

SET UP

Install and use my Winkeo key or my Badgeo card

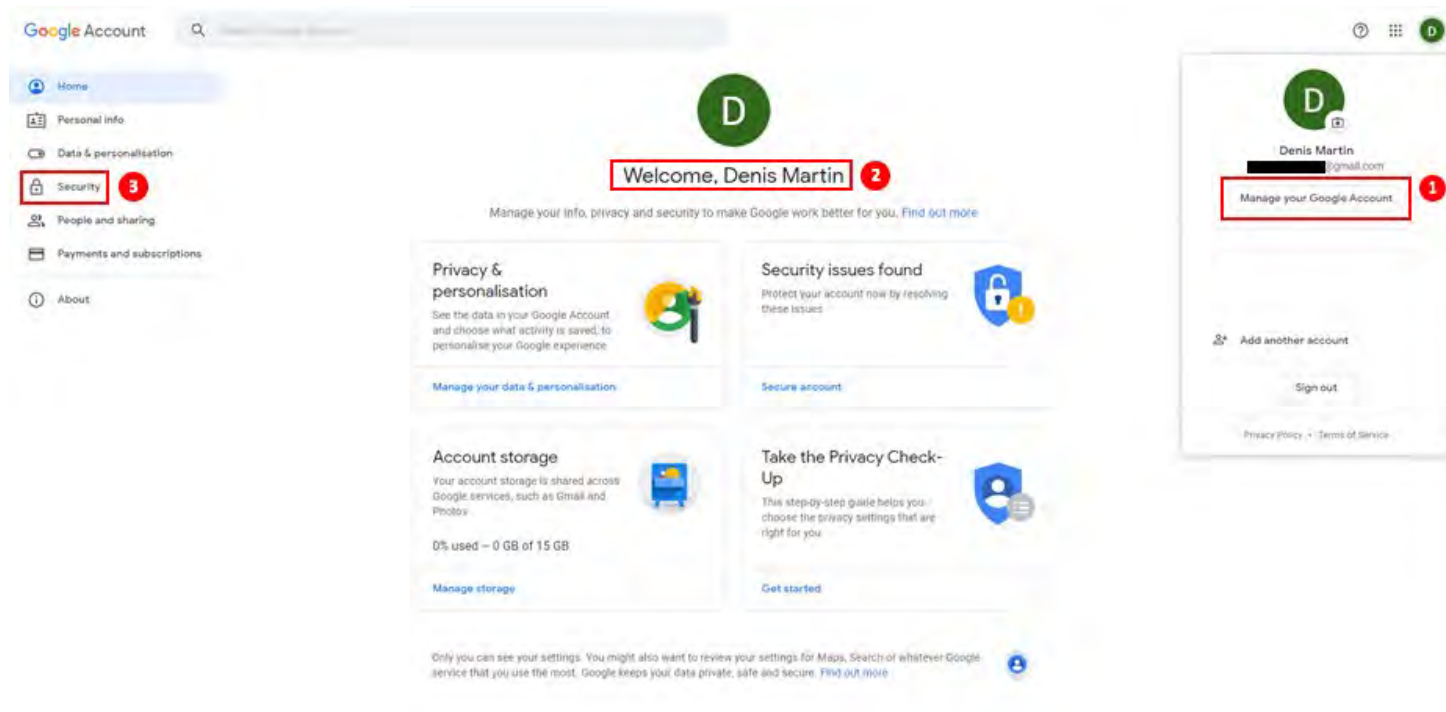
How to use the Winkeo FIDO U2F key

Before using your Winkeo FIDO U2F key, you have to set up two-factor authentication on your online account if it is not yet done. Once activated, you will have to associate your Winkeo FIDO U2F key to your account. You will find the procedure on Google here after as an example. Most web services follow a similar process consisting in selecting the "Security" tab in the "Settings" to activate the "Two-step validation" section and then to "Add a Security Key."

