

# UTILISATION

## Comment installer ma clé Winkeo ou ma carte Badgeo

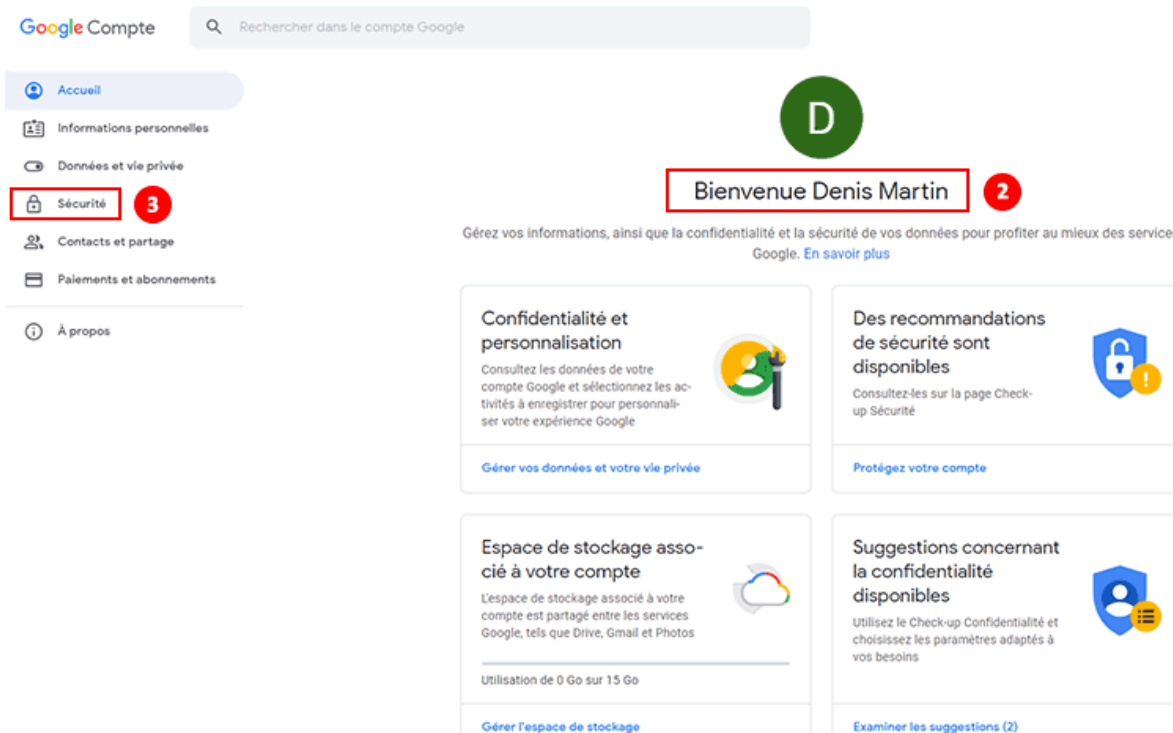
### Comment utiliser ma clé Winkeo FIDO U2F

Avant d'utiliser votre clé Winkeo FIDO U2F, activez la double authentification sur votre compte Web si vous ne l'avez pas encore fait. Une fois activée, associez votre clé Winkeo FIDO U2F à votre compte utilisateur. Nous allons ici montrer la marche à suivre sur Google. La plupart des services Web suivent un processus similaire consistant à sélectionner dans les « Paramètres » l'onglet « Sécurité » afin d'accéder à la section « Validation en deux étapes » pour l'activer et ensuite d'«Ajouter une Clé de sécurité ».

