

# MULTI-FACTOR-AUTHENTICATION USER GUIDE

v 1.0 - 09/09/2025

# Summary

---

**01**

Multi Factor Authentication methods

**02**

Overview of the Memory interface

**03**

Email authentication

**04**

Mobile authentication app

**05**

Web browser authentication

**06**

Hardware security Key

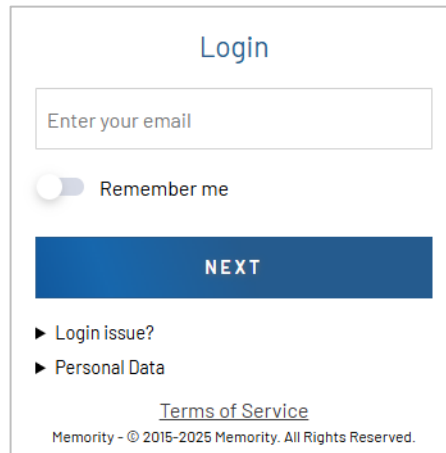


# **Multi Factor authentication methods**



# Multi-Factor Authentication methods (MFA)

## How it Works ?




### 1 – Something you know

Enter your username as usual

### 2 – Something you have

Choose your verification method

- Email verification
- Internet Browser authentication
- Mobile Phone
- Hardware Security Key

Multi-factor authentication (MFA) will be mandatory from **15 October 2025** when logging in to all Safran company customer portals

# Multi-Factor-Authentication methods (MFA)



## Email verification

A One-Time-Password (OTP) sent to your registered email address

OR



## Browser verification

Use your usual internet browser with a registered PIN code

OR



## Authentication app

Enter your PIN code on your smartphone app

OR



## Hardware security key

Plug in a physical USB key to validate your connection

We recommend that you configure your MFA methods **before October 15**

If you do not take action by 15 October 2025, **email verification will be the default MFA method** for your user account.

# MFA tips & support

- **For shared PC**

We recommend the 'Mobile authentication' and 'Security USB key' methods to ensure you can log in independently.

- **For shared account on same PC**

We recommend to use the 'email verification' (if you have access to the mailbox) or 'Browser authentication' methods

- **For shared customer portal account on different PC**

We recommend to use the 'email verification' method (if you have access to the mailbox). We strongly advise against using mobile phone and browsers authentication.

- *E.g. If you register 3 mobile phones or 3 browsers for the same account, the PIN code will be the same. The PIN code is linked to the user's account, not to the device.*



If you encounter any issues with configuring or using MFA, please contact the **support team for the relevant customer portal.**



# How to set your Multi Factor Authentication (MFA)



# My Account

Safran uses the Memory application to manage your MFA methods.

The following interfaces are available by connecting directly to the following Memory link:

<https://my.memory.com/portal/safran/>

The screenshot displays the 'My Account' page in the Memory application. The page is titled 'My Account' and shows user information for John DOE. The user's ID is HR1234, and their email is john.doe@email.com. The user's first name is John, and their last name is DOE. The account is enabled. The page is divided into sections: 'My information', 'Identity', 'Organizations', and 'Technical Information'. The 'My information' section includes tabs for 'My information', 'Edit', and 'Security'. The 'Identity' section displays the user's first name, last name, email, activation date (February 13, 2025), and last modification date (August 26, 2025). The 'Organizations' section shows a legacy organization named 'Organization A123'. The 'Technical Information' section is currently empty.

Field	Value
ID	HR1234
Email	john.doe@email.com
First Name	John
Last Name	DOE
Enabled	true
First Name	John
Last Name	DOE
Email	john.doe@email.com
Activated from	February 13, 2025
Activated until	No Value
Last modification date	August 26, 2025
Legacy Organization	Organization A123

# My Account – My information

## My Information Tab

On the « *My information* » tab it will be possible to find essential account information such as:

- First Name
- Last Name
- Email
- Status
- Organization
- username

The screenshot displays the SAFRAN user interface for account management. The top navigation bar shows the SAFRAN logo and the user's email address (jeremy.guennet.ex@safran.com) and status (Enabled: true). The left sidebar contains two main sections: 'My Account' (highlighted with a blue circle '1') and 'My Applications'. The 'My Account' section is further divided into 'My information' (highlighted with a blue circle '2') and 'Security'. The 'My information' section is expanded, showing the following details:

Identity	
First Name	John
Last Name	DOE
Email	john.doe@email.com
Activated from	February 13, 2025
Activated until	No Value
Last modification date	August 26, 2025

Below the Identity section is the 'Organizations' section, which shows:

Organizations	
Legacy Organization	Organization XXXXX

The 'Technical Information' section is currently empty.

# My Account – Security

## Security Tab

On the « Security » tab it will be possible to find all information regarding your authentication methods.