FIDO U2F Google Tutorial

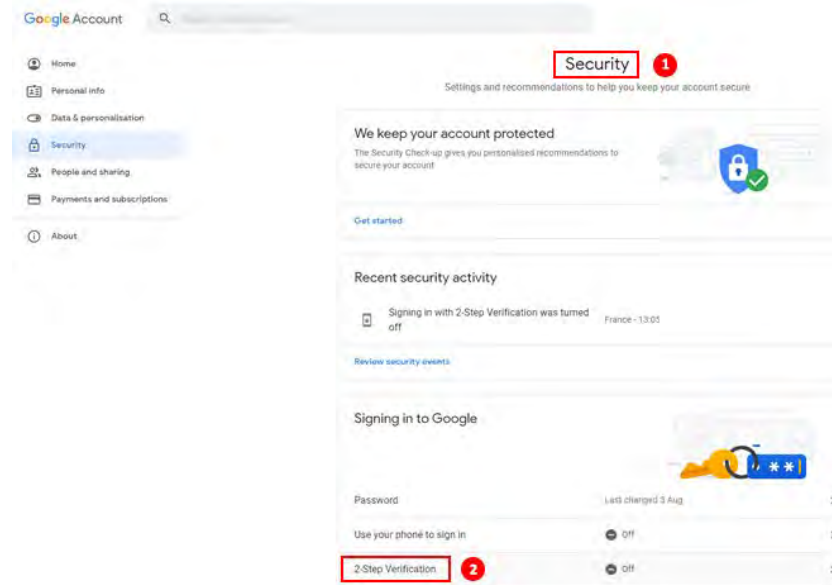
Step1

Login to your Gmail account, then click on "Manage your Google account" in the top right of your screen.



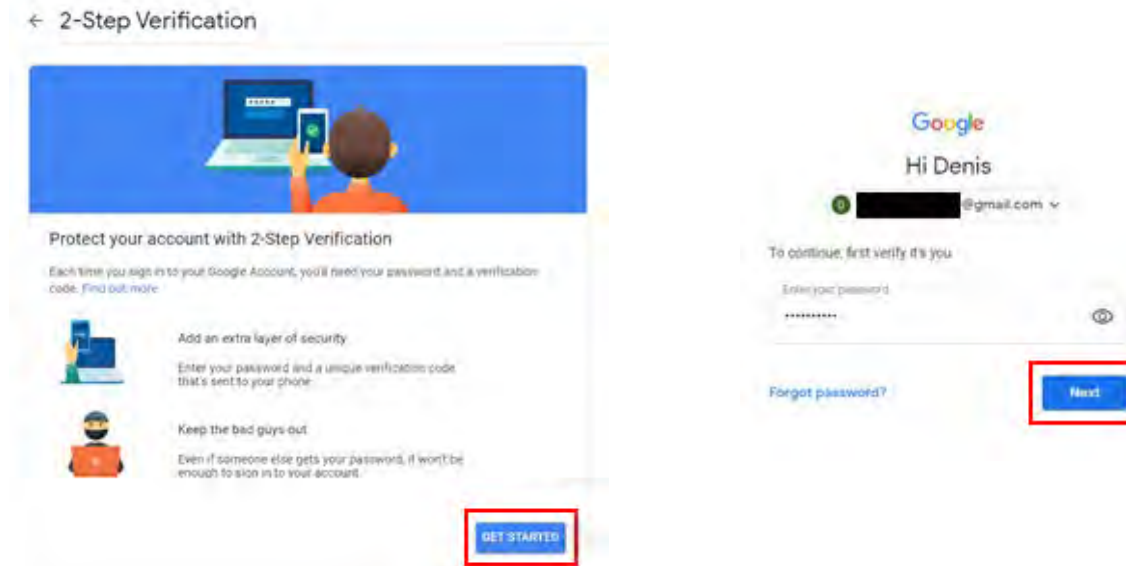
Step 2

On the "Welcome" page click on the "Security" tab. Then under "Sign in to Google" select "Two-step verification".



Step 3


Continue by clicking on "Start". Then you will need to authenticate with your Google account password. When you have done this click on "Next".



