Kensington®

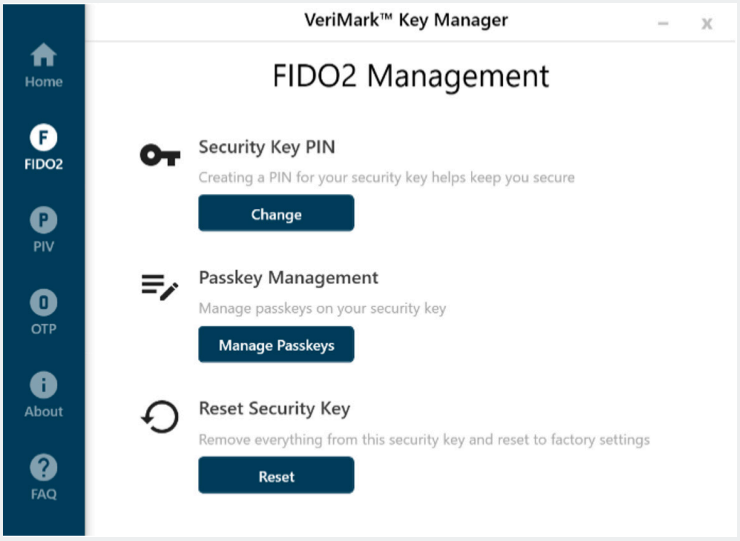
VeriMark™ NFC+ Security Key FAQ

1. Qu'est-ce que la clé de sécurité VeriMark™ NFC+?

La clé de sécurité VeriMark™ NFC+ est un dispositif physique d'authentification compatible avec FIDO2, PIV et HOTP. Elle ajoute une couche de sécurité supplémentaire lors de l'accès aux comptes et aux systèmes.

2. Comment réinitialiser la clé de sécurité VeriMark™ NFC+ dans Windows?

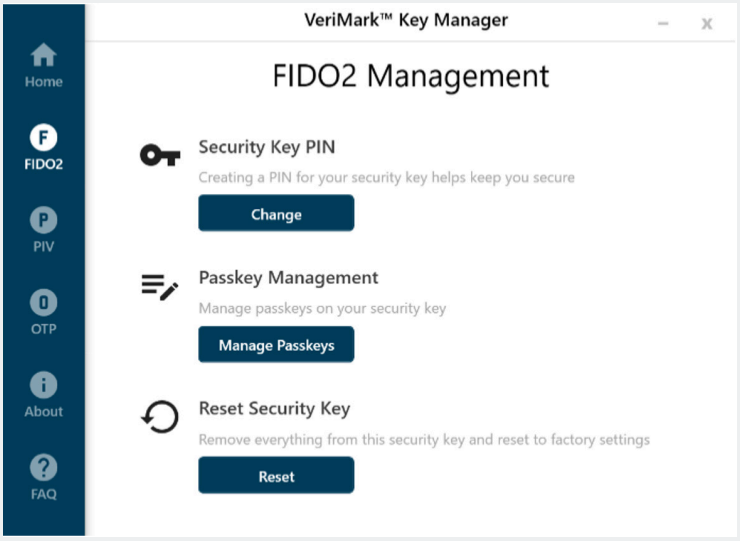
Vous pouvez télécharger VeriMark™ Key Manager et choisir « Réinitialiser » sous l'onglet FIDO2, ou réinitialiser la clé dans Windows en ouvrant les Paramètres à partir du menu Démarrer et en sélectionnant l'icône d'engrenage. Allez ensuite dans la section « Comptes ». Dans « Comptes », sélectionnez « Options de connexion ». Trouvez l'option « Clé de sécurité ». Une fois repérée, cliquez sur « Gérer » et insérez la clé de sécurité VeriMark™ NFC+. Vous verrez alors l'option de réinitialisation.



Veuillez noter que réinitialiser la clé efface toutes les données FIDO®. Si la clé a été enregistrée dans une autre application, elle ne pourra plus être utilisée pour la connexion après réinitialisation.

