



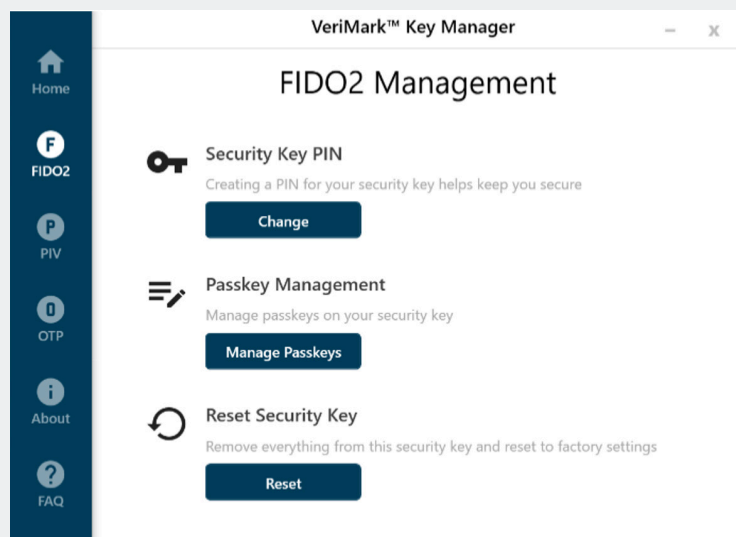
### 1. What is the VeriMark™ NFC+ Security Key?

The VeriMark™ NFC+ Security Key is a physical security device used for authentication that supports FIDO2, PIV, and HOTP. It adds an extra layer of security when accessing accounts and systems.

### 2. How to reset VeriMark™ NFC+ Security Key on Windows?

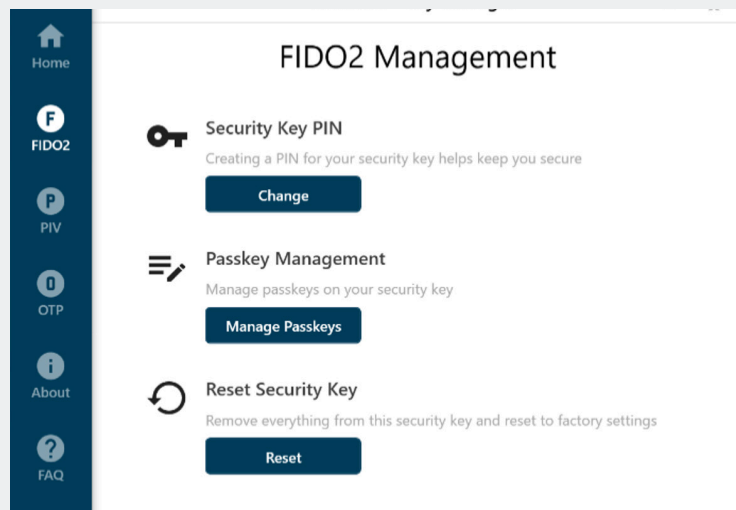
You can download VeriMark™ Key Manager and select “Reset” under the FIDO2 tab, or you can reset it on Windows by opening Settings from the Start menu and selecting the gear icon. Then, navigate to the “Accounts” section. Within “Accounts,” select “Sign-in options.” Locate the option labeled “Security Key.” Once found, click on “Manage” and insert the VeriMark™ NFC+ Security Key. You will then find the reset option available.

Please be aware that resetting the key will erase all FIDO® data. This means if you have previously registered your security key on another application, resetting the security key will render it unusable for login.



### 3. How to change PIN of VeriMark™ NFC+ Security Key on Windows?

You can download VeriMark™ Key Manager and select “Change” under the FIDO2 tab, or you can reset it on Windows by opening Settings from the Start menu and selecting the gear icon. Then, navigate to the “Accounts” section. Within “Accounts,” select “Sign-in options.” Locate the option labeled “Security Key.” Once found, click on “Manage” and insert the VeriMark™ NFC+ Security Key. You will then find the change option available.