Step 4


You will be asked for a backup option with the choice of SMS or phone call. In the case of our tutorial, we will choose the SMS method. Once your telephone number has been entered, the "SMS" option checked, click on "Next". Enter the code received by SMS then click on "Next". The two-factor authentication setup for your Google account is complete. Click on "Activate" to start the activation of two-factor authentication.

← 2-Step Verification



Let's set up your phone

What phone number do you want to use?

 [Redacted phone number]

Google will only use this number to access accounts.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?


Text message Phone call

[Show more options](#)

Step 1 of 3

NEXT

← 2-Step Verification



Confirm that it works

Google just sent a text message with a verification code to [Redacted phone number]

Enter your code

Did not get it? [Resend](#)

[BACK](#) Step 2 of 3 **NEXT**

← 2-Step Verification



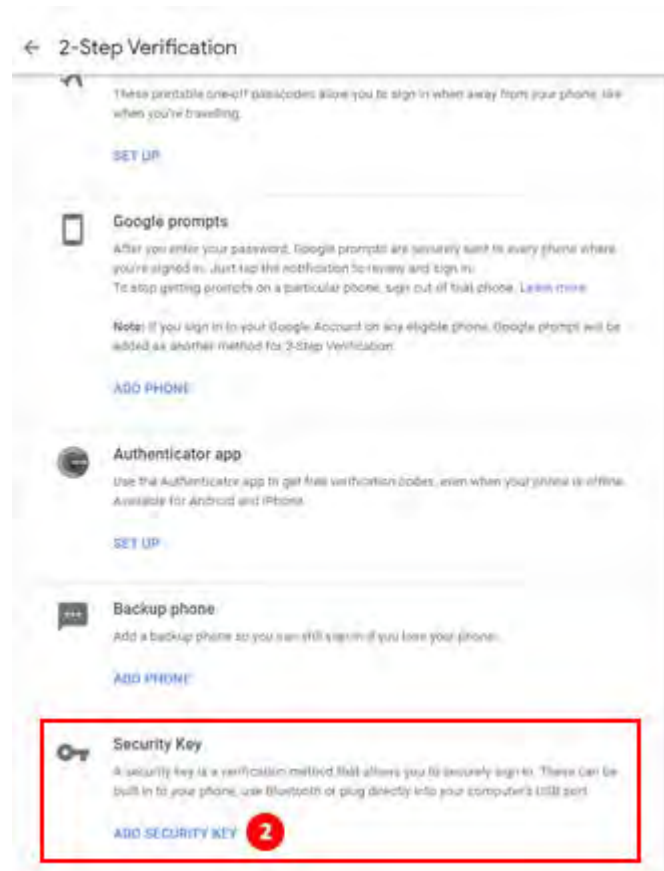
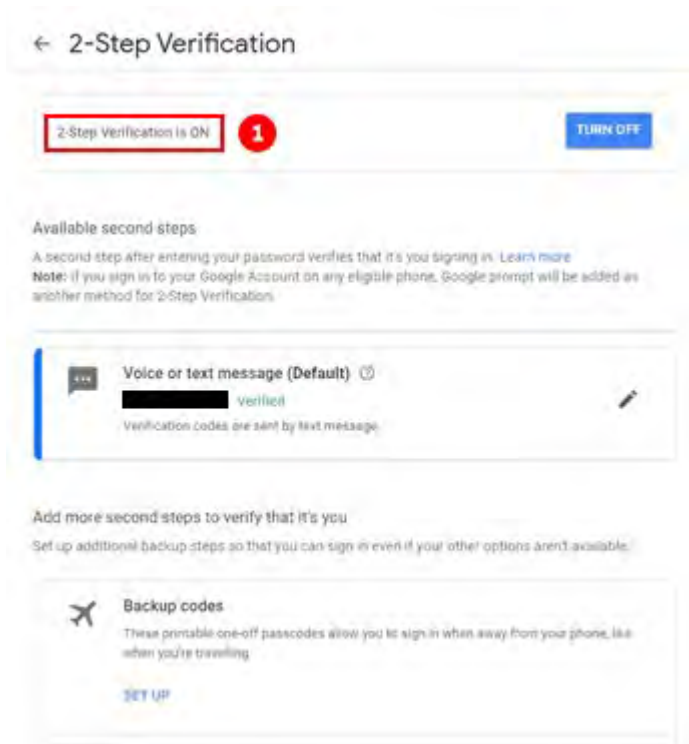
It worked! Turn on 2-Step Verification?