### Tutoriel FIDO U2F sur Google

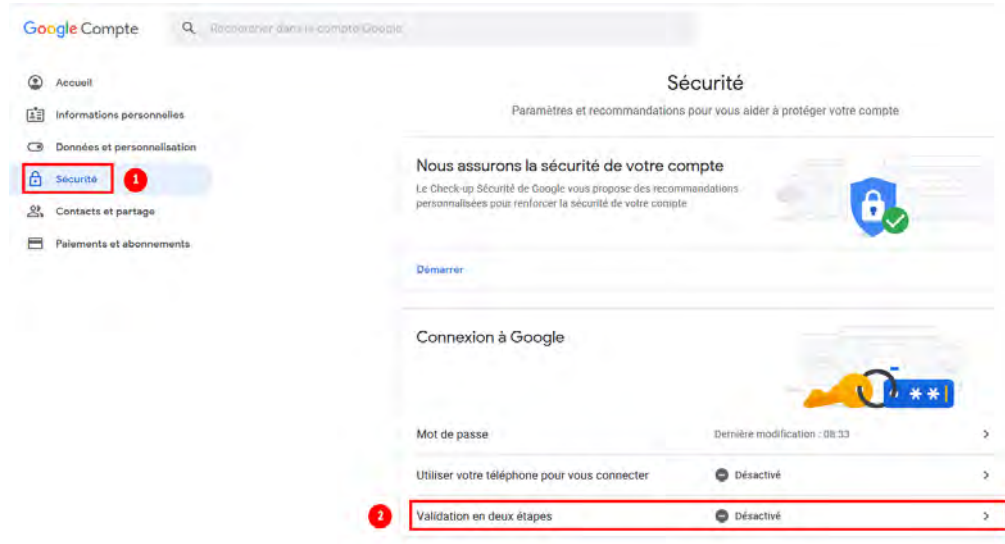
#### Étape 1

Connectez-vous à votre compte Gmail, puis cliquez sur « Gérez votre compte Google » en haut à droite de votre écran.



## Étape 2

Sur la page de « Bienvenue », cliquez sur l'onglet « Sécurité ». Puis sous « Connexion à Google », sélectionnez « Validation en deux étapes ».



## Étape 3

Poursuivez en cliquant sur « Commencer ». Ensuite, il vous sera nécessaire de vous authentifier avec le mot de passe de votre compte Google. Puis cliquez sur « Suivant ».

← Validation en deux étapes



### Protéger votre compte avec la validation en deux étapes

Chaque fois que vous vous connecterez à votre compte Google, vous aurez besoin de votre mot de passe et d'un code de validation. [En savoir plus](#)



#### Ajouter un niveau de sécurité supplémentaire

Saisissez votre mot de passe et le code de validation unique qui vous a été envoyé sur votre téléphone.



#### Protéger votre compte des intrus

Même si un tiers obtient votre mot de passe, ce n'est pas suffisant pour se connecter à votre compte.

COMMENCER

Google

Denis Martin

D

Pour continuer, veuillez confirmer votre identité

Saisissez votre mot de passe

.....|


[Mot de passe oublié ?](#)

Suivant

## Étape 4

Puis, il vous sera demandé une option de secours avec comme choix le SMS ou l'appel téléphonique. Dans le cas de notre tuto, nous choisirons la méthode par SMS. Une fois votre numéro de téléphone renseigné, l'option « SMS » cochée, cliquez sur « Suivant ». Saisissez le code reçu par SMS puis cliquez sur « Suivant ». La configuration de la double authentification pour votre compte Google est terminée. Cliquez sur « Activer » pour lancer l'activation de la double authentification ».

← Validation en deux étapes



Configurer votre téléphone

Quel numéro de téléphone souhaitez-vous utiliser ?

FR - [REDACTED]

Nous utiliserons ce numéro que pour assurer la sécurité de votre compte.  
N'utilisez pas de numéro Google Voice.  
Votre opérateur peut appliquer des frais pour l'envoi de SMS ou la connexion à Internet.

Comment souhaitez-vous obtenir des codes ?

SMS  Appel téléphonique

[Afficher plus d'options](#)

Étape 1 sur 3

**SUIVANT**

← Validation en deux étapes



Confirmer le bon fonctionnement

Nous venons d'envoyer un code de validation par SMS au [REDACTED]

Saisissez le code

\_\_\_\_\_


Vous ne l'avez pas reçu ? [Réenvoyer](#)

RETOUR

Étape 2 sur 3

**SUIVANT**

← Validation en deux étapes



Cela fonctionne ! Activer la validation en deux étapes ?

Maintenant que vous savez comment elle fonctionne, souhaitez-vous activer la validation en deux étapes pour votre compte Google [REDACTED]@gmail.com ?

Étape 3 sur 3

**ACTIVER**

## Étape 5

La validation en deux étapes étant activée, il vous faut ajouter la clé de sécurité Winkeo FIDO U2F comme deuxième étape d'authentification. Défilez vers le bas jusqu'à la section « Clé de sécurité » et cliquez sur « Ajouter une clé de sécurité ».


