NEOWAVE

Winkeo-A/C FIDO2

User guide

PRESENTATION / QUICK GUIDE

Winkeo FIDO2 is a USB security key for strong online authentication. It protects access to your online accounts that support the FIDO U2F and FIDO2 protocols from so-called “phishing” or password theft attacks. .

Using the Winkeo security key is simple. Once the security key has been registered with an account, authentication is carried out by inserting the security key in a USB port and touching the gold disk when requested. There may also be a request to enter the security key’s PIN code.

COMPATIBILITY /DETAILS

Winkeo-A/C FIDO2 products are compatible with USB 2. and 3.X type A/C ports, directly or via a USB Hub. Using a Winkeo-A on a USB type C port or a Winkeo-C on a USB type A port is possible via a simple adapter (not supplied by default with the product).

1) **Compatibility:**
- FIDO2 compatible with Microsoft Entra ID[1]…
- FIDO U2F compatible with Gmail, Facebook, Dropbox… (see list in appendix)
- Extensive compatibility through identity federation services (WebSSO)

2) **Supported operating systems and browsers:**
- Operating systems: Windows 10 build 1903 or later, (Mac) OS X 13.51+, Linux
- Browsers : Chrome, Chromium, Vivaldi, Opera, Mozilla Firefox, Microsoft, Safari[2]

[1] Windows login requires your company to configure an Entra ID directory (see Appendix 2)
[2] For Safari on OSX, if a PIN code is requested/used you need Safari 14 Beta, otherwise Safari 13 is sufficient

3) Details:

- In some cases you will be asked to use the security key in addition to your account password.
- On certain services, you can dispense with the password.
- The PIN code is 4 to 63 characters
- The number of incorrect consecutive PIN codes is limited to 8, after which the security key must be reset.
- Winkeo security key can store up to 1024 FIDO U2F keys and 1024 FIDO2 keys (no “key wrapping”, all private keys are stored in Winkeo). Among these FIDO2 keys, 256 can be “resident” keys: additional information (name, icon, etc.) necessary for certain services (e.g. Microsoft AzureAD) is stored in WInkeo and associated with a FIDO2 key. This public information can be presented locally to the user to inform them about the use of a specific key pair.

For each online service, there are two phases of use:

- The initial enrollment phase

This is the process of associating the token with a specific account.
Pop-up menus will be displayed to guide the user during the enrollment process.

For services supporting the FIDO2 protocol the user must enter the security key’s PIN code, if no security key PIN has been created, the user will be prompted to create one.

The user will be requested to touch the security key to complete the creation of the “Passkey” that will be stored on the security key, and complete the security key - service association.

A security key can be associated with multiple accounts with each account having its own unique “Passkey”.
Multiple security keys can be associated with the same account – useful for creating backup security keys in case of loss or a security key becoming inoperable.

- The authentication phase.

Pop-up menus will be displayed to guide the user during the authentication process.

For services supporting the FIDO2 protocol the user must enter the security key’s PIN code.
The user will be requested to touch the security key. This will be indicated by a pop-up window message and also the security key will flash

Intermediate informational message on Windows 10 build 1903 or later:

Messages encouraging the user to use the security keys are managed and displayed directly by the applications. Depending on the operating system version, these messages can appear in the web browser interface.

On recent versions of Windows 10, the messages are managed directly by the operating system and inform you about the framework for using the token by indicating the domain

name of the online service, the user login, the name of the application and the name of the company that developed this application.

PIN code:

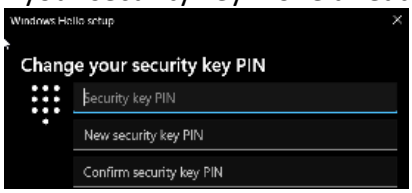
Some services may ask you to increase protection by associating a PIN code with your security key. This PIN code will then be requested for any use of your security key.

The PIN code is not sent to online services, it is only used locally to unlock the use of your security key.

PIN change and security key reset:

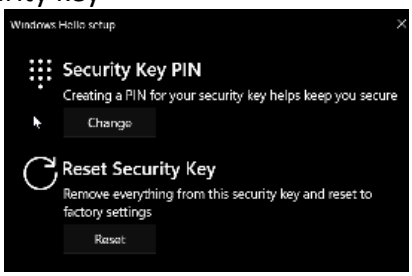
If you are in an enterprise environment, it is important to follow the local recommendations of your security officer or your system/network administrator who may have a particular procedure, offer specific reset tools for your system.