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google account [Redacted email address]@gmail.com?

[Cancel](#) **Turn on**

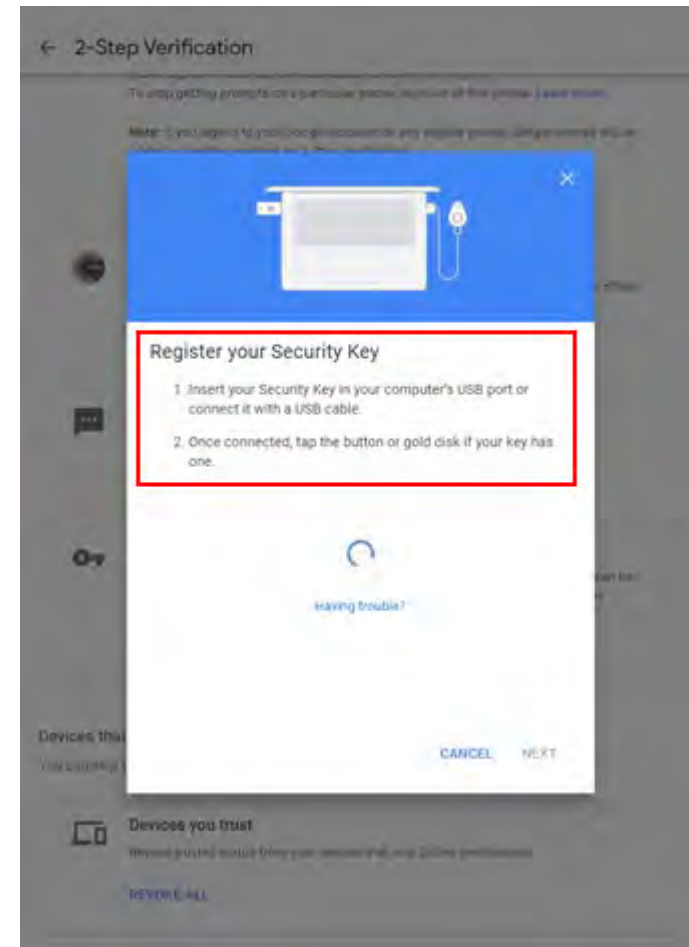
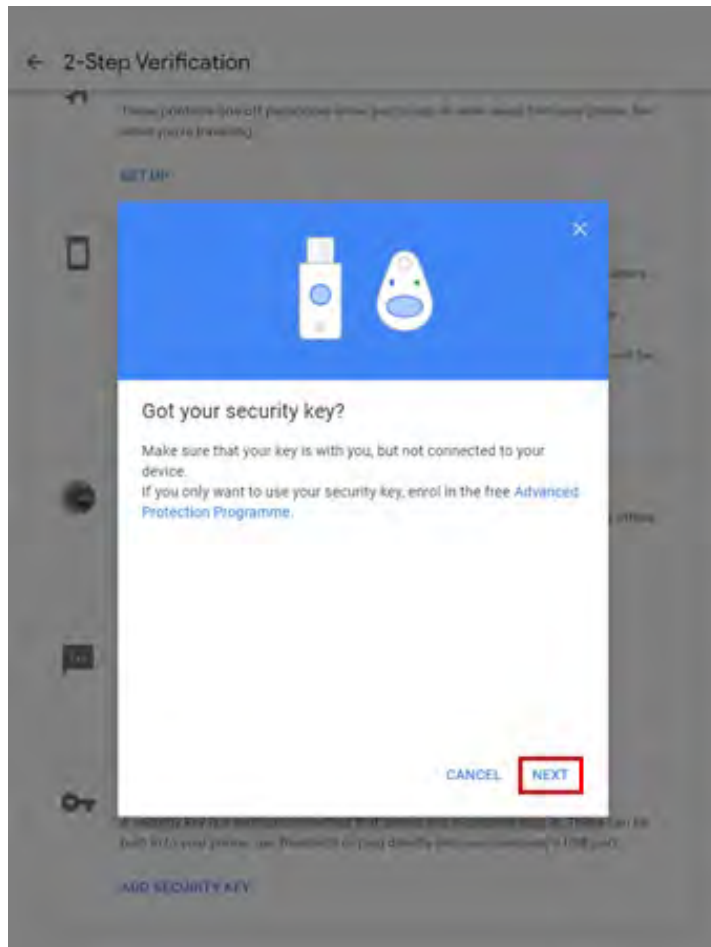
Step 5