**Enrollment will be possible from here.**

The screenshot displays the SAFRAN My Account interface. The left sidebar contains 'My Account' (highlighted with a blue circle '1') and 'My Applications'. The main content area shows 'My Account User TEST' with user details: ID: XC9807, Email: user.test@gmail.com, First Name: User, and Status: ACTIVATED. Below this, the 'Security' tab is selected (highlighted with a blue circle '2'). The Security section includes:

- Password**: Password authentication status is Active; Password Expiration Date is November 22, 2025.
- Enroll my keys** (Windows Hello or Physical Secure Key): Includes a section for Web authentication keys (Registered web authentication keys (FIDO2 & WebAuthn)) with the message 'You have no devices currently enrolled.'
- Enroll the Memory Mobile App or my Web Browser** (Browser or Memory Mobile App): Includes a section for Trusted devices (Registered devices for multi factor authentication).



# Email Authentication

## Enrollment & Login

---

# Email authentication – Enrollment

## Enroll my email address

1. Go to « My Account » > « Security »
2. In “Email code” section click on « **Enroll** » & click on «confirm»

*This will enroll the email address registered in the ‘My information’ section.*

i

If you do not take action by 15 October 2025, email verification **will be the default MFA method** for your user account.

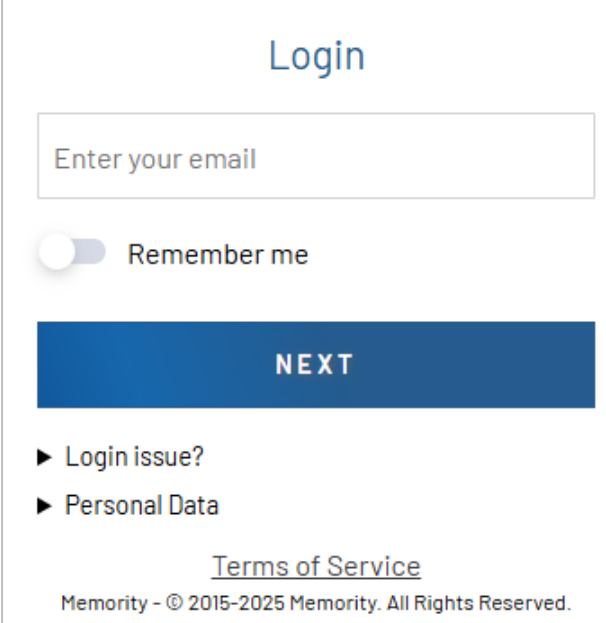
The screenshot shows the SAFRAN My Account Security page. The left sidebar contains 'My Account' and 'My Applications'. The main content area is divided into sections: Password, I enroll my key, Trusted devices, and Email Code. The Email Code section is highlighted with a red box, showing a '+ Enroll' button and a table of enrolled email addresses.

Address	Status	Created At	Last Used	Type	Module
j*****m@g*****l.com	✓ ACTIVE	08/27/2025 10:36:10	Unused	Email	MemoryOtpMail

