Présentation, fonctionnalités et usages en environnement professionnel

La clé de sécurité YubiKey 5 NFC

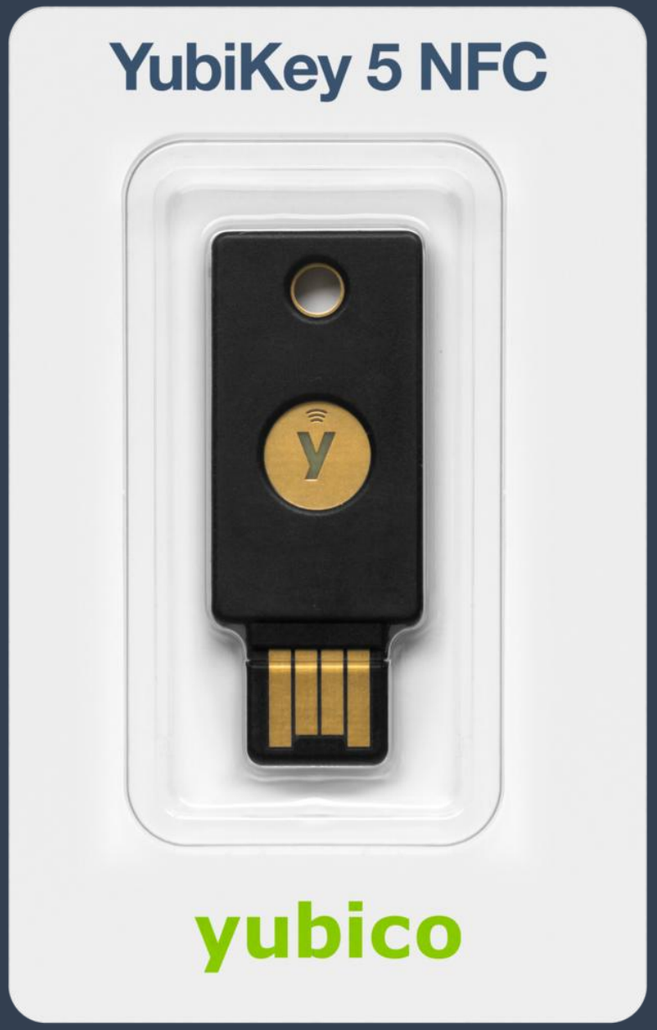
Qu'est-ce qu'une YubiKey ?

Définition

Clé d'authentification matérielle développée par l'entreprise Yubico, servant à prouver l'identité de l'utilisateur de manière physique et sécurisée.

Objectif principal

Renforcer la sécurité des connexions en éliminant les vulnérabilités liées aux mots de passe et en réduisant drastiquement les risques de phishing.



Présentation de la YubiKey 5 NFC

Caractéristiques techniques

- Clé physique avec connecteur USB-A
- Technologie NFC intégrée pour usage mobile
- Aucune batterie requise
- Construction robuste pour usage professionnel intensif
- Résistante à l'eau et aux chocs (Certifié IP68)

Compatibilité étendue

Systèmes d'exploitation : Windows, Linux, macOS

Appareils : ordinateurs de bureau, portables, smartphones et tablettes compatibles NFC

Services : Microsoft 365, Google Workspace, AWS, et des centaines d'autres plateformes..

FONCTIONNALITÉS

Standards et protocoles supportés

FIDO2 / WebAuthn

Authentification moderne sans mot de passe, basée sur la cryptographie asymétrique et résistante au phishing.

OTP (One-Time Password)

Génération de mots de passe à usage unique pour une sécurité renforcée lors de chaque connexion.

Carte à puce PIV

Support du standard PIV pour l'authentification dans les environnements gouvernementaux et d'entreprise.

OpenPGP

Chiffrement et signature numérique pour la protection des communications et des données sensibles.