Windows 10 build 1903 or later include a configuration tool that allows you to:
- change the PIN code of your security key if one already

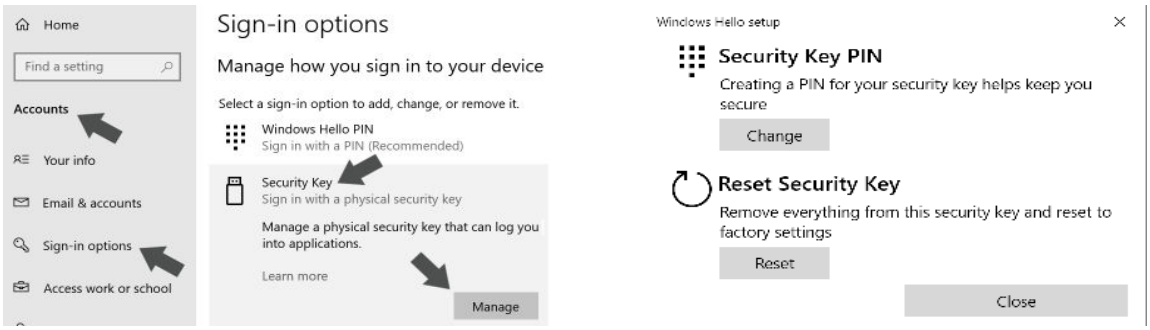


- create a PIN code for your security key if one does not exist

- reset the Winkeo security key



Please note, resetting the Winkeo security key will delete the PIN code if one exists and will also delete ALL the identities contained in the security key (and therefore all the keys (FIDOU2F keys, FIDO2 keys, resident or not).



If you lose the security key, it no longer works or it has been reset :

Online services have, in almost all cases, a support service which will allow you to access to your account through an identity verification procedure. Often another second authentication factor is provided for this purpose. Since you can generally associate several Winkeo security keys with the same account, you can also use a second one as a backup or keep one at your workplace and another at your home. If you lose the security key and are able to access your account, you should be able to delete the lost key from your account..

APPENDIX 1: Non-exhaustive list (without commitment) of services and applications compatible with the “FIDO” standard

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)

CONTENT CREATION
Blogger
Shopify
Silverstripe
Wordpress (2FA plugin)
Youtube

CRYPTO ASSETS
Bitfinex
BitGo
Coinbase
CoinFloor
DSX
Gemini
Stex

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

PASSWORD MANAGER
1Password
Bitwarden
Dashlane

IDENTITY MANAGEMENT (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

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

COMPUTER SECURITY
AppGate
Cloudflare
ISL Online
Kaseya
Norton
SAASPASS
StrongKey
XONA

SOCIAL NETWORKS
Facebook
Twitter

HEALTH
Google Fit
Isosec

OPERATING SYSTEM
Windows (Login via Azure AD)
Linux (Debian, Ubuntu, Fedora)

WEBMAIL
FastMail
Gmail
Hey
Outlook
Tutanota
Zoho Mail

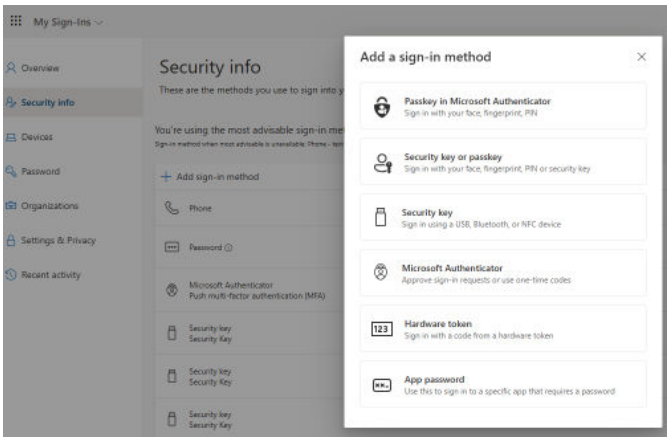
APPENDIX 2 : Entra ID and FIDO2

FIDO2 is integrated into the Entra ID architecture (formerly Azure Active Directory).

The official documentation on this integration is available here:
https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2

The user can then activate the Winkeo security key in their own portal.

https://mysignins.microsoft.com/security-info



After these settings, a new FIDO2 key authentication option for login will appear.

