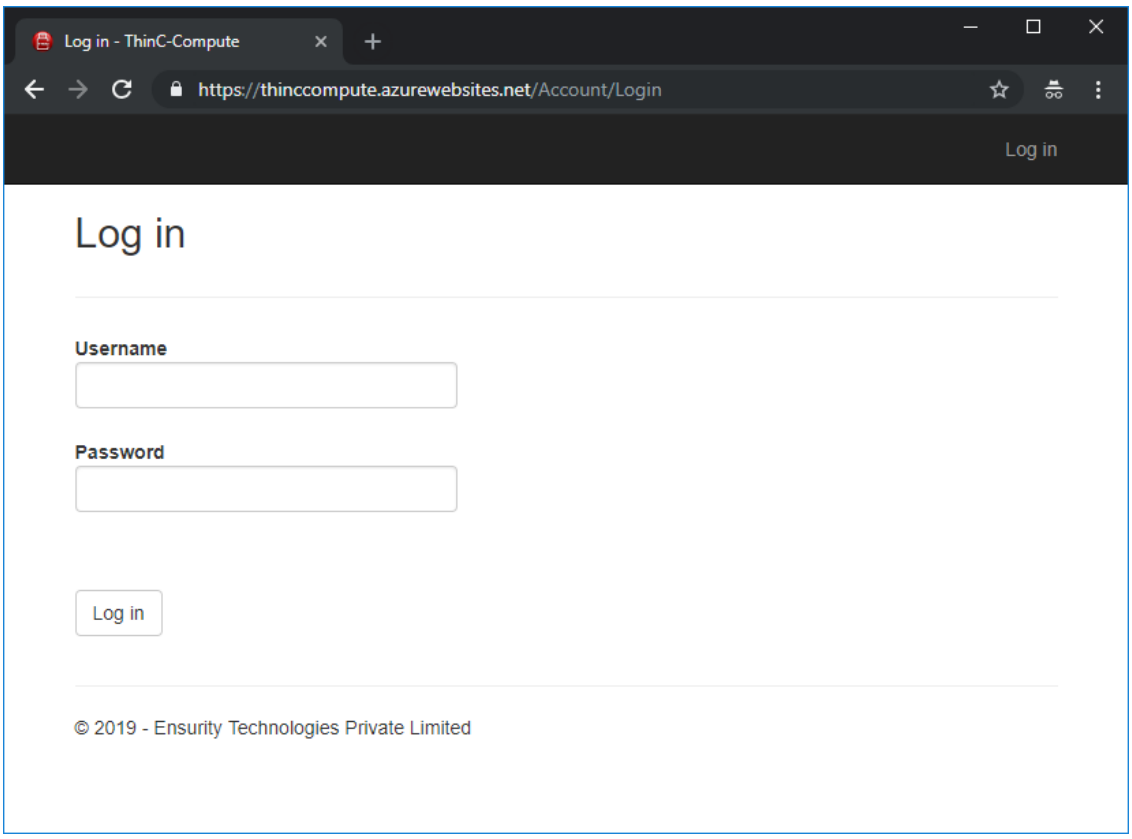
ステップ 1

- URLhttps://thinccompute.azurewebsites.net を使用してサーバーにログインする。自宅の年齢には、既にホワイトリストに登録されている URL が表示されます。