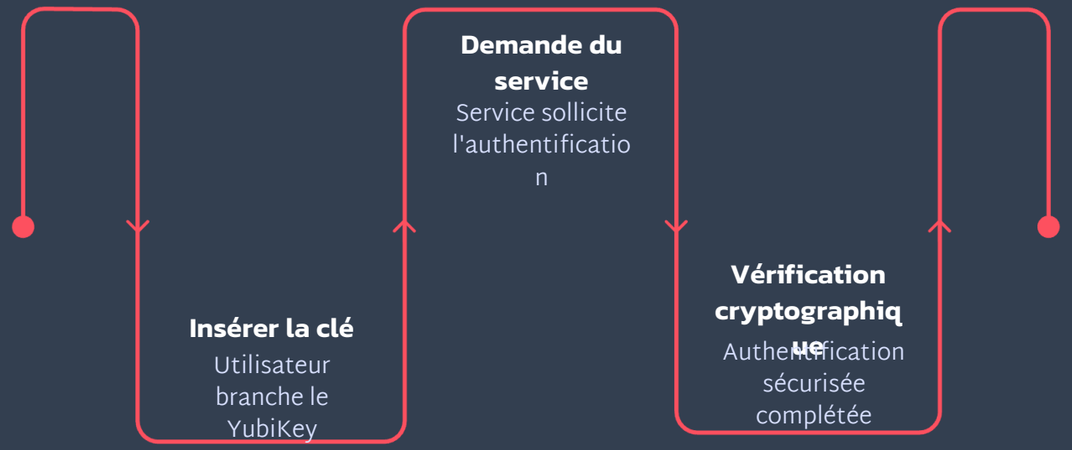
Une seule clé physique pour répondre à de multiples besoins de sécurité professionnels

Focus : FIDO2 / WebAuthn

Principe d'authentification moderne

FIDO2 représente la nouvelle génération d'authentification, permettant des connexions **sans mot de passe** tout en garantissant une sécurité maximale.

Le système repose sur la **cryptographie asymétrique** : une paire de clés publique/privée unique est générée pour chaque service.



La clé privée ne quitte jamais la YubiKey, rendant toute attaque de phishing impossible, même si l'utilisateur visite un site malveillant.

YubiKey et écosystème Microsoft

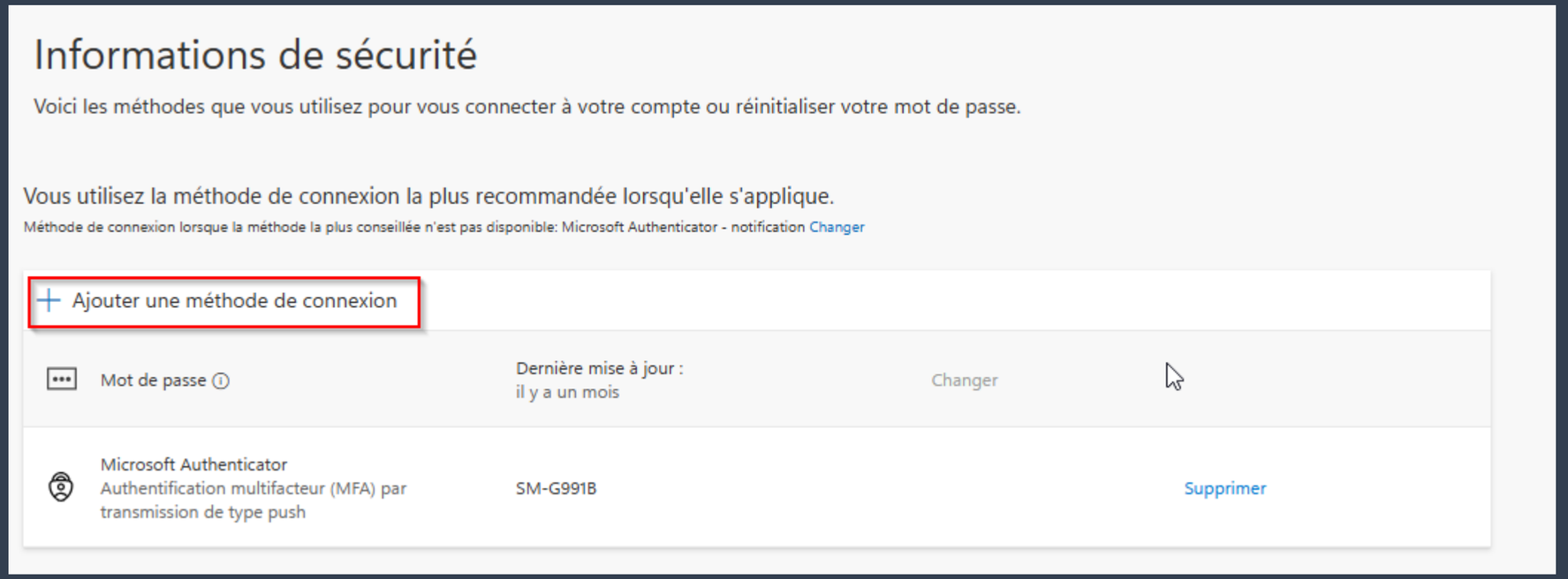
Microsoft 365

Sécurisation complète des accès à la suite bureautique cloud : Outlook, Teams, OneDrive, SharePoint et toutes les applications intégrées.