3. Comment modifier le NIP de la clé de sécurité VeriMark™ NFC+ dans Windows?

Vous pouvez télécharger VeriMark™ Key Manager et choisir « Modifier » sous l'onglet FIDO2, ou modifier le NIP dans Windows en ouvrant les Paramètres à partir du menu Démarrer et en sélectionnant l'icône d'engrenage. Ensuite, allez dans la section « Comptes ». Dans « Comptes », choisissez « Options de connexion ». Trouvez la mention « Clé de sécurité ». Une fois repérée, cliquez sur « Gérer » et insérez votre clé de sécurité VeriMark™ NFC+. L'option de modification du NIP apparaîtra.



Kensington®

VeriMark™ NFC+ Security Key FAQ

4. Comment réinitialiser la clé de sécurité VeriMark™ NFC+ sur macOS?

Vous pouvez télécharger VeriMark™ Key Manager et choisir « Réinitialiser » sous l'onglet FIDO2, ou réinitialiser la clé dans macOS en ouvrant Chrome puis Paramètres > Confidentialité et sécurité > Sécurité > Gérer les clés de sécurité, puis en sélectionnant « Réinitialiser la clé de sécurité ». Notez que la réinitialisation supprime toutes les données FIDO®. Si la clé a été enregistrée dans une autre application, elle ne pourra plus être utilisée pour la connexion après réinitialisation.

5. Comment modifier le NIP de la clé de sécurité VeriMark™ NFC+ sur macOS?

Vous pouvez télécharger VeriMark™ Key Manager et choisir « Modifier » dans l'onglet FIDO2, ou modifier le NIP sur macOS via Chrome en ouvrant le menu des paramètres de Chrome. Accédez ensuite à Confidentialité et sécurité, sélectionnez Sécurité, puis trouvez Gérer les clés de sécurité. Sur cette page, vous verrez l'option « Créer un NIP ».

6. Comment configurer la clé de sécurité VeriMark™ NFC+ dans les applications?

La clé de sécurité VeriMark™ NFC+ prend en charge l'authentification des comptes dans plusieurs applications, et le processus d'inscription est généralement similaire. Vous devez d'abord ouvrir les paramètres du compte, puis accéder à la page de sécurité ou de confidentialité. À cet endroit, sélectionnez les options liées à l'authentification multifacteur ou similaires. Après avoir cliqué, l'option pour ajouter une clé de sécurité apparaîtra. Vous pourrez alors enregistrer votre clé VeriMark™ NFC+.

7. Que dois-je faire si j'oublie le NIP de ma clé de sécurité VeriMark™ NFC+?

Seule vous connaissez le NIP défini pour votre clé de sécurité VeriMark™ NFC+. Si le nombre maximal de tentatives incorrectes est atteint et que la clé est verrouillée, nous recommandons de réinitialiser la clé VeriMark™ NFC+.

Veuillez noter que la réinitialisation supprimera toutes les données FIDO®. Si vous aviez enregistré votre clé dans une autre application, elle ne pourra plus être utilisée pour vous connecter après la réinitialisation.

8. Où puis-je télécharger VeriMark™ Companion pour la connexion à l'ordinateur?

VeriMark™ Companion est offert uniquement sur les appareils mobiles. Veuillez visiter le Google Play Store ou l'Apple App Store pour télécharger l'application sur votre appareil.

Kensington®

VeriMark™ NFC+ Security Key FAQ

9. Comment les employés d'entreprise peuvent-ils utiliser la clé de sécurité VeriMark™ NFC+ pour la connexion à l'ordinateur?

Si votre organisation utilise EntralD, veuillez consulter l'article de soutien Microsoft ci-dessous afin d'activer l'utilisation des passkeys FIDO® avec la clé de sécurité VeriMark™ NFC+.

Comment activer les profils de passkey (FIDO2) dans Microsoft Entra ID (aperçu)

Si EntralD n'est pas pris en charge, la connexion par passkey doit être activée sur le poste client. Veuillez vous référer au logiciel Verimark Access.