← Validation en deux étapes

La validation en deux étapes est **ACTIVEE** [DÉSACTIVER](#)


**Deuxièmes étapes possibles**

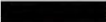
Une deuxième étape de validation après la saisie de votre mot de passe permet de confirmer que c'est bien vous qui essayez de vous connecter. [En savoir plus](#)

**Remarque :** Si vous vous connectez à votre compte Google sur n'importe quel téléphone compatible, des invites Google seront ajoutées comme autre méthode de validation en deux étapes.

 **Vous en avez assez de saisir des codes de validation ?** [AJOUTER UNE INVITE GOOGLE](#)

Recevez une invite Google sur votre téléphone et appuyez sur **Oui** pour vous connecter à votre compte.


 **Message vocal ou SMS (Par défaut)** [?](#)

 Validé

Les codes de validation sont envoyés par SMS.

**Ajouter d'autres deuxièmes étapes pour confirmer votre identité**


Configurez des étapes de secours supplémentaires pour pouvoir vous connecter même si les autres options que vous avez définies ne sont pas disponibles.

 **Codes de secours**

Ces codes imprimables à usage unique vous permettent de vous connecter lorsque vous n'avez pas votre téléphone sur vous, notamment lors de vos déplacements.


[CONFIGURER](#)

← Validation en deux étapes

 **Application Google Authenticator**


Utilisez l'application Google Authenticator pour obtenir des codes de validation gratuits, et ce même lorsque votre téléphone est hors connexion. Disponible sur Android et iPhone.

[CONFIGURER](#)

 **Numéro de téléphone secondaire**

Ajoutez un téléphone secondaire afin de pouvoir vous connecter même si vous perdez votre téléphone.

[AJOUTER UN NUMÉRO DE TÉLÉPHONE](#)

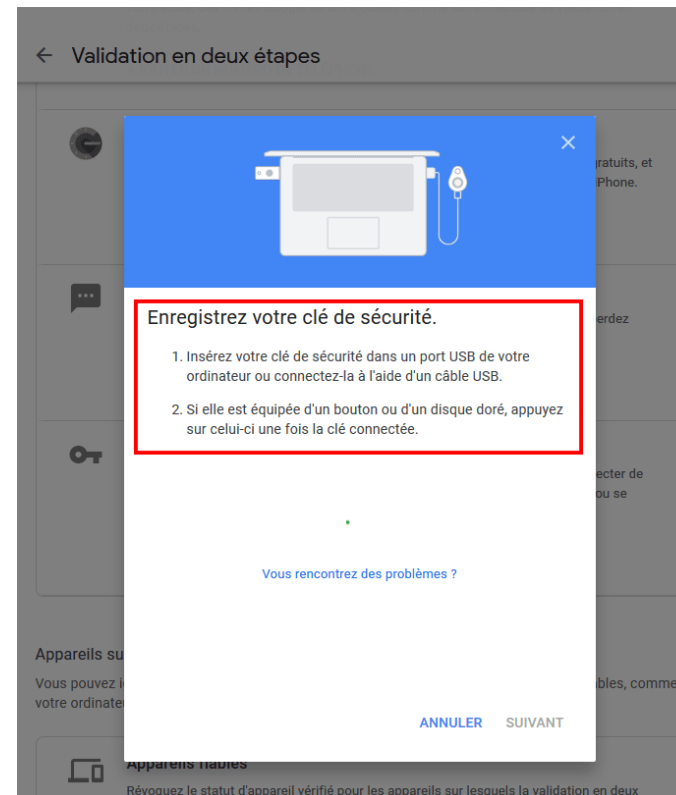
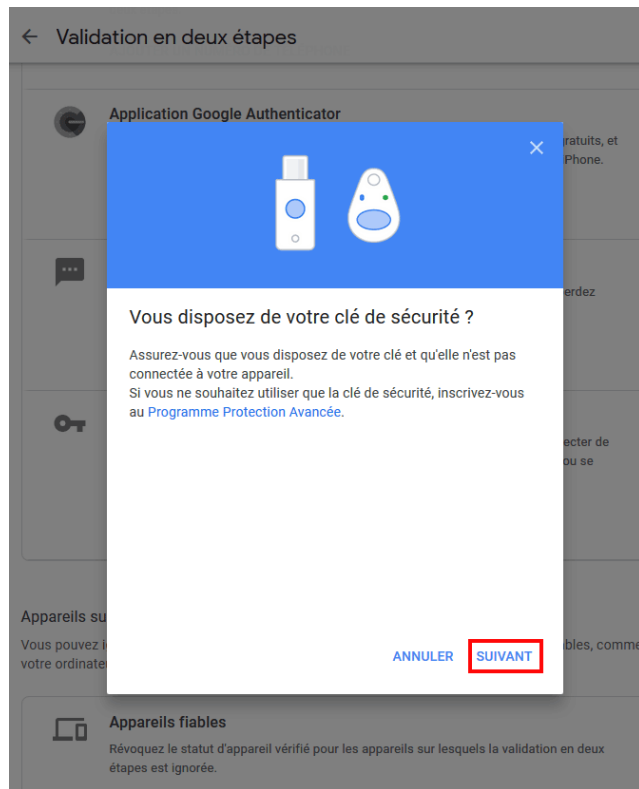
 **Clé de sécurité**