APPENDIX 3 : Use under Linux

You need to add a rule for udev. Create the following file with your favorite editor:

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

With the following content:

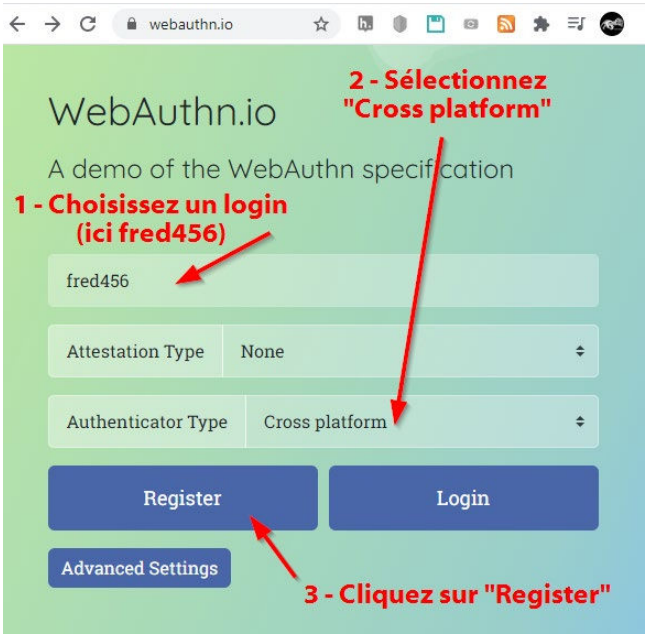
```
ACTION!="add|change", GOTO="neowave_end"
# Neowave rule
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", ATTRS{idVendor}=="1E0D",
ATTRS{idProduct}=="F1D0", TAG+="uaccess"
LABEL="neowave_end"
```

Then reload these rules with the following command:

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

Winkeo should now be usable by web browsers of your Linux distribution.

APPENDIX 4 : Test via the website Webauthn.io



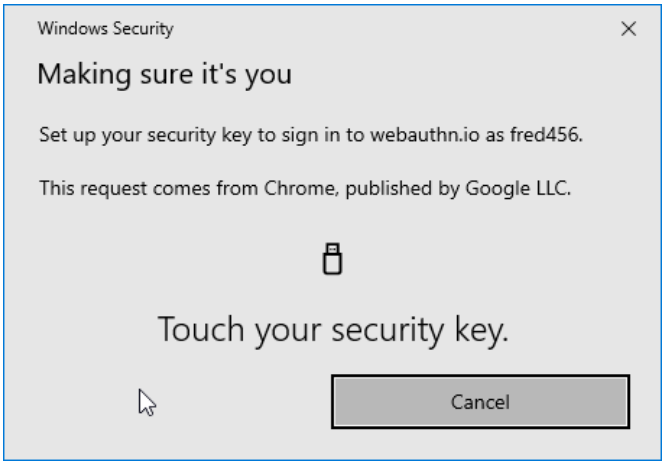
This is a simple test site to verify that your key is visible to your operating system and web browser.

This page allows you to test a key registration and then test the authentication.

Go to the website webautn.io

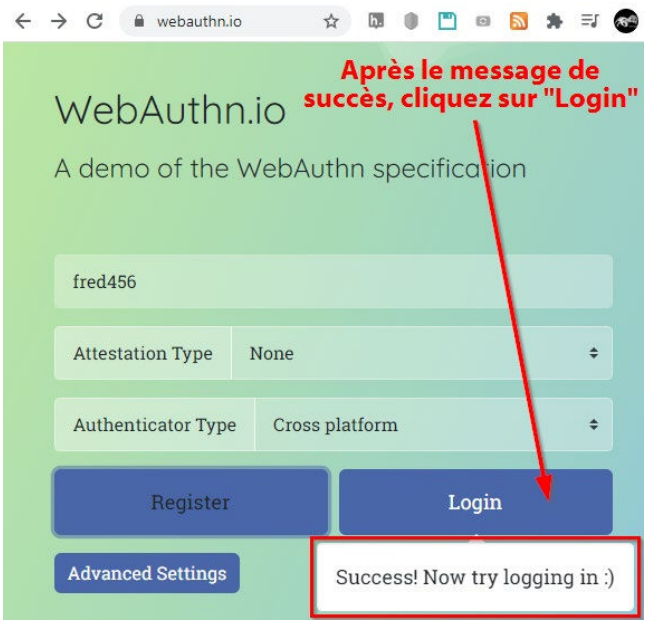
0 – Plug in your Winkeo key
1 - Choose a login
2 - Select “Cross platform” as “Authenticator Type”.