10. Comment les utilisateurs individuels peuvent-ils utiliser la clé de sécurité VeriMark™ NFC+ pour la connexion à l'ordinateur?

À titre d'utilisateur individuel, vous pouvez télécharger VeriMark™ Access à l'adresse kensington.com/verimark-nfc. VeriMark™ Access est spécialement conçu pour la connexion autonome à Windows avec la clé de sécurité Kensington VeriMark™ NFC+.

Vous pouvez également consulter l'article suivant portant sur l'utilisation de la clé de sécurité VeriMark™ NFC+ pour ouvrir une session dans Windows. Cela nécessite de répondre aux exigences de base de Microsoft, énumérées au début de l'article. Si votre système les satisfait, suivez les instructions proposées pour procéder à la configuration.

Article connexe : Microsoft Authentication : Passwordless Security Key Login

11. Quel est le nombre maximal de clés résidentes pouvant être stockées?

La clé de sécurité VeriMark™ NFC+ peut stocker jusqu'à 50 clés résidentes (passkeys). Une fois cette limite atteinte, vous devrez supprimer un identifiant existant avant d'en ajouter un nouveau.

12. Comment supprimer des clés résidentes individuelles ou voir les clés résidentes stockées?

Il n'existe aucun moyen direct de supprimer ou d'afficher des clés résidentes individuelles dans le stockage FIDO2 sans réinitialiser complètement la clé de sécurité. La procédure habituelle pour gérer les clés résidentes consiste à réinitialiser la clé, ce qui supprime toutes les clés enregistrées.

13. Où se trouve la zone de détection NFC d'un téléphone intelligent?

L'antenne NFC de la plupart des téléphones intelligents se situe près de la caméra arrière. Pour effectuer une lecture, tenez la clé de sécurité VeriMark™ NFC+ près du haut de l'appareil ou de la zone de la caméra. L'emplacement de l'antenne NFC peut varier selon le modèle ; veuillez consulter les spécifications du fabricant de votre appareil.

Kensington®

VeriMark™ NFC+ Security Key FAQ

14. Quel est le NIP d'une clé de sécurité VeriMark™ NFC+?

Lorsque vous achetez une clé de sécurité VeriMark™ NFC+, elle n'est fournie avec aucun NIP par défaut. Pour des applications comme Google, Facebook, GitHub et autres, lorsque vous enregistrez votre clé VeriMark™ NFC+ comme méthode de connexion ou d'authentification à deux facteurs, l'application vous demandera de définir un NIP. Une fois configuré, vous devrez saisir ce NIP chaque fois qu'il sera requis pour vous connecter.

15. Pourquoi ma clé de sécurité VeriMark™ NFC+ est-elle bloquée?

Lorsque le message indiquant que la clé de sécurité VeriMark™ NFC+ est verrouillée apparaît, cela est généralement dû à un trop grand nombre de tentatives de NIP erronées. Une fois verrouillée, vous ne pouvez que la réinitialiser et définir un nouveau NIP.

16. Que dois-je faire si ma clé de sécurité VeriMark™ NFC+ est bloquée?

Lorsque la clé de sécurité VeriMark™ NFC+ est verrouillée et inutilisable, un message tel que « La clé de sécurité FIDO® a été bloquée pour des raisons de sécurité » apparaît généralement. Dans ce cas, vous devez réinitialiser votre clé VeriMark™ NFC+ pour la déverrouiller.

Vous pouvez télécharger VeriMark™ Key Manager et choisir « Réinitialiser » dans l'onglet FIDO2. Veuillez noter que la réinitialisation supprimera toutes les données FIDO®, ce qui rendra la clé inutilisable pour la connexion si elle avait été enregistrée dans une autre application.

17. Comment ouvrir une session sur macOS avec la clé VeriMark™ NFC+?

L'utilisation de la clé de sécurité VeriMark™ NFC+ sur macOS nécessite un compte administrateur et la fonctionnalité PIV. Vous devez d'abord télécharger VeriMark™ Key Manager.