Une clé de sécurité est une méthode de validation qui vous permet de vous connecter de manière sécurisée. Elle peut être intégrée à votre téléphone, utiliser le Bluetooth ou se brancher directement sur le port USB de votre ordinateur.

[AJOUTER UNE CLÉ DE SÉCURITÉ](#)

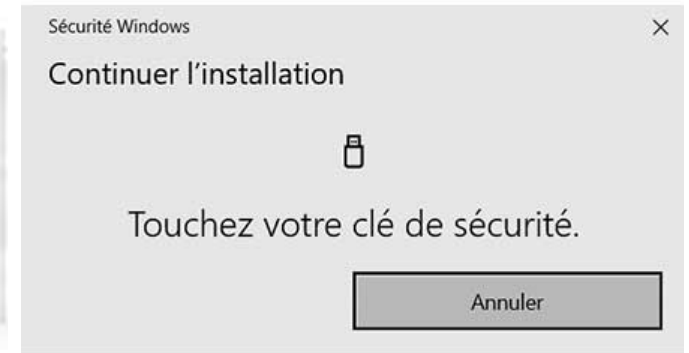
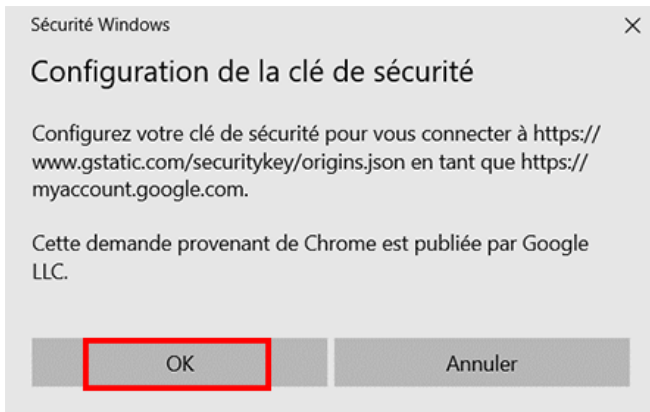
## Étape 6

Il vous sera proposé de choisir votre clé de sécurité, auquel cas cliquez sur « USB ou Bluetooth » ou bien il vous sera demandé directement « Vous disposez de votre clé de sécurité ? » sans passer par l'étape précédente. Puis appuyez sur « Suivant ». Une fenêtre « Enregistrez votre clé de sécurité » s'ouvrira.



