VeriMark™ Key Manager User Manual for Windows

Kensington®

Kensington®

Table of Contents

Kensington®

Introduction

VeriMark™ Key Manager is an official management tool provided by Kensington, designed for configuring and managing the VeriMark™ NFC+ Security Key.

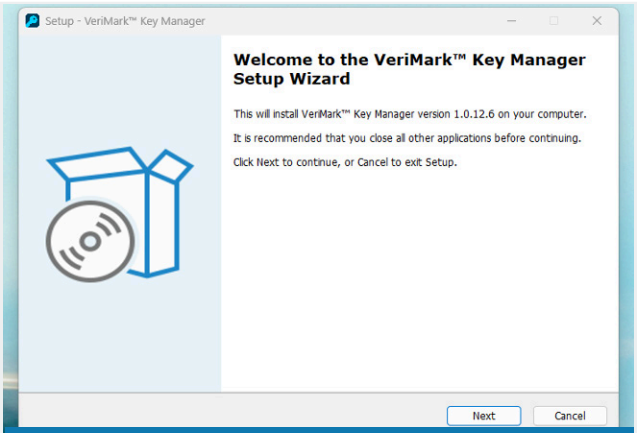
With VeriMark™ Key Manager, users can:

- View device information such as serial number, FIDO2 version, and firmware version
- Manage PIN and digital certificates
- Perform operations for FIDO2, PIV, and OTP functions

Kensington®

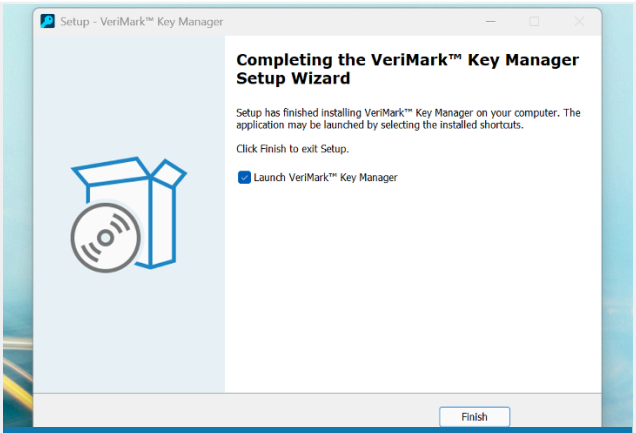
How to Install and Use VeriMark™ Key Manager

1. INSTALL



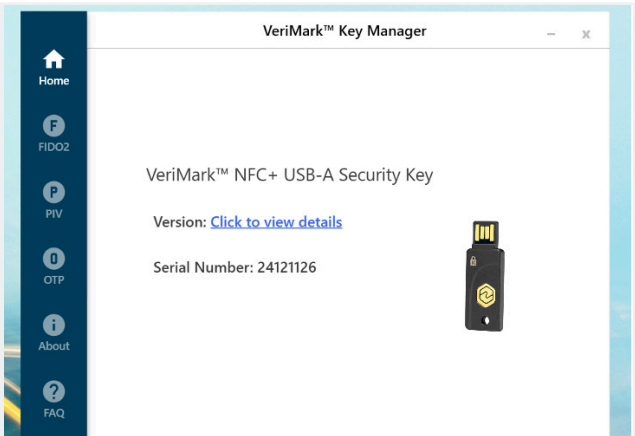
1.1

Download Link:
kensington.com/verimark-nfc



1.2

Double-click the .exe file to begin installation and follow the on-screen instructions to complete the process.



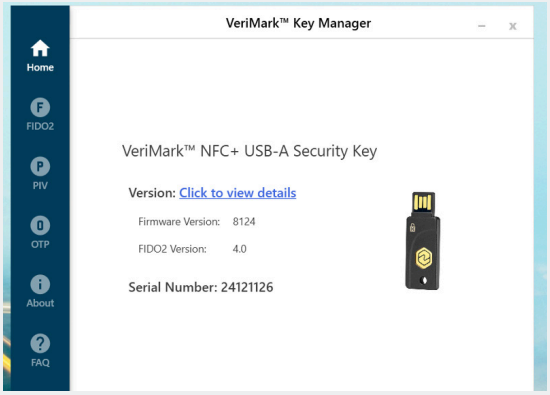
1.3

Once the installation is complete, you can open and start using VeriMark™ Key Manager.

Kensington®

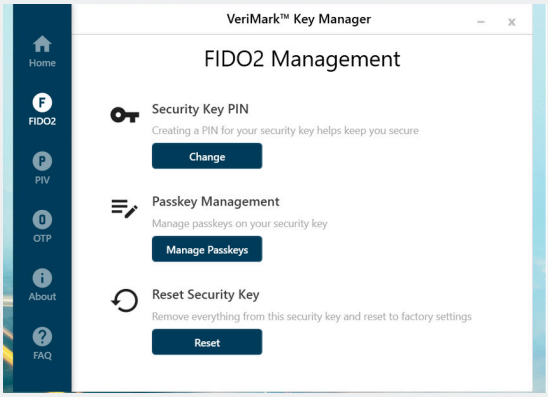
How to Use VeriMark™ Key Manager

2.1 HOME



After opening VeriMark™ Key Manager and inserting the VeriMark™ NFC+ Security Key, you can find relevant information about your VeriMark™ NFC+ Security Key on the home page. Clicking “Click to view details” will display the version of Firmware and FIDO2 details.