#### 4. How to reset the VeriMark™ NFC+ Security Key on macOS?

You can download VeriMark™ Key Manager and select “Reset” under the FIDO2 tab, or reset it on macOS by opening Chrome > Settings > Privacy and Security > Security > Manage security keys, then select Reset your security key. Please be aware that resetting your security key will erase all FIDO® data. This means if you have previously registered your security key on another application, resetting the security key will render it unusable for login.

#### 5. How to change PIN of the VeriMark™ NFC+ Security Key on macOS?

You can download VeriMark™ Key Manager and select “Change” under the FIDO2 tab, or you can change it on macOS via Chrome by opening Chrome’s Settings menu. Then navigate to Privacy and security, select Security, and locate Manage security keys. On that page, you will find the Create a PIN option.

#### 6. How to set up the VeriMark™ NFC+ Security Key on applications?

The VeriMark™ NFC+ Security Key supports account authentication for various applications, and the registration process is mostly similar. Typically, you first enter the account settings screen, then navigate to the security or privacy-related page. Once on that page, you select options related to multi-factor authentication or similar. After clicking into it, you’ll see the option for a security key. At this point, you can register your VeriMark™ NFC+ Security Key.

#### 7. What should I do if I forget my PIN of the VeriMark™ NFC+ Security Key?

Currently, no one except yourself knows the PIN set for the VeriMark™ NFC+ Security Key, and if the maximum number of incorrect PIN entries has been reached, resulting in the VeriMark™ NFC+ Security Key being locked, we can only recommend resetting the VeriMark™ NFC+ Security Key. Please be aware that resetting the key will erase all FIDO® data. This means that if you have previously registered your security key with another application, resetting it will render the key unusable for login.

#### 8. Where can I download VeriMark™ Companion for computer login?

VeriMark™ Companion is only available on mobile devices. Please visit the Google Play Store or Apple App Store to download the app to your device.



### 9. How can enterprise employees apply VeriMark™ NFC+ Security Key for computer login?

If your organization deploys EntraID, please refer to Microsoft's support article below to enable the use of FIDO® Passkeys with Verimark™ NFC+ Security Key enablement.

[How to enable passkey \(FIDO2\) profiles in Microsoft Entra ID \(preview\)](#)

If EntraID is not supported, Passkey login needs to be enabled on the client. Please refer to the Verimark Access software.

### 10. How can individuals apply VeriMark™ NFC+ Security Key for computer login?

As an individual user, you can download VeriMark™ Access from here [kensington.com/verimark-nfc](https://kensington.com/verimark-nfc). VeriMark™ Access is specifically designed for standalone login on Windows using the Kensington VeriMark™ NFC+ Security Key.

Alternatively, you can refer to the following article on using the VeriMark™ NFC+ Security Key to log in to Windows. This requires meeting Microsoft's basic requirements, which are listed at the beginning of the article. If your system meets these requirements, follow the instructions in the article to proceed with the setup.

Related article: [Microsoft Authentication: Passwordless Security Key Login](#)

### 11. What's the maximum number of stored resident keys?

The VeriMark™ NFC+ Security Key can store up to 50 resident keys (passkeys). Once the key reaches this limit, you'll need to remove an existing credential before adding a new one.

### 12. How to delete individual resident keys or view the stored resident keys?

There isn't a direct method to delete or view individual resident keys stored in the FIDO2 storage without performing a complete reset of the security key. The standard procedure for managing resident keys usually involves resetting the security key, which leads to the removal of all stored keys.

### 13. Where is the NFC detection area of smartphone?

The NFC antenna on most smartphones is located near the rear camera. When scanning, hold the VeriMark™ NFC+ Security Key near the top of the phone or camera area. NFC antenna placement may vary by model, so please consult your phone manufacturer's specifications for details.



### 14. What is the PIN of a VeriMark™ NFC+ Security Key?

When you purchase a VeriMark™ NFC+ Security Key, it comes without a default PIN. For applications such as Google account, Facebook, GitHub, and others, when you register your VeriMark™ NFC+ Security Key as a login or two-factor authentication option, the application will prompt you to set a PIN for your VeriMark™ NFC+ Security Key. Once set up, you will be required to enter this PIN whenever prompted to log in.