Authentification multifacteur

Remplacement des méthodes MFA traditionnelles (SMS, applications authenticator) par une authentification matérielle inviolable, permettant même la connexion sans mot de passe si souhaité.

Ajouter Ubikey dans Microsoft 365



Informations de sécurité

Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.

Vous utilisez la méthode de connexion la plus recommandée lorsqu'elle s'applique.

Méthode de connexion lorsque la méthode la plus conseillée n'est pas disponible: Microsoft

+ Ajouter une méthode de connexion

Mot de passe ⓘ	Dernière mise il y a un mois	
Microsoft Authenticator Authentification multifacteur (MFA) par transmission de type push	SM-G991B	

Appareil perdu ? Se déconnecter partout

Ajouter une méthode de connexion

Clé d'accès dans Microsoft Authenticator
Connectez-vous à l'aide de votre visage, de votre empreinte digitale, de votre code PIN

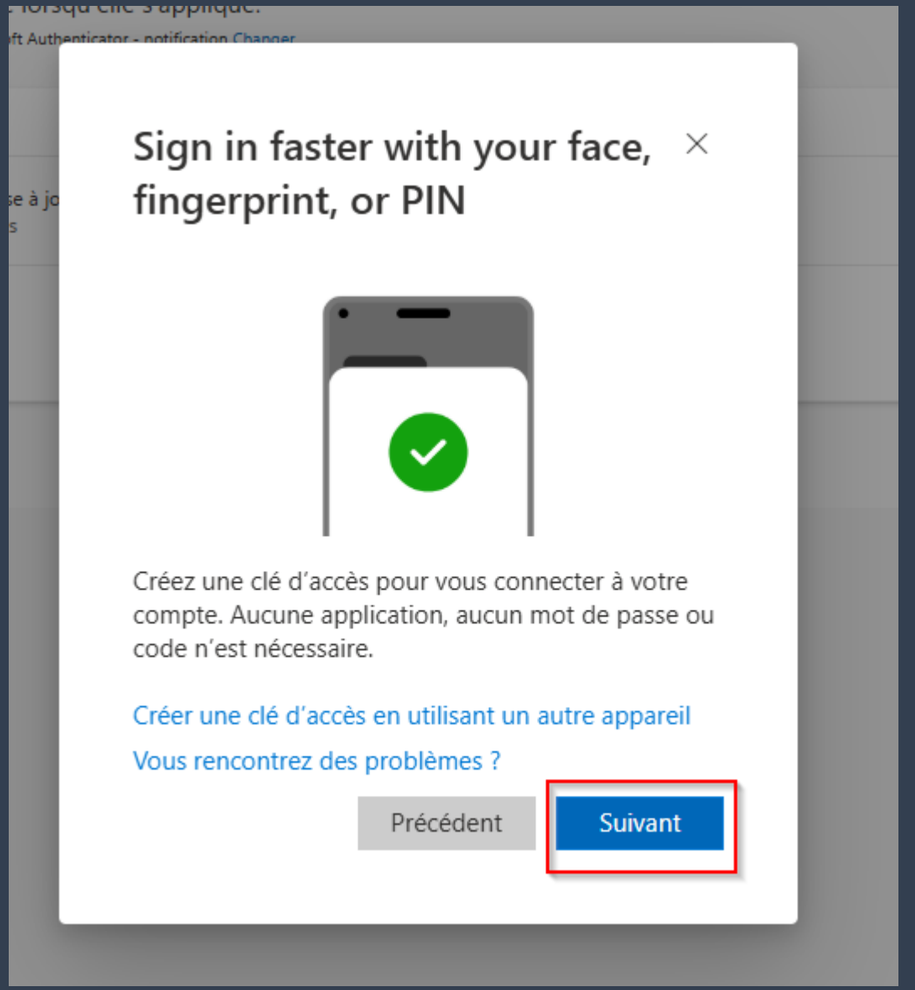
Clé d'accès
Connectez-vous à l'aide de votre visage, d'une empreinte digitale, d'un code PIN ou d'une clé de sécurité