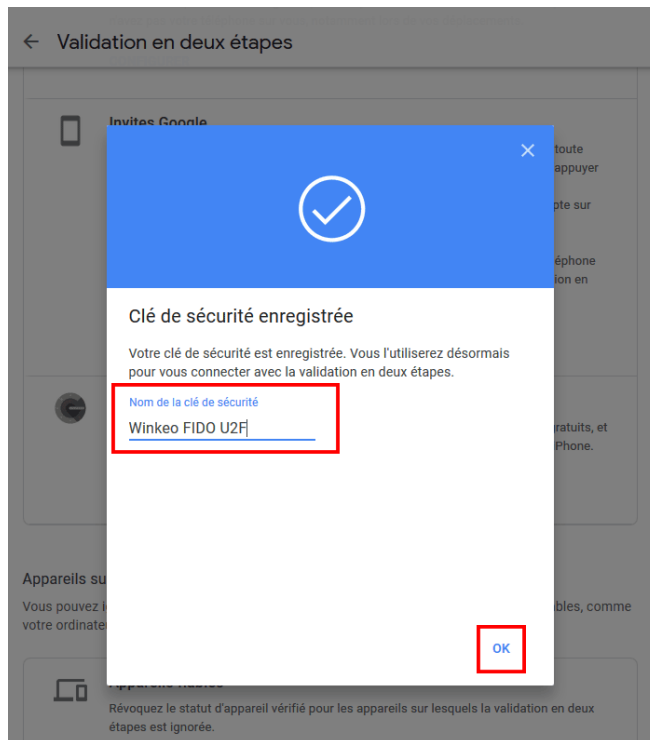
## Étape 7

Insérez votre clé de sécurité dans un port USB de votre ordinateur (la LED clignote). Cliquez « OK » sur les fenêtres qui s'ouvriront puis touchez votre clé de sécurité quand il vous le sera demandé. Pour la clé Winkeo FIDO U2F, appuyez sur le disque doré dont elle est équipée.



## Étape 8

Votre clé de sécurité est désormais enregistrée et sera utilisée pour vous connecter avec la validation en deux étapes. Nommez votre clé de sécurité, « Winkeo FIDO U2F » pour l'exemple, et appuyez sur « OK ». La validation en deux étapes est activée et votre clé de sécurité est enregistrée.



## ← Validation en deux étapes

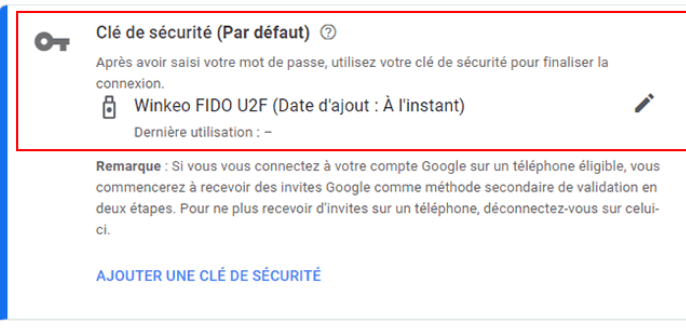
La validation en deux étapes est ACTIVÉE

DÉSACTIVER

### Deuxièmes étapes possibles

Une deuxième étape de validation après la saisie de votre mot de passe permet de confirmer que c'est bien vous qui essayez de vous connecter. [En savoir plus](#)

**Remarque :** Si vous vous connectez à votre compte Google sur n'importe quel téléphone compatible, des invites Google seront ajoutées comme autre méthode de validation en deux étapes.



## Futures Connexions

Pour toute future connexion à votre compte Gmail, vous devrez désormais rentrer votre mot de passe puis insérer la clé de sécurité Winkeo FIDO U2F et appuyer sur le bouton pour vous authentifier.



Google

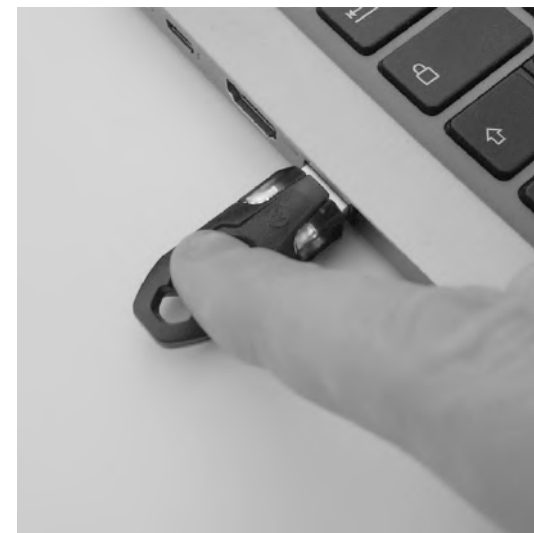
Denis Martin

Pour continuer, veuillez confirmer votre identité

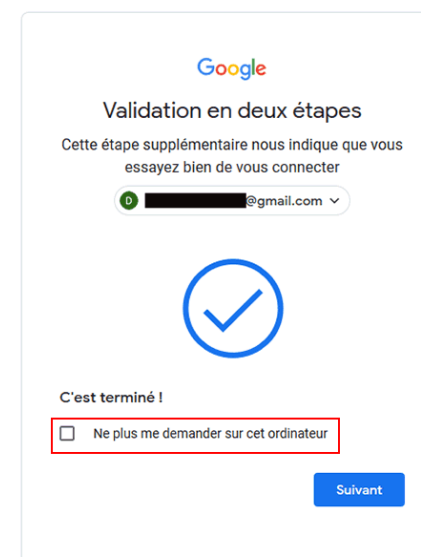
Saisissez votre mot de passe

Mot de passe oublié ?