3 - Click on “Register”.rs of your Linux distribution



In Windows 10, the following information window should appear. On other operating systems, a window of the same type should invite you to touch your Winkeo key.

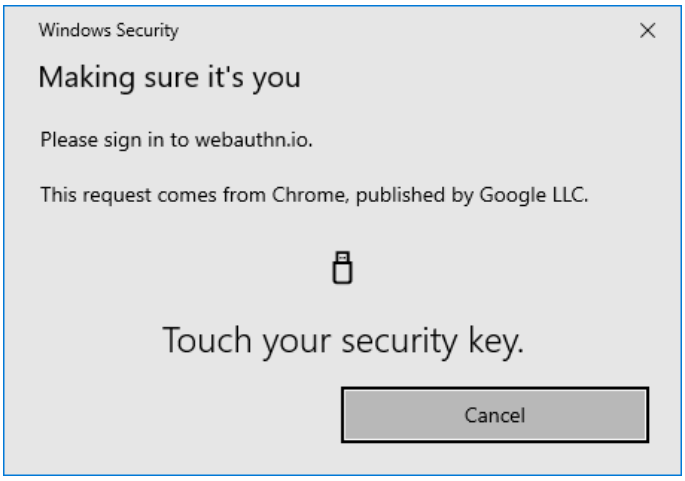
4 – Touch your Winkeo key (lightly press on its golden circle).



A success message should appear inviting you to test the “login” part now that the registration is complete.

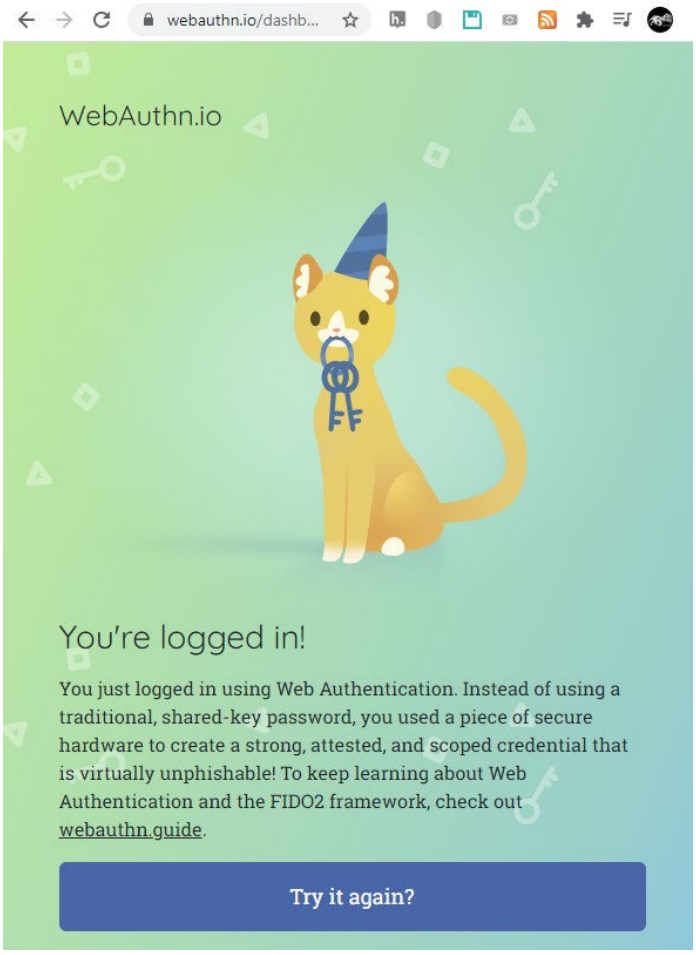
(you can check that your login and choice of authenticator have not changed).

5 - Click on the “Login” button.



The information window should appear again to invite you to touch your Winkeo key.

6 – Touch your Winkeo key (lightly press on its golden circle).



7 – A success message should appear.

Reminder: this is only a test site with no real functionality, only to test the correct functioning of the key on your browser.