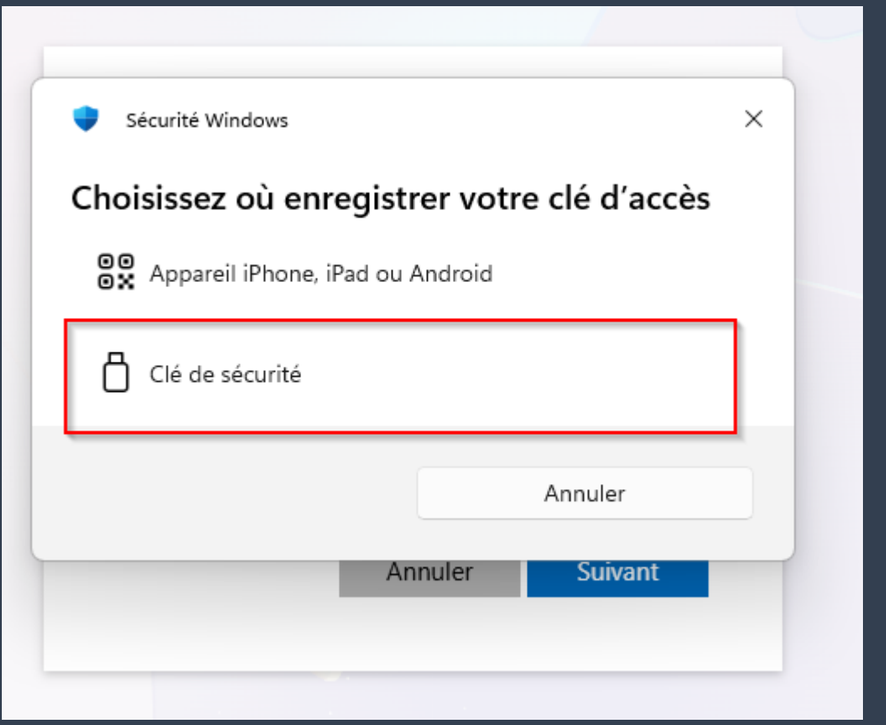
Microsoft Authenticator
Approuver les demandes de connexion ou utiliser des codes à usage unique

Jeton matériel
Se connecter avec un code provenant d'un jeton matériel

Téléphone
Recevoir un appel ou un SMS pour vous connecter avec un code

En savoir plus sur chaque méthode pour vous aider à choisir.


Sign in faster with your face, fingerprint, or PIN
Créez une clé d'accès pour vous connecter à votre compte. Aucune application, aucun mot de passe ou code n'est nécessaire.
Créer une clé d'accès en utilisant un autre appareil
Vous rencontrez des problèmes ?
Précédent
Suivant


Sécurité Windows
Choisissez où enregistrer votre clé d'accès
Appareil iPhone, iPad ou Android
Clé de sécurité
Annuler
Annuler
Suivant

Sécurité Windows

Utiliser votre clé d'accès

[redacted]
Clé d'accès pour login.microsoft.com

Vous devez créer un code PIN pour cette clé de sécurité.