Suivant



Si vous ne voulez pas utiliser votre clé de sécurité chaque fois que vous vous connectez à votre compte Google, cochez la case « Ne plus me demander sur cet ordinateur ». Vous indiquez ainsi que votre ordinateur est fiable. Toutefois, cette possibilité est à opter uniquement sur les appareils que vous utilisez régulièrement et que vous ne partagez avec personne d'autre. Sinon, décochez la case.



Google

Validation en deux étapes

Cette étape supplémentaire nous indique que vous essayez bien de vous connecter

@gmail.com

C'est terminé !

Ne plus me demander sur cet ordinateur

Suivant

## Comment utiliser la clé Winkeo FIDO2 ou la carte Badgeo FIDO2

Pour associer la clé Winkeo FIDO2 ou la carte FIDO2 aux services et applications web, nous vous invitons à contacter notre équipe ou votre administrateur système/réseaux afin de suivre les recommandations et la procédure adéquates.

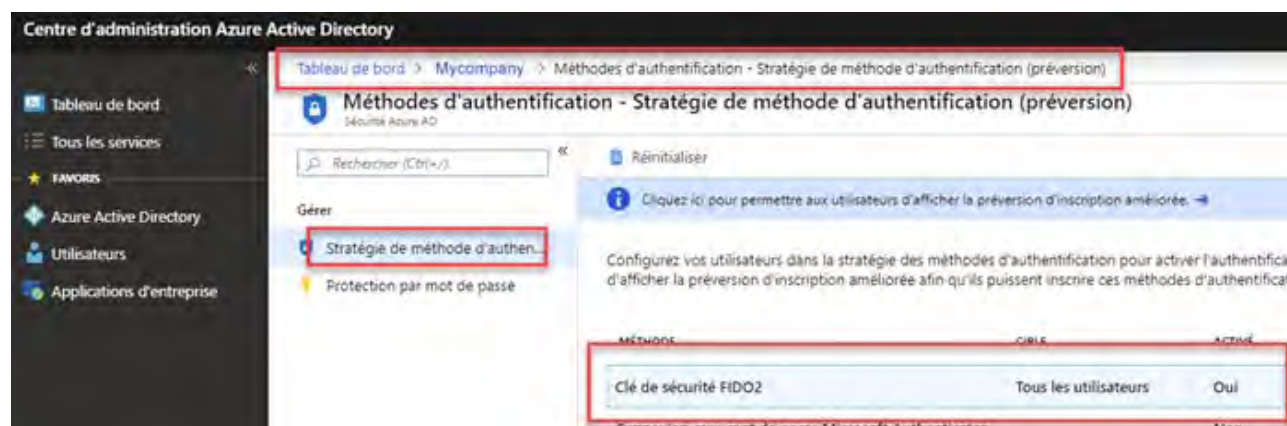
Des guides pratiques proposés par Microsoft vous proposent également les étapes clés pour [activer la connexion par clé de sécurité sans mot de passe](#), notamment à des appareils [Windows 10 à l'aide d'Azure Active Directory](#).

Nous vous proposons également un guide résumé sur l'activation d'une clé Winkeo FIDO2 comme moyen d'authentification sur votre annuaire d'entreprise Azure Active Directory.

## Tutoriel FIDO2 avec Microsoft

### Étape 1

Votre administrateur réseau devra activer la clé Winkeo FIDO2 et / ou la carte Badgeo FIDO2 dans la « Stratégie de méthode d'authentification » le centre d'administration de votre Azure Active Directory <https://aad.portal.azure.com/>





## Étape 2

L'administrateur devra ensuite choisir les utilisateurs qui pourront utiliser cette méthode. Il devra aussi désactiver la « restriction de clé » qui bloque certains fabricants de matériel.

The screenshot shows two panels from an administrative interface. The left panel, titled 'CIBLE', contains a dropdown menu with 'Tous les utilisateurs' selected and a 'Sélectionner les utilisateurs' button. Below this is a table with columns 'NOM', 'TYPE', and 'INSCRIPTION'. The first row shows 'Tous les utilisateurs', 'Groupe', and a dropdown menu with 'Facilité' and a plus icon. The right panel, titled 'GÉNÉRAL', has two toggle switches: 'Autoriser la configuration libre-service' (set to 'Oui') and 'Appliquer l'attestation' (set to 'Oui'). Below this is a section titled 'STRATÉGIE DE RESTRICTION DE CLÉ' with a toggle switch for 'Appliquer les restrictions de clé' set to 'Non'.