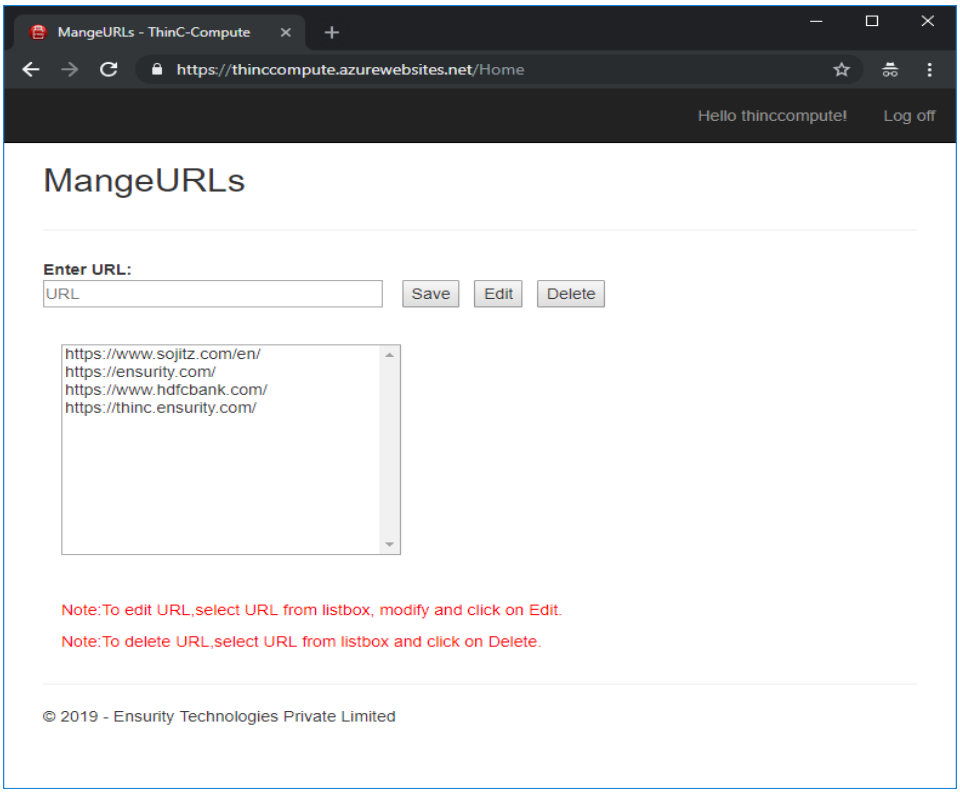
ステップ 2

- リストを変更するには、[ログイン]ボタンをクリックして、サポートチームが共有する認証情報を入力します

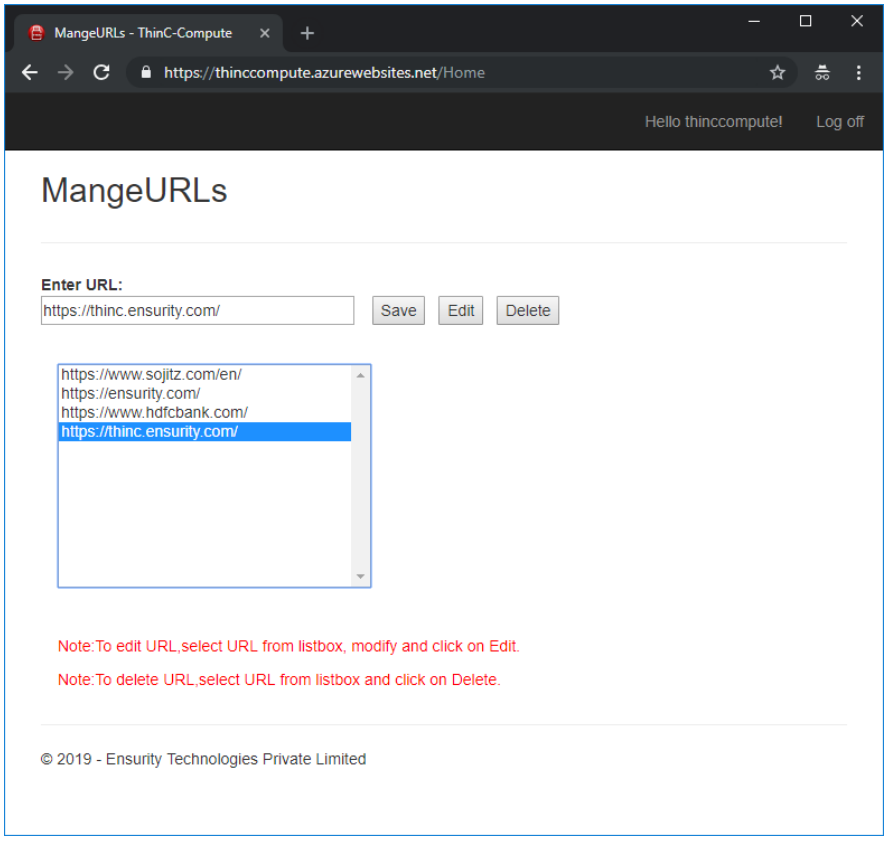


ステップ **3:**

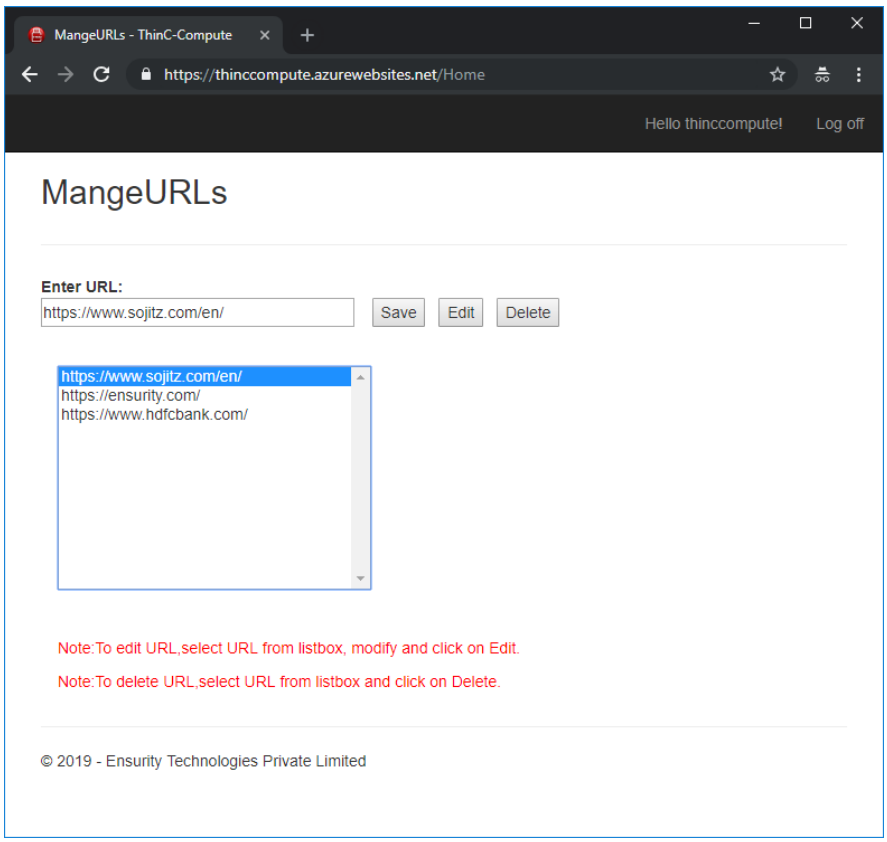
- ホワイトリストに登録する URL を入力し、[保存]をクリックして URL を追加します。



- ホワイトリストから削除する URL をクリックし、削除ボタンをクリックして URL を削除します。



- ホワイトリストから削除する URL をクリックし、削除ボタンをクリックして URL を削除します。

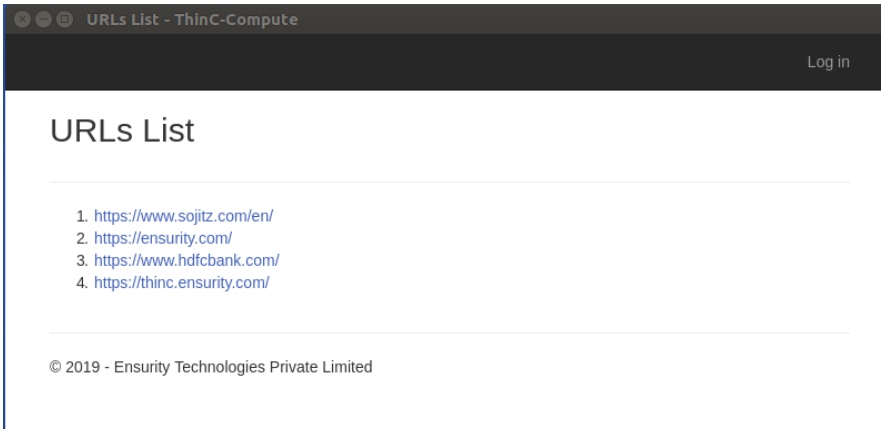


2.5.2 クライアント

セキュアブラウザ（クライアントサブシステム）は https://thinccompute.azurewebsites.net/ Web サイトにのみアクセスするように設定されています。ユーザはウェブサイトにアクセスし、さらにウェブページにリストされているウェブリンクをクリックしてそれに関連するサービスにアクセスすることができます。

- クライアントサブシステムを使用するには、ThinC-Compute を起動し、有線または無線ネットワークを介してインターネットに接続します。
- https://thinccompute.azurewebsites.net/ Web ページのコンテンツにアクセスするには、セキュアブラウザアプリを開きます。

注 - この機能が動作するにはインターネット接続が必須です。



- SecurePage アイコンをクリックして、URL リストに表示されている任意の Web ページリンクを選択します。

例：Ensurity Web ページを示すスクリーンショット。