NEOWAVE

Winkeo-A/C FIDO2

Guide d’utilisation

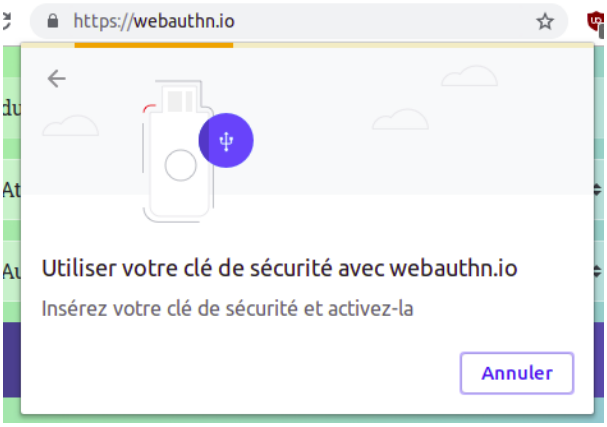
PRESENTATION / GUIDE RAPIDE

Winkeo FIDO2 est une clé USB de sécurité pour une authentification forte en ligne. Elle protège l'accès à vos comptes de manière plus efficace qu'un simple mot de passe.

L'utilisation standard se fait via un navigateur web sur un service en ligne permettant d'associer une clé à votre compte utilisateur pour vous authentifier de manière sécurisée et vous protéger des attaques dites de «phishing» (hameçonnage) ou vol de mot de passe.

Ce dispositif d'authentification forte est de plus très simple à utiliser. L'authentification se fait par le biais de la clé que l'on insère dans un port USB sur laquelle il suffit de poser son doigt (sur la surface ronde dorée au centre qui sert de « bouton ») pendant qu'elle clignote.

Dans certains cas, une fenêtre vous demandera de confirmer que vous autorisez le service en ligne à utiliser la clé (parfois appelée « clé de sécurité ») ou à accéder aux informations liées au fabricant.



Exemple de fenêtre de demande

Ce support d'authentification forte « sans mot de passe » ou « second facteur » permet de protéger vos comptes en ligne sur les services supportant les protocoles dénommés « FIDO[1] U2F » et « FIDO2 ». Un service peut aussi utiliser des termes différents comme « Security Key » ou encore « périphérique compatible WebAuthn ».

COMPATIBILITE / DETAILS

Les produits Winkeo-A/C FIDO2 est compatible avec les ports USB 2. et 3.X de type A/C, en direct ou via un Hub USB. Une utilisation d'un Winkeo-A sur un port USB de type C ou un Winkeo-C sur un port USB de type A est possible via un simple adaptateur (non fourni par défaut avec le produit).

1) **Compatibilité :**
- FIDO2 compatible Microsoft Entra ID[2]…
- FIDO U2F compatible avec Gmail, Facebook, Dropbox… (voir liste en annexe)
- Compatibilité étendue à travers des services de fédération d'identité (WebSSO)

2) **Systèmes d'exploitation et navigateurs supportés :**
- Systèmes d'exploitation : Windows 10 build 1903 ou ultérieure, (Mac) OS X 13.51+, Linux
- Navigateurs : Chrome, Chromium, Vivaldi, Opera, Mozilla Firefox, Microsoft, Safari[3]

3) **Détails :**
- Dans la majorité des cas d'utilisation, il vous sera demandé d'utiliser cette clé en plus de votre mot de passe.
- Sur certains services, vous pourrez vous dispenser du mot de passe.
- La longueur du code PIN peut varier de 4 et 63 caractères (la limite dépend de l'encodage) et le nombre d'essais du code PIN est limité à 8 (ensuite la carte doit être réinitialisée).
- Winkeo peut stocker jusqu'à 1024 clés FIDO U2F et 1024 clés FIDO2 (aucun « wrapping », toutes les clés privées sont stockées dans le Winkeo). Parmi ces clés FIDO2, 256 peuvent être des clés « résidentes » (resident keys) : des informations supplémentaires (nom, icone…) nécessaires à certains services (ex : Microsoft AzureAD) sont alors stockées dans le WInkeo et associées à une clé FIDO2. Ces informations publiques peuvent être présentées localement à l'utilisateur pour l'informer sur l'utilisation d'une paire de clé précise.

Pour chaque service en ligne, il y a deux phases d'utilisation :

- La phase initiale d'enrôlement qui consiste à associer la clé à votre compte d'utilisateur.