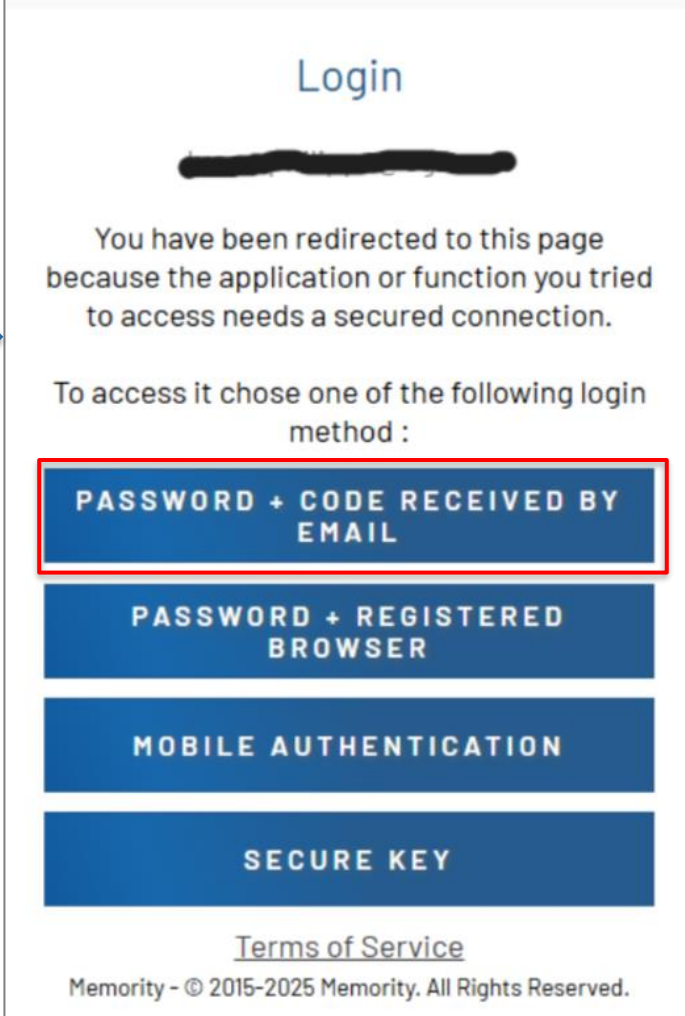
# Email authentication – How to login

## 1 - Login page

- Go on the **customer portal** login page
- Fill in the login field with your email address.
- Click on « Next »



**2 – Select « Password + code received by email »**

# Email authentication – How to login

The diagram illustrates the login process in two stages. On the left, the 'Password' screen features a grey password input field, a text input field labeled 'Password', a blue 'LOG IN' button, a white 'CHANGE LOGIN' button, a link for 'Forgot my password', and a list of links: 'Login issue?' and 'Personal Data'. At the bottom, it reads 'Memory - © 2015-2025 Memory. All Rights Reserved.' An arrow points to the right, where the 'Login' screen is shown. This screen has a grey password input field, a 'Choose a mail address' section with a radio button selected next to 'j\*\*\*\*\*m@g\*\*\*\*\*l.com', a blue 'SEND OTP' button, a white 'CHANGE LOGIN' button, and the same footer text.

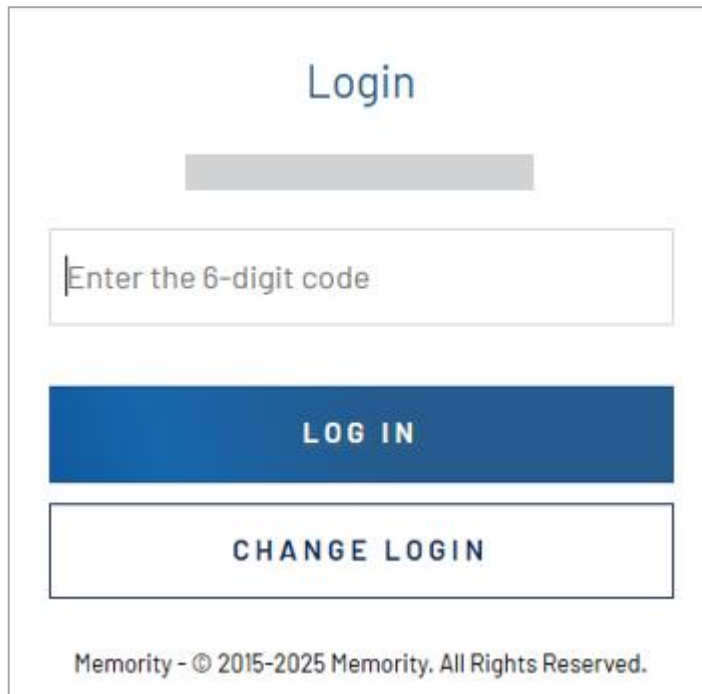
**3** – Enter your Password & click on « log in »

