VeriMark™ Key Manager ユーザーマニュアル macOS 版

Kensington®

Kensington®

目次

Kensington®

はじめに

VeriMark™ Key Manager は、Kensington が提供する公式の管理ツールで、VeriMark™ NFC+ セキュリティキーの設定と管理のために設計されています。

VeriMark™ Key Manager を使用すると、ユーザーは以下のことが可能になります:

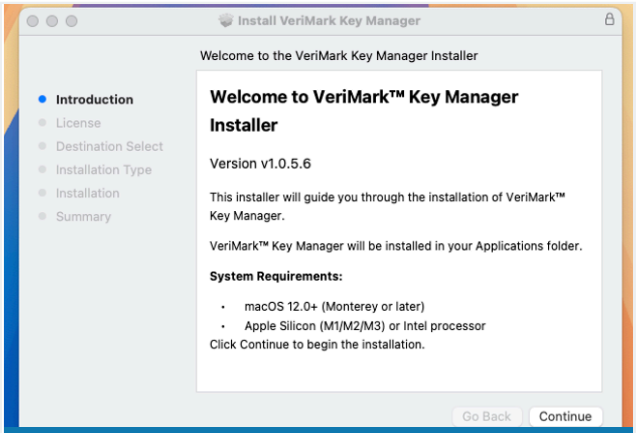
- シリアル番号、FIDO2 バージョン、ファームウェアバージョンなどのデバイス情報を表示する
- PIN およびデジタル証明書を管理する
- FIDO2、PIV、および OTP 機能の操作

macOS 互換性
VeriMark™ Key Manager は、macOS 14 以降で PIV および OTP 機能をサポートして います。
macOS 14 未満のバージョンを実行しているシステムでは、PIV および OTP はサポートさ れておらず、FIDO2 機能のみが利用可能です。