You now need to add the Winkeo FIDO U2F security key as a second authentication step. Scroll down to the “Security Key” section and click “Add Security Key”.



Step 6

You will be offered to choose your security key, in which case click on "USB or Bluetooth" or you will be asked directly "Do you have your security key?" without going through the previous step. Then press "Next". A window "Register your security key" will open.

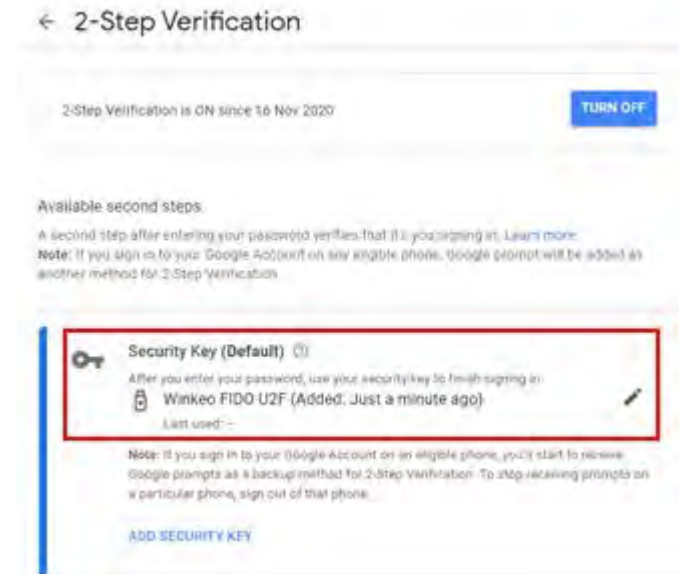
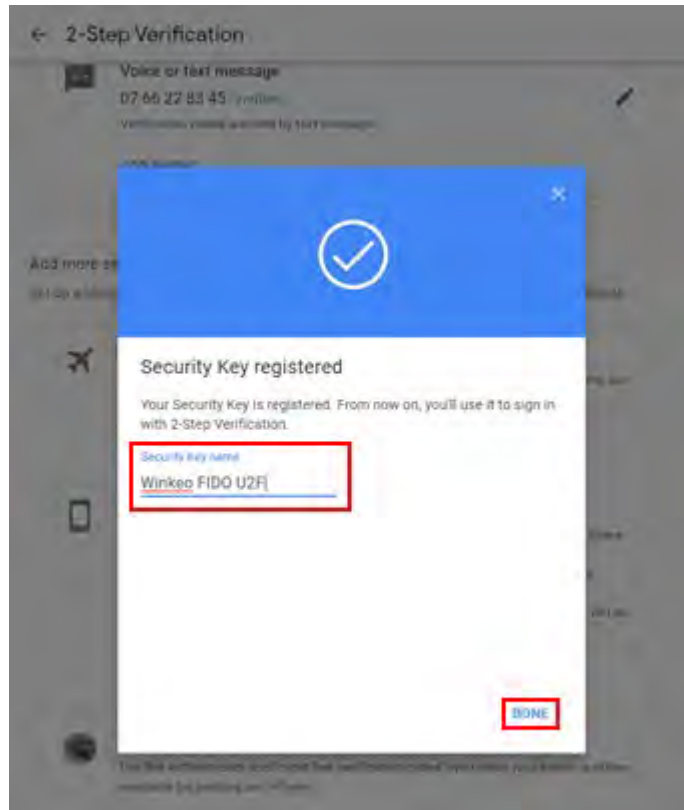


Step 7

Insert your security key into the USB port of your computer (the LED is flashing). Click "OK" on the pop-up windows that will open (« Configuring the security key » and « Continue the installation »). Once done, you will be prompted to press the golden button with which the Winkeo FIDO U2F key is equipped.