Cette étape n'est à effectuer qu'une seule fois par compte utilisateur. Chaque « Passkey » créée est propre à un compte sur un service en particulier. Si vous utilisez un autre compte sur ce même service en ligne ou sur un autre, vous devrez refaire cette phase

[1] Les standards FIDO/WebAuthn sont développés par la Fido Alliance (fidolalliance.org) et le W3C (w3.org/TR/webauthn-2)
[2] L'ouverture de session Windows nécessite le paramétrage d'un annuaire Entra ID par votre entreprise (voir Annexe 2)
[3] Pour Safari sur OSX, si un code PIN est demandé/utilisé il faut Safari 14 Beta, sinon Safari 13 suffit

d'enregistrement. Une nouvelle « Passkey » sera créée, différente de la précédente, sans l'écraser.

Il est ainsi possible d'utiliser une même clé Winkeo sur des centaines de comptes et services différents. (Note : il est aussi souvent possible d'utiliser plusieurs clés Winkeo pour protéger un même compte, ce qui peut vous permettre d'avoir une clé de backup).

- La phase d'authentification en elle-même une fois que l'association a été faite.

Certains services vous demanderont d'utiliser la clé à chaque authentification, d'autres servent d'autres mécanismes de sécurité pour ne vous la demander que de temps en temps (c'est parfois paramétrable sur le service en ligne concerné).

Il suffit de poser n'importe quel doigt sur le bouton doré de la clé. Il n'est pas nécessaire d'appuyer fortement. Il ne s'agit pas d'un capteur biométrique d'empreintes digitales.

Message d'information intermédiaire sur Windows 10 build 1903 ou ultérieure**:**

Les messages incitant l'utilisateur à utiliser la clé peuvent être gérés et affichés directement par les applications. Ainsi, sur certaines anciennes versions de Windows 10 build 1903 ou ultérieure , sur OSX ou Linux, ces messages apparaissent généralement dans l'interface des navigateurs web.

Sur les versions récentes de Windows 10, les messages sont gérés directement par le système d'exploitation et vous informent sur le cadre d'utilisation de la clé en vous indiquant le nom de domaine du service en ligne, le login de l'utilisateur, le nom de l'application et le nom de l'entreprise qui a développé cette application.

Code PIN :

Certains services peuvent vous demander d'augmenter la protection en associant un code PIN à votre clé. Ce code PIN sera ensuite demandé pour toute utilisation de votre clé.

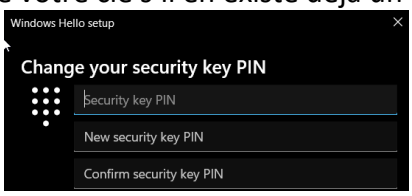
Ce code n'est pas envoyé aux services en ligne, il n'est utilisé que localement pour débloquer l'usage de votre clé.

Changement de code PIN et réinitialisation de la clé :

Si vous êtes dans un environnement d'entreprise, il est important de suivre les recommandations locales de votre officier de sécurité ou de votre administrateur système/réseaux qui peut avoir une procédure particulière, proposer des outils de remise à zéro spécifiques pour votre système d'exploitation (mais qui dans tous les cas supprimeront toutes les informations du produit en dehors du firmware).

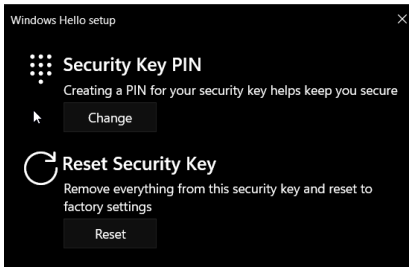
Windows 10 build 1903 ou ultérieure intègre par défaut un outil de configuration qui permet de :

- changer le code PIN de votre clé s'il en existe déjà un

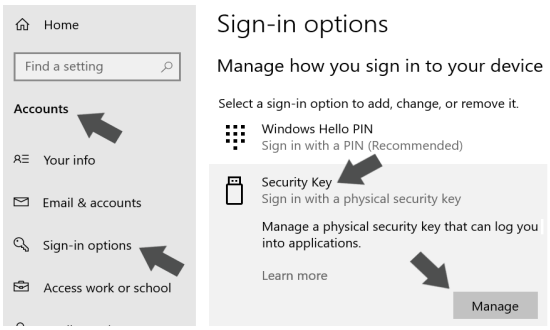


- créer un code PIN pour votre clé s'il n'en existe pas

- réinitialiser la clé Winkeo



Attention, réinitialiser la clé Winkeo supprimera le code PIN s'il en existe un (vous pourrez en choisir un autre) mais supprimera aussi TOUTES les identités contenues dans la clé (et donc toutes les clés (clés FIDOU2F, clés FIDO2, résidentes ou pas).
Si vous vous serviez de cette clé pour différents comptes, vous ne pourriez plus utiliser cette clé pour vous authentifier.