Kensington®

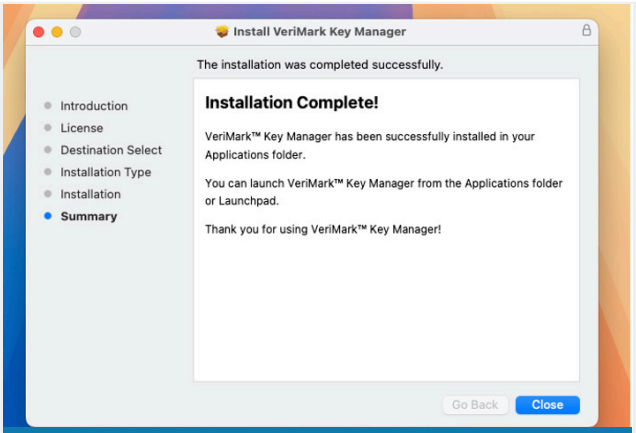
VeriMark™ Key Manager のインストールと使用方法

1. インストール



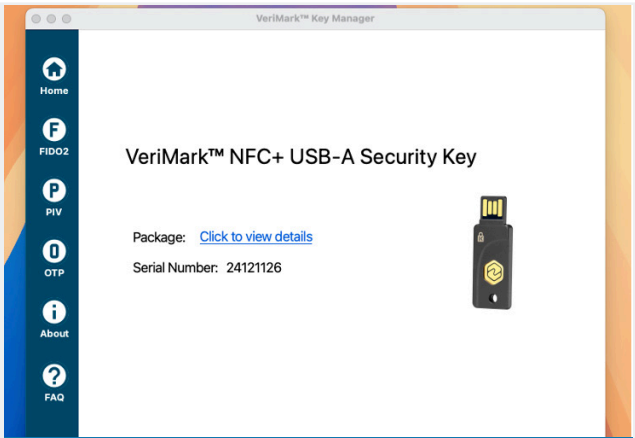
1.1

ダウンロードリンク : kensington.com/verimark-nfc



1.2

.pkg ファイルをダブルクリックしてインストール を開始し、画面の指示に従ってプロセスを完 了してください。



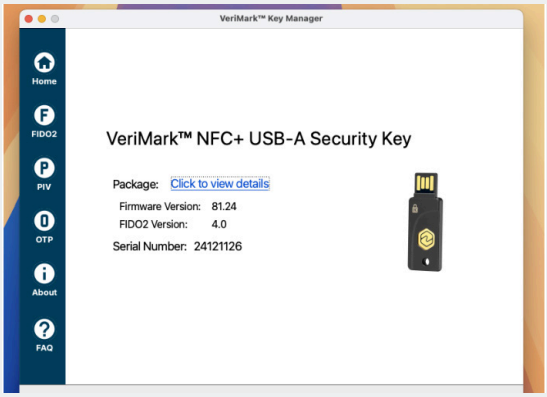
1.3

インストールが完了すると、VeriMark™ キー管 理者を開いて使用を開始できます。

Kensington®

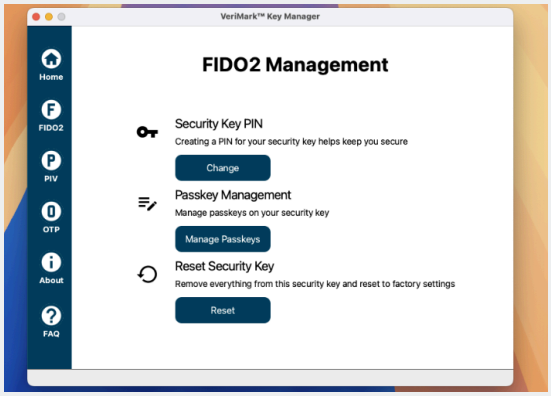
VeriMark™ Key Manager の使用方法

2.1 HOME



VeriMark™ Key Manager を開き、VeriMark™ NFC+ セキュリティキーを挿入すると、ホームページに VeriMark™ NFC+ セキュリティキーに関する情報が表示さ れます。「詳細を表示する」をクリックすると、ファーム ウェアのバージョンと FIDO2 の詳細が表示されます。

2.2 FIDO2

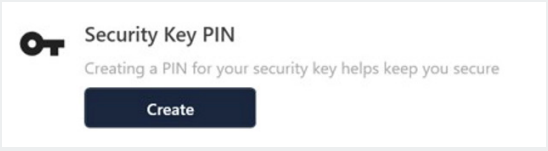


FIDO2 ページでは、PIN の作成 / 変更、パスキー管理、VeriMark™ NFC+ セキュリティキーのリセットを行うこと ができます。

注意すべき重要なポイントが 2 つあります:

- パスキー管理機能はすべてのバージョンでサポートされているわけではありません。
- キーをリセットすると、すべての FIDO® データが消去 されます。これは、以前に他のアプリケーションでセキュリティキーを登録していた場合、キーをリセットした後はログインに使用できず、再登録が必要になることを意味します。

2.2.1 PIN の作成 / 変更

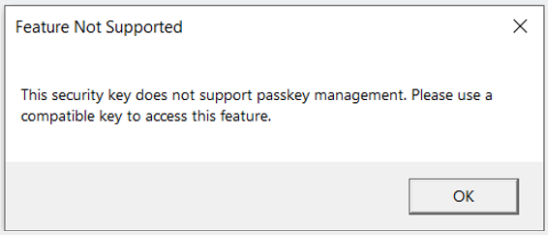


新しい VeriMark™ NFC+ キーには FIDO2 PIN は存在しませ ん。ユーザーは PIN を設定する必要があります。PIN を設 定していない場合、セキュリティキー PIN セクションに表 示されるオプションは「作成」になります。すでに PIN を 設定している場合、表示されるオプションは「変更」にな ります。

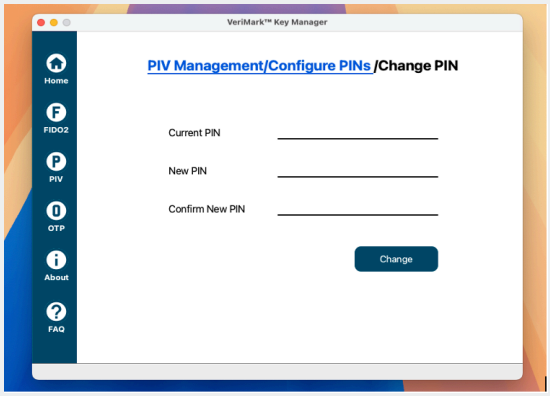
Kensington®

VeriMark™ Key Manager の使用方法

2.2.2 パスキー管理



VeriMark™ NFC+ セキュリティキーがサポートされていない場合、次のメッセージが表示されます。



VeriMark™ NFC+ セキュリティキーがサポートされている場合、FIDO® PIN を入力した後、資格情報管理コマンドをサポートするキーを見ることができます。このページから資格情報を削除できます。