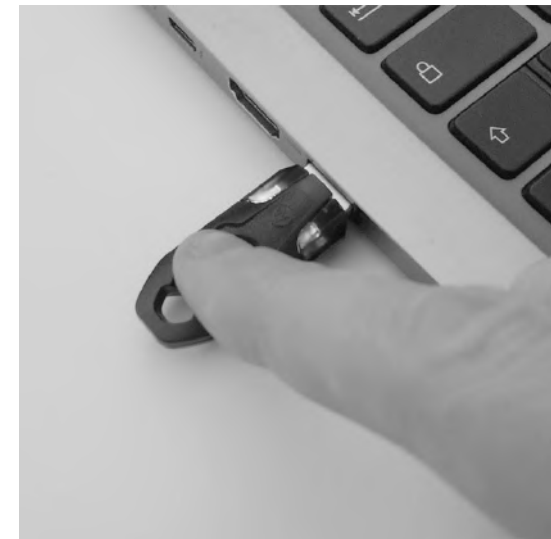
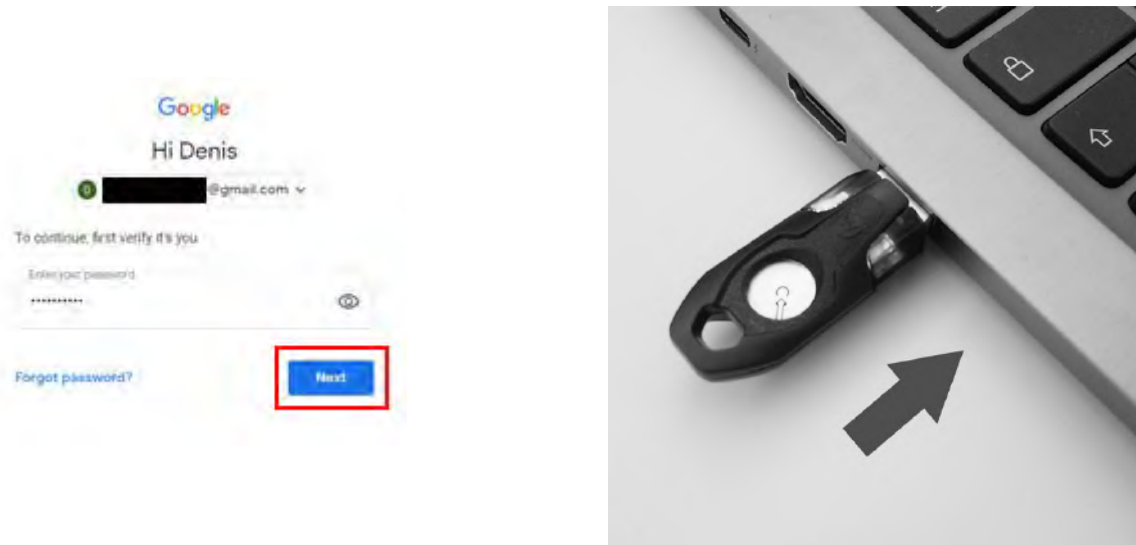
Step 8

Your security key is now saved and will be used to log in with two-step verification. Name your security key and press "OK". Two-step verification is enabled and your security key is registered.