- Gestion PIV – Configuration du NIP :
  1. Vous pouvez modifier le NIP, le PUK et la clé de gestion PIV sur cette page.
  2. Le NIP par défaut de PIV est 123456 ; le PUK par défaut est 12345678.
  3. La clé de gestion par défaut est 010203040506070801020304050607080102030405060708. Vous pouvez cocher « Utiliser la valeur par défaut » si vous ne l'avez jamais modifiée.
- Gestion PIV – Certificats :
  1. Vous devez générer ou importer des certificats pour l'authentification (9a) et la gestion des clés (9d).
  2. Cliquez sur « Générer » ou « Importer ».
  3. Choisissez ensuite l'algorithme. Notez que RSA1024 et ECCP384 ne sont pas pris en charge pour la connexion macOS. Choisissez RSA2048 ou ECCP256.
  4. Le NIP par défaut de PIV est 123456. Vous pouvez modifier le NIP et la clé de gestion dans la page de gestion des NIP.
  5. Cliquez sur « Confirmer ».

Kensington®

VeriMark™ NFC+ Security Key FAQ

17. Comment ouvrir une session sur macOS avec la clé VeriMark™ NFC+? (suite)

- Configuration de la clé pour macOS :
  1. Une notification apparaît lors de l'insertion.
  2. Cliquez sur « Associer ».
  3. Si rien n'apparaît, lancer : sc_auth pairing_ui -f
  4. Entrer :
     - Mot de passe.
     - NIP de PIV.
     - Mot de passe encore.
- Connexion macOS :

  Insérez la clé et entrez le NIP pour déverrouiller.

18. La clé de sécurité VeriMark™ NFC+ est-elle compatible avec l'identifiant Apple?

La clé de sécurité VeriMark™ NFC+ est-elle compatible avec l'identifiant Apple : https://support.apple.com/en-us/102637

19. Je souhaite enregistrer la clé VeriMark™ NFC+ comme méthode de connexion dans M365, mais je ne vois pas l'option de clé de sécurité dans l'inscription MFA. Que dois-je faire?

Si l'option n'est pas affichée, assurez-vous que la clé de sécurité FIDO2 est activée dans Microsoft Entra ID. L'administrateur doit :

1. Se connecter au centre d'administration Microsoft Entra
2. Choisir Protection/Méthodes d'authentification
3. Cliquer sur Politiques > Clé de sécurité FIDO2
4. Activer l'option FIDO2

Ensuite, l'utilisateur pourra vérifier si l'option apparaît dans l'enregistrement MFA.

20. Quels sont le NIP, le PUK et la clé de gestion par défaut pour PIV?

Le NIP par défaut de PIV est 123456.
Le PUK par défaut est 12345678.
La clé de gestion par défaut est 010203040506070801020304050607080102030405060708.

Kensington®

VeriMark™ NFC+ Security Key FAQ

21. Pourquoi ma clé VeriMark™ NFC+ inscrit-elle automatiquement un code lorsque je la touche?

Cela se produit lorsque votre clé est configurée avec HOTP (mot de passe à usage unique). En la touchant, elle génère un code et l'inscrit automatiquement dans le champ actif, y compris le champ du NIP Windows. Ce comportement est normal pour les clés HOTP.

22. Quelles versions de macOS prennent en charge les fonctions de VeriMark™ Key Manager?

- macOS 14 et plus : prend en charge les fonctionnalités PIV et OTP.
- Versions antérieures à macOS 14 : PIV et OTP ne sont pas pris en charge; seules les fonctions FIDO2 sont disponibles.

23. Pourquoi est-ce que deux demandes de NIP apparaissent lorsque j'utilise ma clé de sécurité sur Android?

Sur certains appareils Android, deux demandes de NIP peuvent apparaître lors de l'utilisation de la clé VeriMark™ NFC+. Après avoir entré le NIP deux fois, l'authentification réussit. Ce comportement semble lié au système Android plutôt qu'à la clé elle-même.

Q: Ce problème affecte-t-il la fonctionnalité de la clé?
R: Non. La clé fonctionne correctement malgré la double demande de NIP.