資格情報を削除すると、すべての FIDO® データが消去されることに注意してください。これは、以前に他のアプリケーションでセキュリティキーを登録していた場合、削除後はログインに使用できなくなり、再登録が必要になることを意味します。

2.2.3 セキュリティキーのリセット

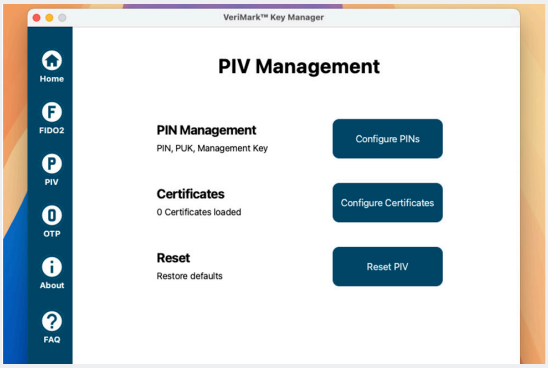
リセットにより、VeriMark™ NFC+ セキュリティキーが初期状態に戻ります。このプロセスでは、FIDO® データがすべて消去され、FIDO2 PIN および以前に登録されたすべてのアプリケーション記録が含まれます。その結果、セキュリティキーは以前に登録されたアプリケーションへのログインに使用できなくなります。引き続き使用するには、各サービスにキーを再登録する必要があります。

リセットプロセスを完了するには、画面の指示に従ってください（VeriMark™ NFC+ セキュリティキーを再挿入し、指定された時間内にタッチします。

Kensington®

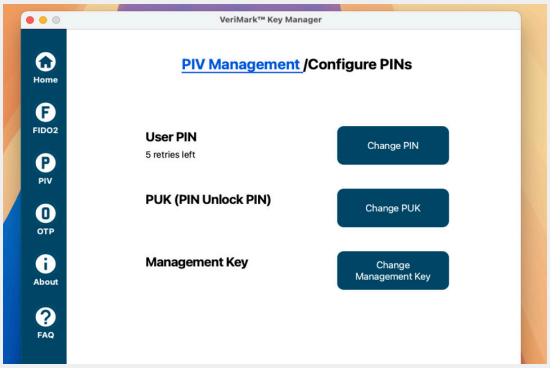
VeriMark™ Key Manager の使用方法

2.3 PIV



PIV ページでは、PIN、PUK、管理キー、および関連する証 明書を管理できます。

2.3.1 PIN 管理

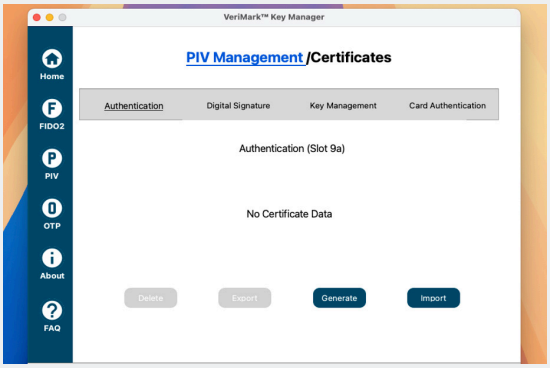


PIN 管理セクションでは、PIV PIN、PUK、および管理キーを管理できます。

デフォルト値は以下の通りです。

- ユーザー PIN：123456
- PUK：12345678
- 管 理 キ ー：010203040506070801020304050607080102030405060708

2.3.2 証明書



証明書ページでは、生成、インポート、エクスポート、削 除などの操作を行うことで証明書を管理できます。プロセ ス中は、ツールが要求する対応するパラメータ(PIV PIN または管理キーなど)を入力して操作を進めてください。