Si vous perdez la clé ou si elle ne fonctionne plus ou si vous l'avez réinitialisée par erreur :

Les services en ligne ont, dans la quasi-totalité des cas, un service de support qui vous permettra de récupérer l'accès à votre compte à travers une procédure de vérification d'identité. Souvent un autre second facteur d'authentification est prévu à cet effet. Puisque que généralement, vous pouvez associer plusieurs clés Winkeo à un même compte, vous pouvez aussi en acquérir une seconde en guise de backup par précaution ou pour en conserver une sur votre lieu de travail et une autre à votre domicile. Si vous avez perdu la clé et que vous avez fini par récupérer l'accès à votre compte, vous devriez pouvoir désactiver l'association de la clé perdue avec votre compte sur l'interface d'administration de ce service.

ANNEXE 1 : Liste non-exhaustive (sans engagement) de services et d'applications compatibles avec le standard « FIDO »

BACKUP
Boxcryptor
Dropbox
Files.com
Google Drive
OneDrive

CLOUD
Amazon Web Services
Google Cloud Platform
Microsoft Azure

COLLABORATION/OFFICE
Basecamp
Campfire
Google docs
Hangouts
Nulab
Office 365
RelateIt
Salesforce
SeguLink
Skype (MS Account)

CREATION DE CONTENU
Blogger
Shopify
Silverstripe
Wordpress (2FA plugin)
Youtube

CRYPTO ACTIFS
Bitfinex
BitGo
Coinbase
CoinFloor
DSX
Gemini
Stex

DEVELOPPEMENT
Bitbucket
Github
GitLab
JetBrains
Jira (2FA for JIRA)
Pypi
Sentry
Visual Studio Codespaces

GESTIONNAIRE DE MOT DE PASSE
1Password
Bitwarden
Dashlane

GESTION DES IDENTITES (SSO / IAM)
AuthStack
Axiad
Centrify
Code Enigma
Daon
Data Guard
DUO
Egnyte Protect
ForgeRock
Gluu
Green Rocket
HelloID
IBM Security Access Manager
ID.me
Idaptive
InfoAnywhere
Keeper
Keycloak
MicroFocus
Modis
Okta
OneLock
OneLogin
PingIdentity
PrivacyIDEA
PushCoin
Rohos
RSA SecurID Access
Sign&Go SSO (Ilex)
Thycotic
Trustelem (WALLIX)
TRUU
WSO2
XTN Cognitive Security

HEBERGEMENT
Gandi
GoDaddy
Google Domains
IPS Hosting
Namecheap
Opalstack
OVH
Registro.fr

SECURITE INFORMATIQUE
AppGate
Cloudflare
ISL Online
Kaseya
Norton
SAASPASS
StrongKey
XONA

RESEAUX SOCIAUX
Facebook
Twitter

SANTE
Google Fit
Isosec

SYSTEME D'EXPLOITATION
Windows (Login via Azure AD)
Linux (Debian, Ubuntu, Fedora)

WEBMAIL
FastMail
Gmail
Hey
Outlook
Tutanota
Zoho Mail

ANNEXE 2 : Entra ID et FIDO2

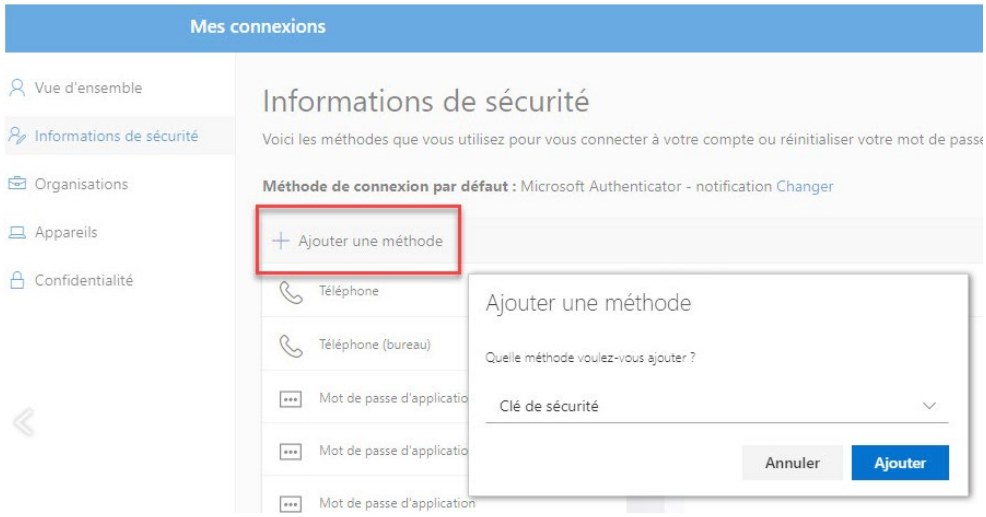
FIDO2 est intégré dans l'architecture Entra ID (auparavant Azure Active Directory).