Q: Quels appareils et versions Android sont touchés?
R: Voici un résumé des appareils testés et de leur comportement :

Appareil	Version du Système	Comportement VeriMark NFC+
Samsung A53	Android 14	Deux demandes de NIP ; authentification réussie
Samsung A53	Android 15	Problème occasionnel ; authentification réussie
Samsung S23+	Android 15 & 16	Fonctionne normalement
Samsung Z Flip 4/5	Android 14 - 16	Fonctionne normalement
Sony Xperia	Android 15	Fonctionne normalement
Google Pixel 7/10	Android 16	Deux demandes de NIP ; authentification réussie

Kensington®

VeriMark™ NFC+ Security Key FAQ

24. Pourquoi ma clé VeriMark™ NFC+ ne fonctionne-t-elle pas avec Safari sur macOS lorsque plusieurs clés sont enregistrées dans mon compte?

Safari peut avoir du mal à reconnaître les clés NFC lorsqu'un trop grand nombre de clés sont associées à un même compte utilisateur. Safari tente de traiter toutes les clés enregistrées en même temps, ce qui peut dépasser la capacité mémoire des clés NFC.

Pour corriger le problème, supprimez les clés inutiles de votre compte, videz le cache du navigateur et essayez de vous reconnecter.

25. Pourquoi le clavier à l'écran ne s'affiche-t-il pas lors de la saisie du NIP FIDO®?

Sur les téléphones et tablettes, les utilisateurs s'appuient normalement sur le clavier à l'écran pour saisir du texte. Toutefois, lorsqu'une clé de sécurité USB est branchée, certains systèmes peuvent la détecter comme un clavier physique et masquer automatiquement le clavier à l'écran, ce qui peut nuire à la saisie du NIP FIDO®.

Certaines clés de sécurité offrent une fonction OTP via une interface USB Keyboard HID. Lorsqu'un appareil mobile détecte un clavier matériel, le système peut empêcher l'affichage du clavier virtuel. Le comportement peut varier selon le fabricant, la version du système et le modèle de l'appareil.

Comportement des plateformes

- Android et plus récent
  - L'ancien paramètre
    - Système > Clavier > Clavier physique > Utiliser le clavier à l'écran a été retiré dans Android 16.
- L'utilisateur doit activer manuellement le clavier virtuel
  1. Appuyer sur le champ du NIP
  2. Appuyer sur l'icône flottante du clavier
  3. Sélectionner « Afficher le clavier à l'écran »
- Android et plus récent
  - Possibilité d'activer:
    - Réglages > Système > Clavier > Clavier physique > Utiliser le clavier à l'écran

iPhone / iPadOS (iOS & iPadOS)

iOS/iPadOS traitent aussi la clé USB comme un clavier matériel.

Comportements observés :

- Lorsque la clé VeriMark™ est branchée, le clavier à l'écran peut ne pas apparaître pour la saisie normale.
- Le retrait de la clé rétablit le clavier.
- Important : lors des opérations FIDO® (telles que la saisie du NIP FIDO®), iOS/iPadOS affichent correctement le clavier même si la clé est branchée.
- L'ancien paramètre.

Kensington®

VeriMark™ NFC+ Security Key FAQ

25. Pourquoi le clavier à l'écran ne s'affiche-t-il pas lors de la saisie du NIP FIDO®? (suite)

Il s'agit d'un comportement normal du système d'exploitation et non d'un problème avec l'appareil.

Apple n'offre pas actuellement d'option système permettant de contourner ce comportement lorsqu'un clavier matériel est détecté.

Résumé

- Les systèmes d'exploitation mobiles peuvent masquer le clavier à l'écran lorsqu'un clavier matériel est détecté
- Le comportement varie selon la version du système et le modèle de l'appareil
- Android 16 nécessite l'activation manuelle du clavier virtuel
- iOS/iPadOS suppriment le clavier dans les champs de texte généraux, mais l'affichent correctement lors de la saisie du NIP FIDO®

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

Kensington
The Professionals' Choice™