Nouveau code PIN de la clé de sécurité

••••

Confirmer le code PIN de la clé de sécurité

••••

Ceci sera enregistré dans votre clé de sécurité. Modifier

OK Annuler

Sécurité Windows

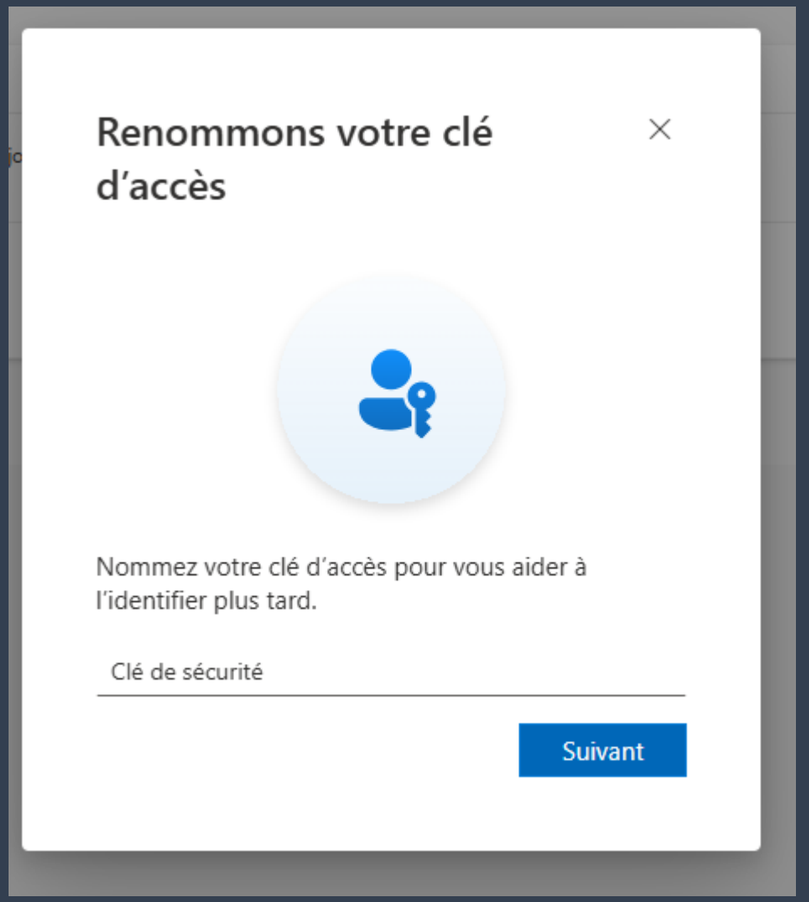
Utiliser votre clé d'accès

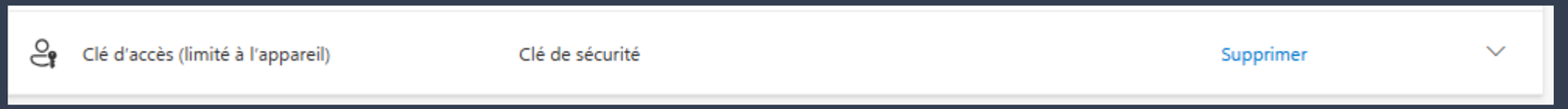
[redacted]
Clé d'accès pour login.microsoft.com

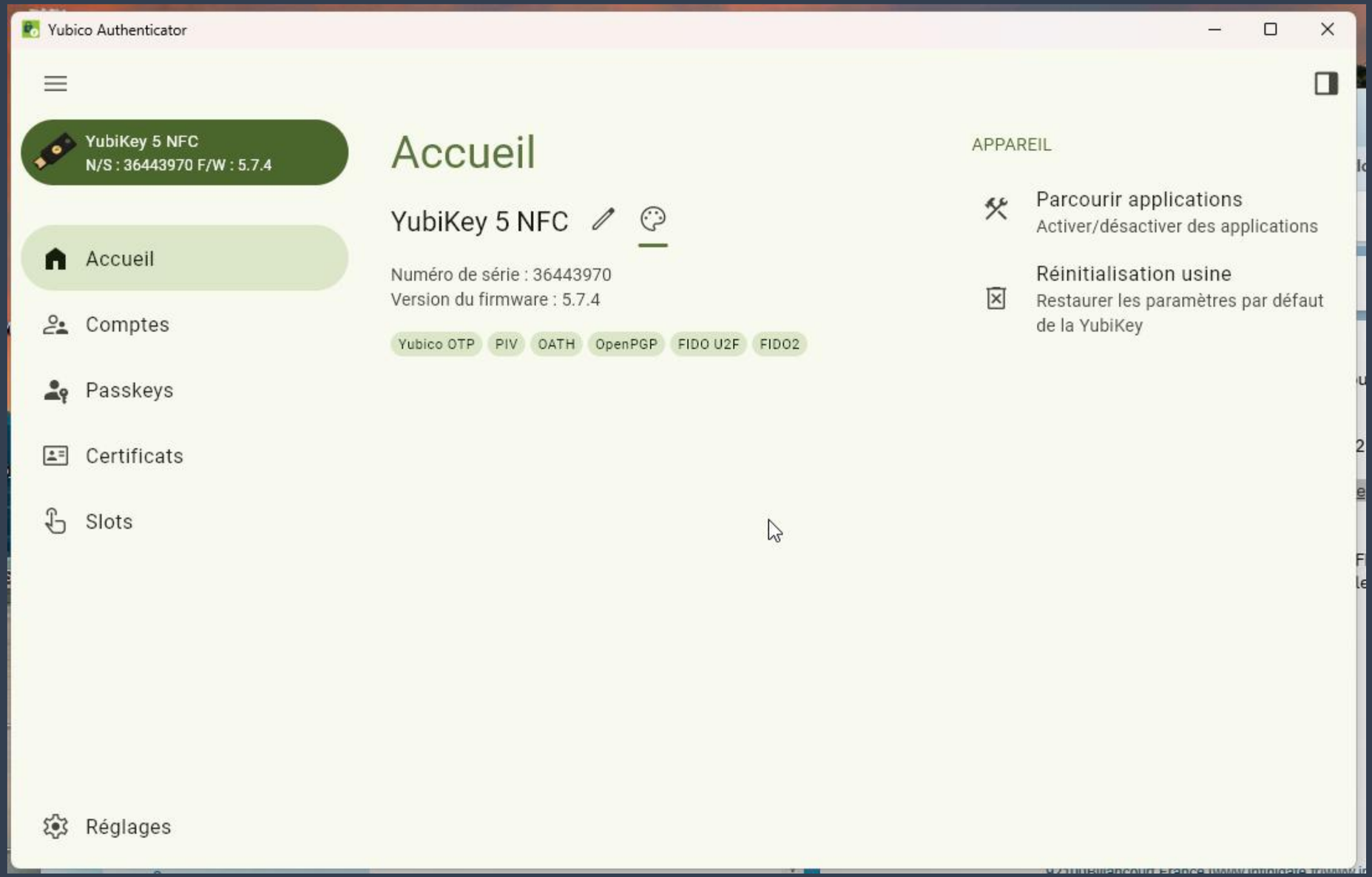
Touchez votre clé de sécurité.