2.2 FIDO2



On the FIDO2 page, you can perform Create/Change PIN, Passkey Management, and Reset the VeriMark™ NFC+ Security Key.

There are two important points to note:

- The Passkey Management feature is not supported in all versions.
- Resetting the key will erase all FIDO® data. This means that if you have previously registered your security key with other applications, you will not be able to use it for login after resetting the key and will need to re-register it

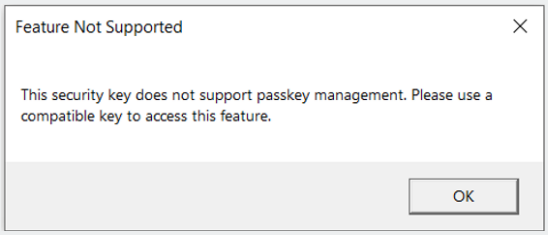
2.2.1 CREATE/CHANGE PIN

The FIDO2 PIN does not exist on the new VeriMark™ NFC+ Security Key. The user needs to set a PIN. If you have not set a PIN, the option displayed in the Security Key PIN section will be “Create.” If you have already set a PIN, the option displayed will be “Change”.

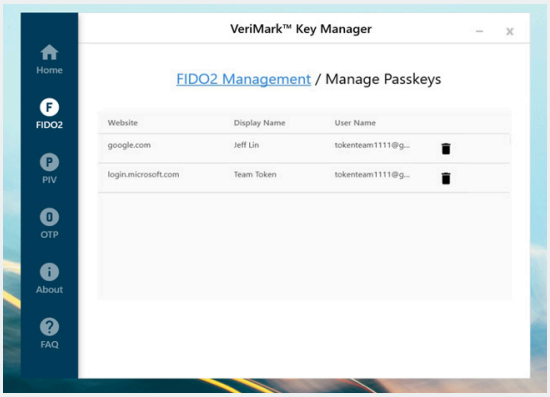
Kensington®

How to Use VeriMark™ Key Manager

2.2.2 PASSKEY MANAGEMENT



If your VeriMark™ NFC+ Security Key is not supported, the following message will be displayed.



If your VeriMark™ NFC+ Security Key is supported, you will be able to see the keys that support the Credential Management command after entering the FIDO® PIN. You can delete credentials from this page.

Please note that deleting the credentials will erase all FIDO® data. This means that if you have previously registered your security key with other applications, you will no longer be able to use it for login after deletion and will need to re-register it.

2.2.3 RESET SECURITY KEY

Resetting the key will restore the VeriMark™ NFC+ Security Key to its initial state. This process will erase all FIDO® data, including the FIDO2 PIN and all previously registered application records. As a result, the security key will no longer work for logging into previously registered applications. To continue using it, you will need to re-register the key with each service.

Please follow the on-screen instructions to complete the reset process (reinsert the VeriMark™ NFC+ Security Key and touch it within the given time).

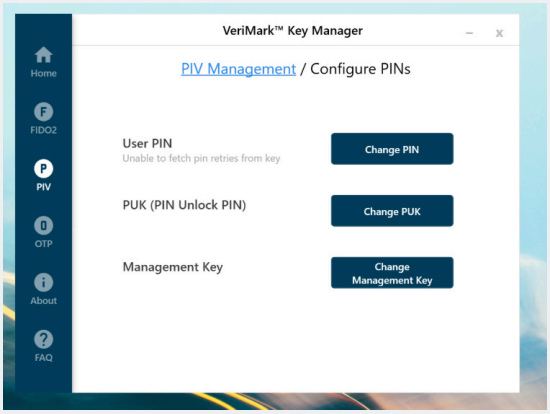
Kensington®

How to Use VeriMark™ Key Manager

2.3 PIV

On the PIV page, you can manage the PIN, PUK, Management Key, as well as the associated certificates.

2.3.1 PIN MANAGEMENT

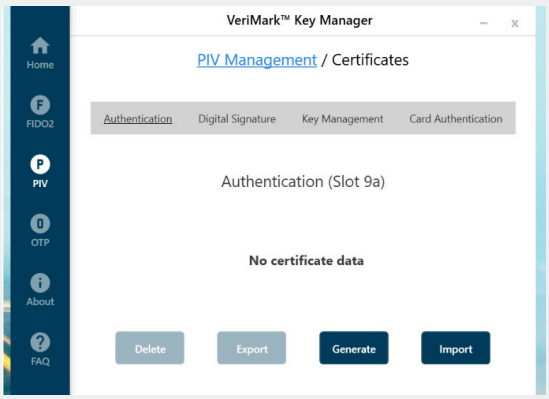


In the PIN Management section, you can manage your PIV PIN, PUK, and Management Key.