La documentation officielle sur cette intégration est disponible ici :
https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2

https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-enable-passkey-fido2

L'utilisateur pourra ensuite activer la clé de sécurité Winkeo dans son propre portail.

https://mysignins.microsoft.com/



Après ces paramétrages, une nouvelle option d'authentification par clé FIDO2 pour l'ouverture de session apparaîtra.

ANNEXE 3 : Utilisation sous Linux

Il faut ajouter une règle pour udev. Créez le fichier suivant avec votre éditeur préféré :

```
/etc/udev/rules.d/70-neowave.rules
```

Avec le contenu suivant :

```
ACTION!="add|change", GOTO="neowave_end"
# Neowave rule
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", ATTRS{idVendor}=="1E0D",
ATTRS{idProduct}=="F1D0", TAG+="uaccess"
LABEL="neowave_end"
```

Puis rechargez ces règles avec la commande suivante :

```
sudo udevadm control --reload-rules
```

Winkeo devrait maintenant être utilisable par les navigateurs web de votre distribution Linux.

ANNEXE 4 : Test via le site Webauthn.io

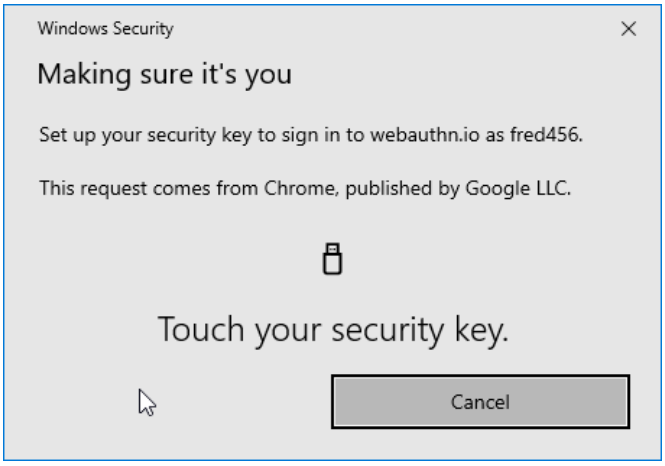
C'est un simple site de test pour vérifier que votre clé est visible par votre système d'exploitation et votre navigateur web.

Cette page permet de tester un enregistrement de la clé puis de tester l'authentification.

Allez sur le site web webautn.io

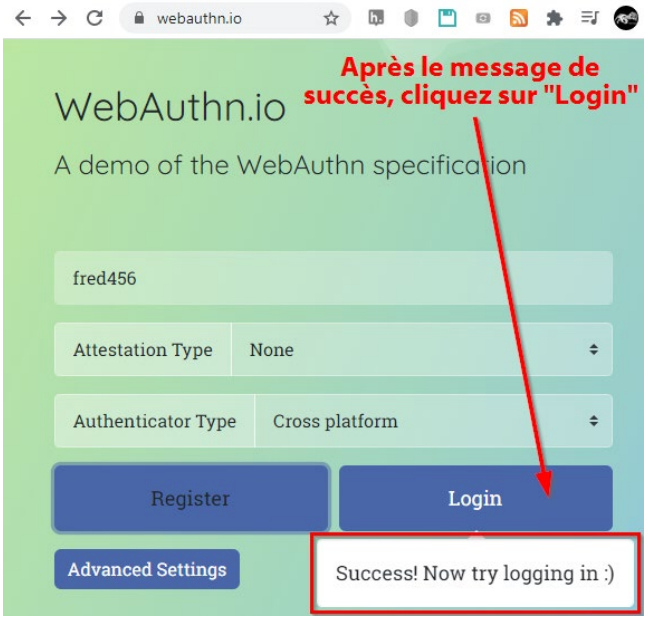
0 – Branchez votre clé Winkeo
1 - Choisissez un login
2 - Sélectionnez « Cross platform » comme « Authenticator Type ».