Ceci sera enregistré dans votre clé de sécurité. Modifier

Annuler


Renommons votre clé d'accès
Nommez votre clé d'accès pour vous aider à l'identifier plus tard.
Clé de sécurité
Suivant


Clé d'accès (limité à l'appareil)
Clé de sécurité
Supprimer


Yubico Authenticator
YubiKey 5 NFC
N/S : 36443970 F/W : 5.7.4
Accueil
Comptes
Passkeys
Certificats
Slots
Réglages
Accueil
YubiKey 5 NFC
Numéro de série : 36443970
Version du firmware : 5.7.4
Yubico OTP
PIV
OATH
OpenPGP
FIDO U2F
FIDO2
APPAREIL
Parcourir applications
Activer/désactiver des applications
Réinitialisation usine
Restaurer les paramètres par défaut de la YubiKey

Gestion du PIN FIDO2

Un PIN unique

La YubiKey possède un seul PIN FIDO2 qui protège physiquement la clé, quel que soit le nombre de comptes enregistrés.

Plusieurs comptes possibles

Une même clé peut stocker les informations d'authentification pour des dizaines de services différents simultanément.

Sécurité par conception

Le PIN empêche l'utilisation non autorisée de la clé en cas de perte ou de vol, ajoutant une couche de protection essentielle.

Le PIN FIDO2 est distinct des mots de passe des comptes en ligne. Il sécurise uniquement l'accès à la clé physique elle-même.

Configuration recommandée

Choisir un PINde 6 à 8 chiffres, facile à mémoriser mais difficile à deviner. Après plusieurs tentatives erronées (8 par défaut) , la clé se verrouille automatiquement.

Exemple d'utilisation multi-comptes

01

Une YubiKey physique

Un seul dispositif matériel à transporter

02

Deux comptes Microsoft distincts

Par exemple : compte professionnel 1 et compte professionnel 2

03

Deux mots de passe différents

Chaque compte conserve ses propres identifiants*

04

Un seul PIN pour la clé

Protection commune de l'accès à la YubiKey

*Résultat : Séparation logique complète des identités tout en conservant la simplicité d'usage d'un seul dispositif de sécurité.

Watchguard…

Phase de test/bêta en cours pour les clés FIDO

https://www.watchguard.com/wgrd-blog/authpoint-passkeys

Forti

Avantages et limites de la solution

Avantages majeurs

- Très haut niveau de sécurité certifié
- Protection totale contre le phishing
- Interface d'utilisation intuitive (USB/NFC)
- Indépendance vis-à-vis du réseau
- Pas de batterie à recharger
- Support multi-plateforme et multi-services

Limites à considérer

- Un seul PIN FIDO2 par clé physique
- FIDO2 non utilisable pour connexion locale sur Active Directory pur
- Coût d'acquisition supérieur aux solutions logicielles
- Nécessité de posséder physiquement la clé
- Très facile à perdre

50€

Prix moyen

Investissement pour une YubiKey 5 NFC professionnelle

250+

Services compatibles

Nombre de plateformes supportant l'authentification FIDO2