## Étape 3

L'utilisateur pourra ensuite activer la clé de sécurité Winkeo FIDO2 et/ou la carte Badgeo FIDO2 dans son propre portail.

Il devra se rendre sur <https://mysignins.microsoft.com/> dans l'onglet « Informations de sécurité », cliquer sur « Ajouter une méthode » puis sur « Clé de sécurité » dans le menu déroulant.

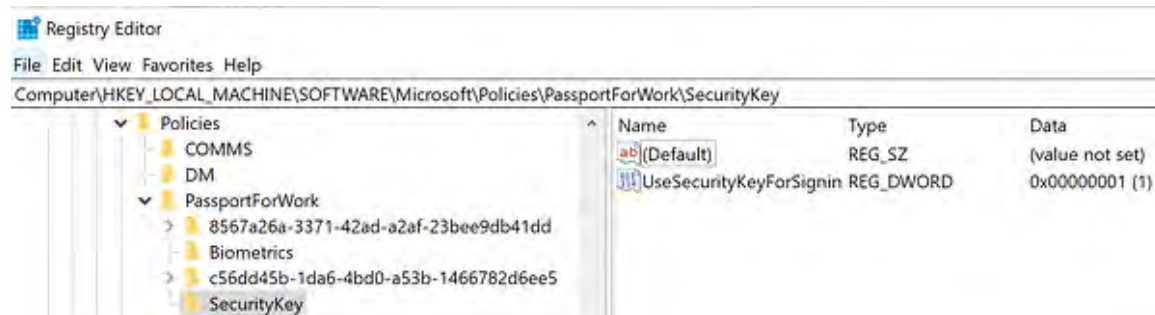
The screenshot shows a user's 'Mes connexions' (My connections) page. The 'Informations de sécurité' (Security information) section is active, showing the current default connection method as 'Microsoft Authenticator'. A red box highlights the '+ Ajouter une méthode' (Add a method) button. A modal dialog titled 'Ajouter une méthode' (Add a method) is open, asking 'Quelle méthode voulez-vous ajouter ?' (Which method do you want to add?). A dropdown menu is open, showing 'Clé de sécurité' (Security key) selected. The dialog has 'Annuler' (Cancel) and 'Ajouter' (Add) buttons.

## Étape 4

L'administrateur devra ensuite faire la modification suivante dans la «registry» locale de votre poste :

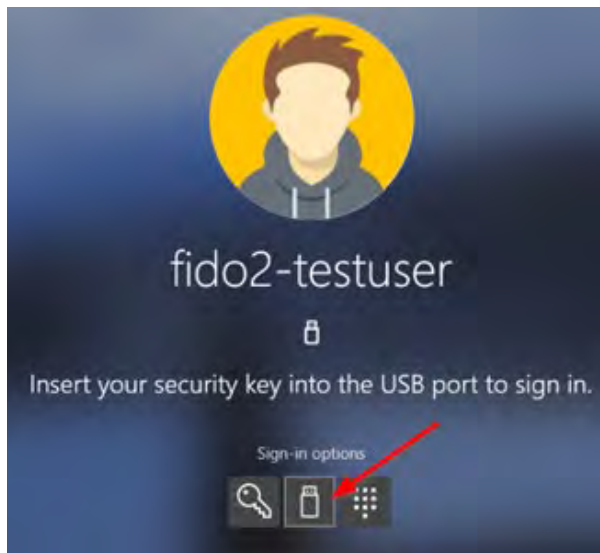
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]

« UseSecurityKeyForSignin »=dword:00000001



## Étape 5

Après ces paramètres, une nouvelle option d'authentification par clé FIDO2 et/ou carte FIDO2 pour l'ouverture de session apparaîtra.



# NEOWAVE

Pôle d'activités Yvon Morandat

1480 rue d'Arménie

13120 Gardanne

France

Tel: +33 (0)4 42 50 70 05

Email: [contact@neowave.fr](mailto:contact@neowave.fr)

<https://www.neowave.fr>

<https://www.authentication-web.fr>