### 15. Why is my VeriMark™ NFC+ Security Key blocked?

When the message indicating that the VeriMark™ NFC+ Security Key is locked appears, it is usually due to entering the wrong PIN too many times. Once locked, you can only reset it and set a new PIN.

### 16. What should I do if my VeriMark™ NFC+ Security Key is blocked?

When the VeriMark™ NFC+ Security Key is locked and unusable, it usually accompanies a message like "The FIDO® security key has been blocked for security reasons." At this point, you must reset your VeriMark™ NFC+ Security Key to unlock it.

You can download VeriMark™ Key Manager and select "Reset" under the FIDO2 tab. Please keep in mind that resetting the key will erase all FIDO® data, making it unusable for login if registered on another application.

### 17. How to log in to macOS with VeriMark™ NFC+ Key?

Using a VeriMark™ NFC+ Security Key as an option for macOS requires admin account and utilizing the PIV functionality. You must first download VeriMark™ Key Manager.

- PIV Management-Configure PINs:
  1. You can change the PIN, PUK of PIV and management key on this page.
  2. The default PIN of PIV is 123456; The default PUK of PIV is 12345678.
  3. The default management key is 010203040506070801020304050607080102030405060708. You can click the checkbox next to "Use Default" to obtain the management key, this applies if you have never changed the management key.
- PIV Management-Certificates:
  1. You need to generate or import certificates for both Authentication(9a) and Key Management(9d).
  2. Please click "Generate" or "Import".
  3. Then you will need to choose the algorithm. Please note that RSA1024 and ECCP384 are unsupported for macOS login. Please choose RSA2048 or ECCP256
  4. The default PIN of PIV is 123456. You can change PIN of PIV and management key in PIN Management page.
  5. Then click "Confirm".



### 17. How to log in to macOS with VeriMark™ NFC+ Security Key? (cont.)

- Configuring VeriMark™ NFC+ Security Key for macOS account login:
  1. When you insert the VeriMark™ NFC+ Security Key into the macOS device, a notification will appear
  2. Then click "Pair"
  3. If no message appears, you can use a command to bring it up. Open Terminal and enter the command "sc\_auth pairing\_ui -f"
  4. You will be prompted to enter the password and the PIN of PIV
    - Firstly, please enter the password of user's account
    - Secondly, please enter the PIN of PIVs
    - Finally, please enter the password of user's account again
- Log in to macOS:

To verify the setup, lock your Mac and ensure that the password field prompts for a PIN when you insert your VeriMark™ NFC+ Security Key. Attempt to unlock your session using your VeriMark™ NFC+ Security Key by entering the PIN.

### 18. Is VeriMark™ NFC+ Security Key compatible with Apple ID?

Yes, VeriMark™ NFC+ Security Key is suitable for use with Apple ID. You can refer to the following link for information on the required device conditions and setup paths. <https://support.apple.com/en-us/102637>

### 19. I would like to register VeriMark™ NFC+ Security Key as my login method on M365, but I can't find the security key option in Multi-Factor Authentication registration from Microsoft website. What should I do?

Regarding the absence of the security key option in Multi-Factor Authentication registration on M365. Please ensure that the FIDO2 security key option is enabled in the administrator's Windows Entra ID.management system. The administrator can follow the steps below to access the settings:

1. Log in Microsoft Entra admin center
2. Choose Protection/Authentication methods
3. Click Policies > FIDO2 security key
4. Enable FIDO2 security key option

Then the user can check if there is an option to register a security key as part of the multi-factor authentication on M365.



### 20. What are the default PIN, PUK, and management key for PIV?

The default PIN of PIV is 123456.

The default PUK of PIV is 12345678.

The default management key is 010203040506070801020304050607080102030405060708.

### 21. Why does touching my VeriMark™ NFC+ Security Key automatically type a code into a text field?

This happens when your VeriMark™ NFC+ Security Key is configured with HOTP (One-Time Password). When you touch the key, it generates an OTP and automatically enters it into whichever text field is active, including places like the Windows PIN field. This behavior is normal for HOTP-enabled keys.