3 - Cliquez sur « Register ».



Sous Windows 10, la fenêtre d'information suivante doit apparaître. Sur d'autres systèmes d'exploitation, une fenêtre du même type doit vous inviter à toucher votre clé Winkeo.

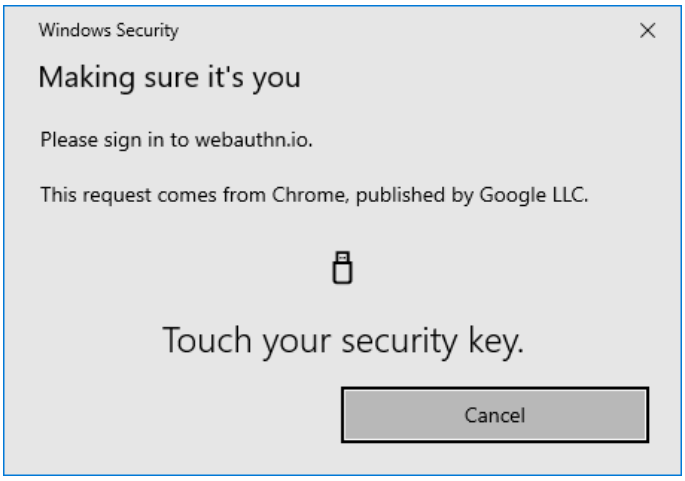
4 – Touchez votre clé Winkeo (appuyez légèrement sur son cercle doré).



Un message de succès doit s'afficher vous invitant à tester la partie « login » maintenant que l'enregistrement est effectué.

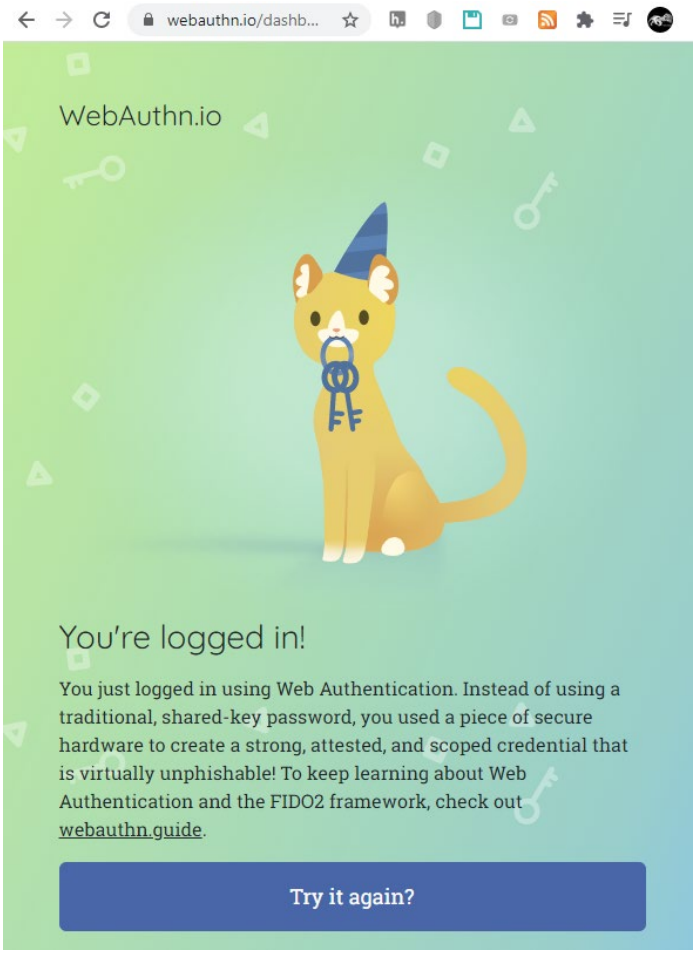
(vous pouvez vérifier que votre login et le choix d'authenticator n'ont pas changé).

5 - Cliquez sur le bouton « Login ».



La fenêtre d'information doit de nouveau apparaître pour vous inviter à toucher votre clé Winkeo.

6 – Touchez votre clé Winkeo (appuyez légèrement sur son cercle doré).



7 – Un message de succès doit apparaître.

Rappel : ce n'est qu'un site de test sans réelle fonctionnalité, uniquement pour tester le bon fonctionnement de la clé sur votre navigateur.