The default values are shown below.

- User PIN: 123456
- PUK: 12345678
- Management Key: 010203040506070801020304050607080102030405060708

2.3.2 CERTIFICATES



On the Certificates page, you can manage certificates by performing actions such as Generate, Import, Export, and Delete. During the process, please enter the corresponding parameters as required by the tool, such as the PIV PIN or Management Key, to proceed with the operation.

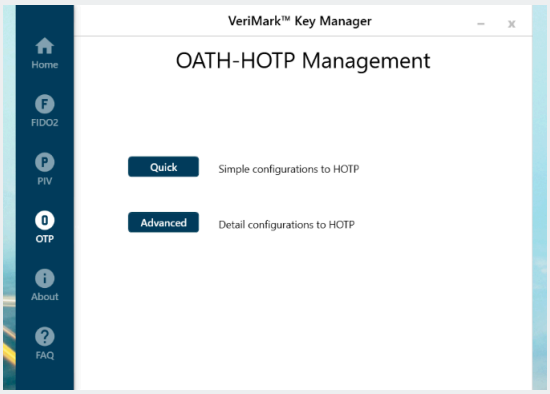
Kensington®

How to Use VeriMark™ Key Manager

2.3.3 RESET

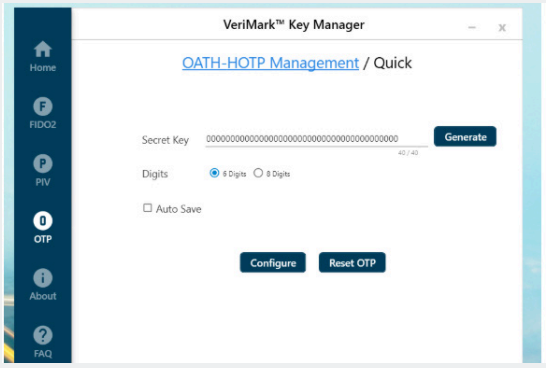
Reset will restore the VeriMark™ NFC+ Security Key to its initial state. This process will erase all PIV data, reset the PIN, PUK, and Management Key to their default values, and delete all stored certificates.

2.4 OTP

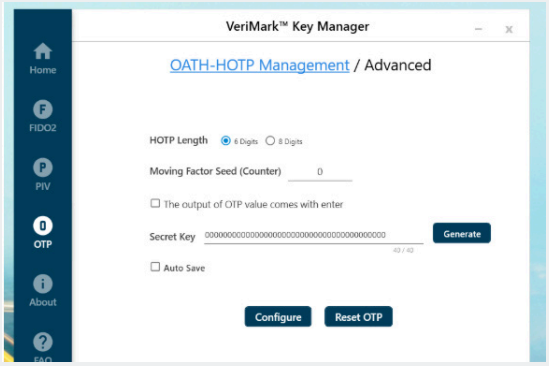


OTP supports the HOTP type. Configuration is available in two modes: Quick and Advanced, allowing users to choose based on their needs. Quick mode is suitable for general users and offers a simple setup process, while Advanced mode provides more customizable options, such as manually entering the secret key and setting the counter, making it ideal for users with advanced requirements.

2.4.1 QUICK/ADVANCED



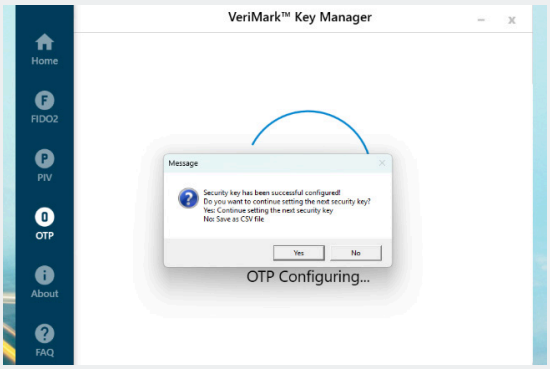
You can click “Generate” to create a Secret Key or enter your own specific Secret Key to complete the configuration.



Kensington®

How to Use VeriMark™ Key Manager

2.4.1 QUICK/ADVANCED (CONT.)



After configuring OTP on the first VeriMark™ NFC+ Security Key, a message will appear asking whether you would like to configure additional VeriMark™ NFC+ Security Keys. If you do, click “Yes” and insert the second, third, and so on to proceed with setup. If not, click “No”. You will then be prompted to choose a location to save the OTP configuration file.

VeriMark™ Key Manager setup is complete — experience the full potential of your VeriMark™ NFC+ Security Key.

FOR MORE INFORMATION CONTACT: 1-855-692-0054 | sales@kensington.com

Kensington
The Professionals’ Choice™