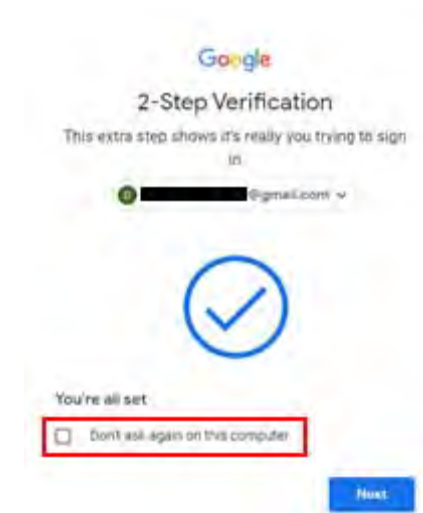


Future Connections

For any future connection to your Gmail account, you will now have to enter your password then insert the Winkeo FIDO U2F security key and press the button to authenticate yourself.



If you don't want to use your security key every time you sign in to your Google Account, check the "Don't ask me again on this computer" box. This is to indicate that your computer is reliable. However, this possibility is to be chosen only on the devices that you use regularly and that you do not share with anyone else. Otherwise, uncheck the box.



How to use the Winkeo FIDO2 key or Badgeo FIDO2 card

To associate the Winkeo FIDO2 key or Badgeo FIDO2 card with online services and applications, we invite you to contact our team or your system / network administrator in order to follow the recommendations and the appropriate procedure.

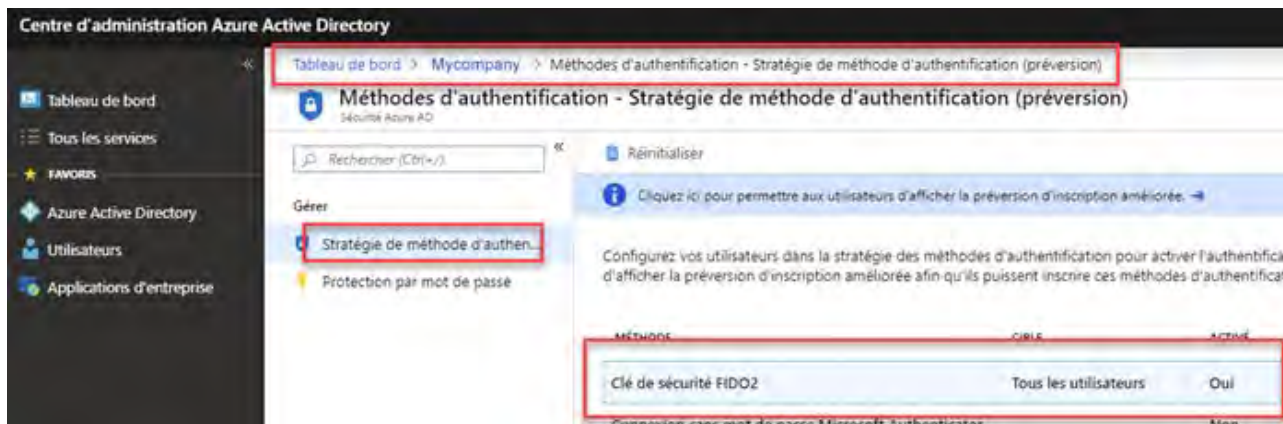
Detailed [how-to guides from Microsoft](#) also provide you with key steps to enable passwordless security key sign-in, including to [Windows 10 devices with Azure Active Directory](#).

We also provide a brief guide on how to activate a Winkeo FIDO2 key or a Badgeo FIDO2 card as a means of authentication on your Azure AD corporate directory.

FIDO2 Microsoft Tutorial

Step 1

Your network administrator will have to activate the "FIDO2 security keys" in the "Authentication method policy" in the administration centre of your Azure Active Directory <https://aad.portal.azure.com>



Step 2

The administrator will then have to choose the users who can use this method and will also have to deactivate the "key restriction" which blocks certain hardware manufacturers.

The image shows two screenshots from an administrative interface. The left screenshot, titled "CIBLE", shows a selection interface for users. A button labeled "Tous les utilisateurs" is highlighted, and a table below it lists "Tous les utilisateurs" under the "NOM" column, "Groupe" under the "TYPE" column, and "Facilité" under the "INSCRIPTION" column. The right screenshot, titled "GÉNÉRAL", shows configuration options. The "Autoriser la configuration libre-service" and "Appliquer l'attestation" options are set to "Oui". The "STRATÉGIE DE RESTRICTION DE CLÉ" section shows the "Appliquer les restrictions de clé" option set to "Non".