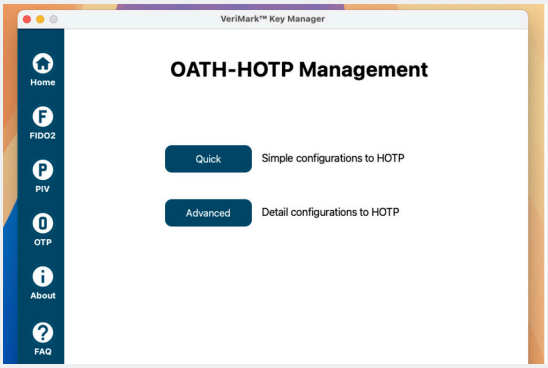
Kensington®

VeriMark™ Key Manager の使用方法

2.3.3 リセット

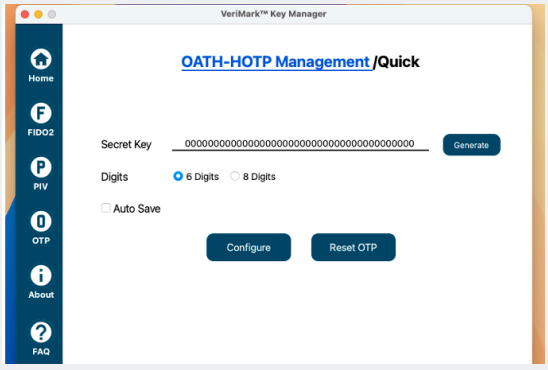
リセットにより、VeriMark™ NFC+ セキュリティキーが初期状態に戻ります。このプロセスでは、すべての PIV データが消去され、PIN、PUK、および管理キーがデフォルト値にリセットされ、すべての保存された証 明書が削除されます。

2.4 OTP

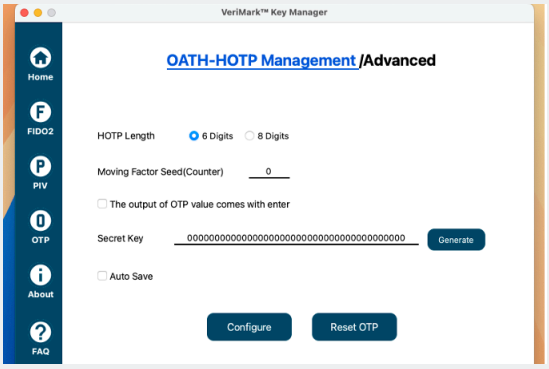


OTP は HOTP タイプをサポートしています。構成は 2 つの モードで利用可能です:クイックとアドバンスドで、ユーザー がニーズに基づいて選択できます。クイックモードは一般ユー ザーに適しており、シンプルなセットアッププロセスを提供 しますが、アドバンスドモードは秘密鍵を手動で入力したり、 カウンターを設定したりするなど、よりカスタマイズ可能な オプションを提供し、高度な要件を持つユーザーに最適です。

2.4.1 QUICK/ADVANCED



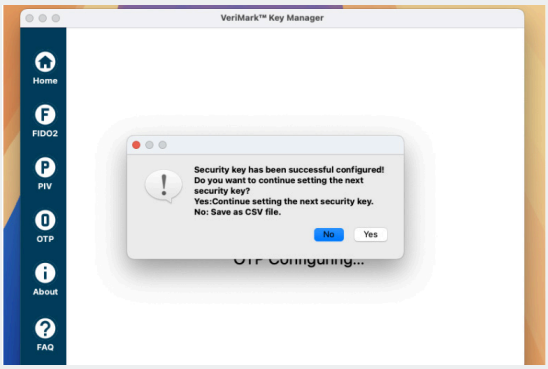
「生成」をクリックすると、秘密鍵を作成するか、特定の秘 密鍵を入力して構成を完了できます。



Kensington®

VeriMark™ Key Manager の使用方法

2.4.1 QUICK/ADVANCED (続き)



最初の VeriMark™ NFC+ セキュリティキーで OTP を設定した後、追加の VeriMark™ NFC+ セキュリティキーを設定するかどうかを尋ねるメッセージが表示されます。設定する場合は、「はい」をクリックし、2 番目、3 番目など を挿入して設定を進めてください。設定しない場合は、「い いえ」をクリックしてください。次に、OTP 構成ファイルを 保存する場所を選択するように求められます。

VeriMark™ Key Manager の設定が完了しました — VeriMark™ NFC+ セキュリティキーの全機能を体験してください。

問い合わせ先： 1-855-692-0054 | sales@kensington.com

Kensington
The Professionals' Choice™