### 22. What macOS versions support VeriMark™ Key Manager features?

- macOS 14 and above: Supports PIV and OTP features.
- macOS versions below 14: PIV and OTP are not supported; only FIDO2 functions are available.

### 23. Why am I seeing two PIN prompts when using my security key on Android devices?

On some Android devices, users may encounter two PIN prompts when inserting your VeriMark™ NFC+ Security Key. After entering the PIN twice, authentication completes successfully. This behavior appears to be related to the Android operating system rather than the key itself.

**Q:** Does this issue affect the functionality of the key?

**A:** No. Despite the double PIN prompt, the key functions correctly and authentication is successful.

**Q:** Which devices and OS versions are affected?

**A:** Here's a summary of tested devices and their behavior:

Device	OS Version	VeriMark NFC+ Behavior
Samsung A53	Android 14	Two PIN prompts; authentication successful
Samsung A53	Android 15	Occasional issue; authentication successful
Samsung S23+	Android 15 & 16	Works normally
Samsung Z Flip 4/5	Android 14 - 16	Works normally
Sony Xperia	Android 15	Works normally
Google Pixel 7/10	Android 16	Two PIN prompts; authentication successful



### 24. Why doesn't my VeriMark™ NFC+ Security Key work with Safari on macOS when I have multiple keys registered to my account?

Safari may fail to recognize NFC security keys when too many keys are registered to a single user account. This happens because Safari attempts to process all registered keys simultaneously during authentication, which can overwhelm the memory capacity of NFC keys.

To resolve this issue, remove any unnecessary registered security keys from your account, clear your browser cache, and try logging in again.

### 25. Why does the on-screen keyboard not appear when entering the FIDO® PIN?

On smartphones and tablets, users typically rely on the on-screen keyboard for text input. However, when a USB security key is connected, some operating systems may detect the key as a hardware keyboard and automatically hide the on-screen keyboard. This can affect entering the FIDO® PIN or interacting with certain UI elements.

Some security keys expose an OTP function through a USB Keyboard HID interface. When a mobile device detects a hardware keyboard, the OS may suppress the soft keyboard. The actual behavior varies across manufacturers, OS versions, and device models.

#### Platform Behaviors

- Android and newer
  - The historical setting
    - System > Keyboard > Physical keyboard > Use on-screen keyboard has been removed in Android 16.
- Users must manually trigger the soft keyboard
  1. Tap the PIN text field
  2. Tap the floating keyboard icon
  3. Select "Show on-screen keyboard"
- Android and newer
  - Users may enable:
    - Settings > System > Keyboard > Physical keyboard > Use on-screen keyboard

#### iPhone / iPadOS (iOS & iPadOS)

iOS/iPadOS also treat the USB security key as a hardware keyboard.

#### Observed Behaviors:

- When the VeriMark™ Key is plugged in, the soft keyboard may not appear for normal text input.
- Removing the key restores the soft keyboard.
- Important: When operating FIDO® functions (such as entering the FIDO® PIN), iOS/iPadOS do correctly display the soft keyboard even with the security key plugged in.
- The historical setting

# Kensington®

## VeriMark™ NFC+ Security Key FAQ



### 25. Why does the on-screen keyboard not appear when entering the FIDO® PIN? (cont.)

This is expected OS behavior and not a device malfunction.

Apple currently does not offer system-level settings to override this behavior when a hardware keyboard is detected.

#### Summary

- Mobile operating systems may hide the on-screen keyboard when a hardware keyboard is detected
- Behavior varies depending on OS version and device model
- Android 16 requires manual soft keyboard activation
- iOS/iPadOS suppress the keyboard in general text fields, but still present it correctly during FIDO® PIN entry



All specifications are subject to change without notice. Products may not be available in all markets. Kensington® and Kensington, The Professionals' Choice™ are trademarks of ACCO Brands. All other registered and unregistered trademarks are the property of their respective owners. © 2026 Kensington Computer Products Group, a division of ACCO Brands. K26\_4494

**FOR MORE INFORMATION CONTACT:** 1-855-692-0054 | [sales@kensington.com](mailto:sales@kensington.com)

# Kensington

The Professionals' Choice™