Step 3

You can then activate the Winkeo FIDO2 security key and / or the Badgeo FIDO2 card in your own portal. You must go to <https://mysignins.microsoft.com> and on the "Security information" tab, click on "Add a method" then choose "Security key" from the drop-down menu.

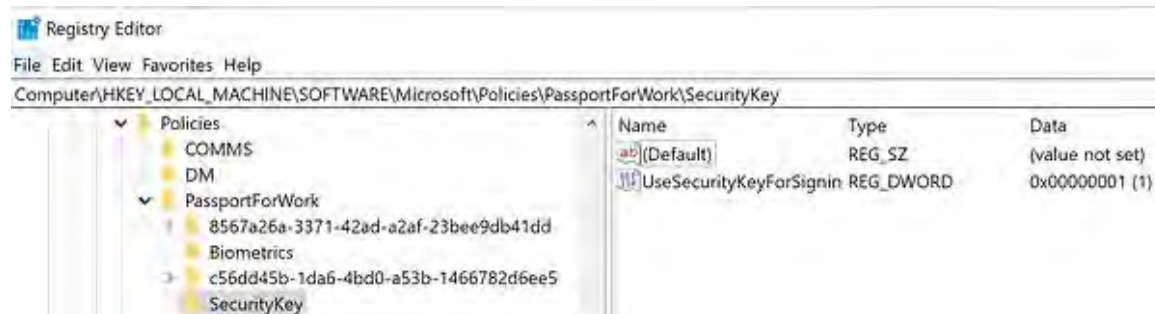
The image shows a screenshot of the "Mes connexions" (My connections) page in a user portal. The "Informations de sécurité" (Security information) section is active, showing the default connection method as "Microsoft Authenticator". A red box highlights the "+ Ajouter une méthode" (Add a method) button. A modal dialog is open, asking "Quelle méthode voulez-vous ajouter ?" (Which method do you want to add?). The "Clé de sécurité" (Security key) option is selected in the dropdown menu. The "Ajouter" (Add) button is highlighted.

Step 4

The administrator must then make the following modification in the local "registry" of your workstation:

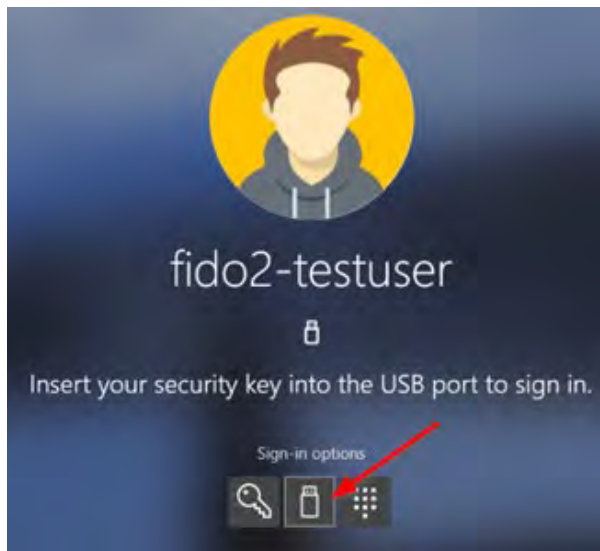
[HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Policies \ PassportForWork \ SecurityKey]

"UseSecurityKeyForSignin" = dword: 00000001



Step 5

After these changes have been performed, a new authentication option by FIDO2 key and / or FIDO2 card for opening the session will appear.



In order to be as close as possible to your web security requirements, NEOWAVE products are sold throughout Europe

Distribution partner of NEOWAVE for the United Kingdom

Open Seas

Open Seas (UK) Ltd

The Old School House

The Causeway

East Hanney

Oxfordshire

OX12 0JN

Tel: 01235 537391

Fax: 01235 535168

Email: info@openseas.co.uk

<https://www.openseas.co.uk/>