**i**

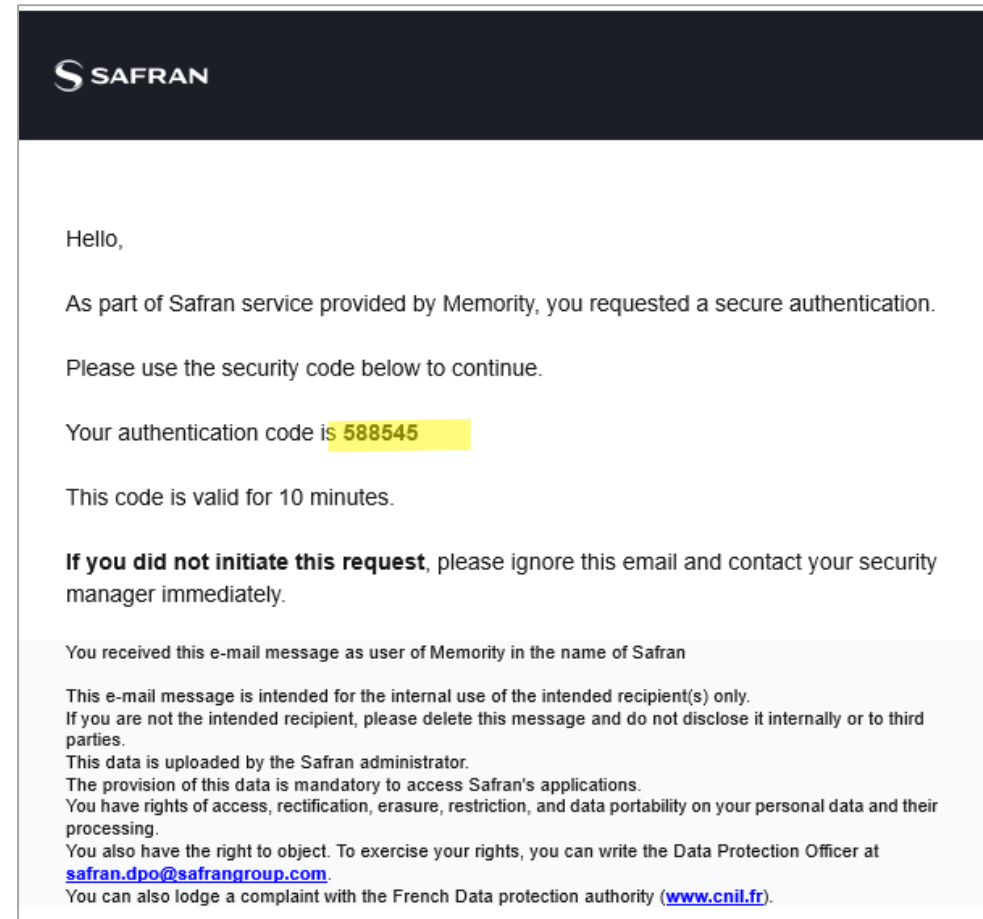
This is the password you use to log into your customer portal.

**4** – Select the email and click on « **Send OTP** »

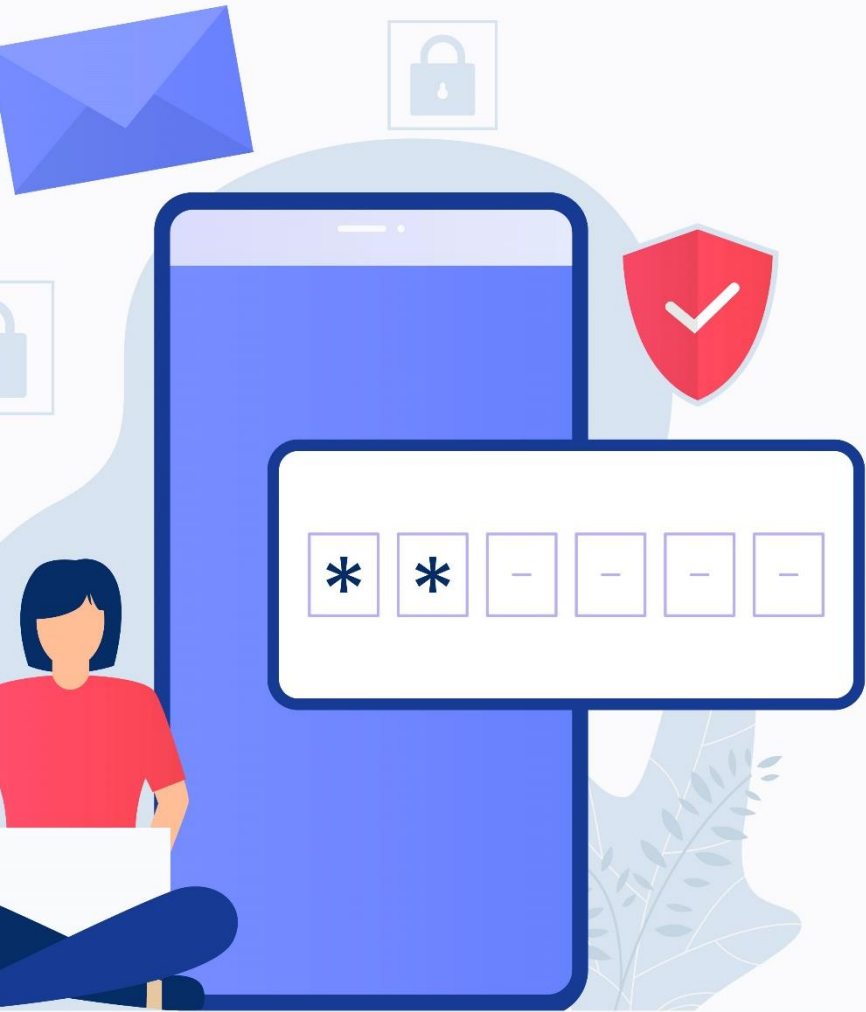
# Email authentication – How to login



**5** – Enter the **code received by email** and click on « Log In »



*Email received with authentication code*



# Mobile authentication application

## Enrollment & login

---

# Mobile Authentication application - Enrollment

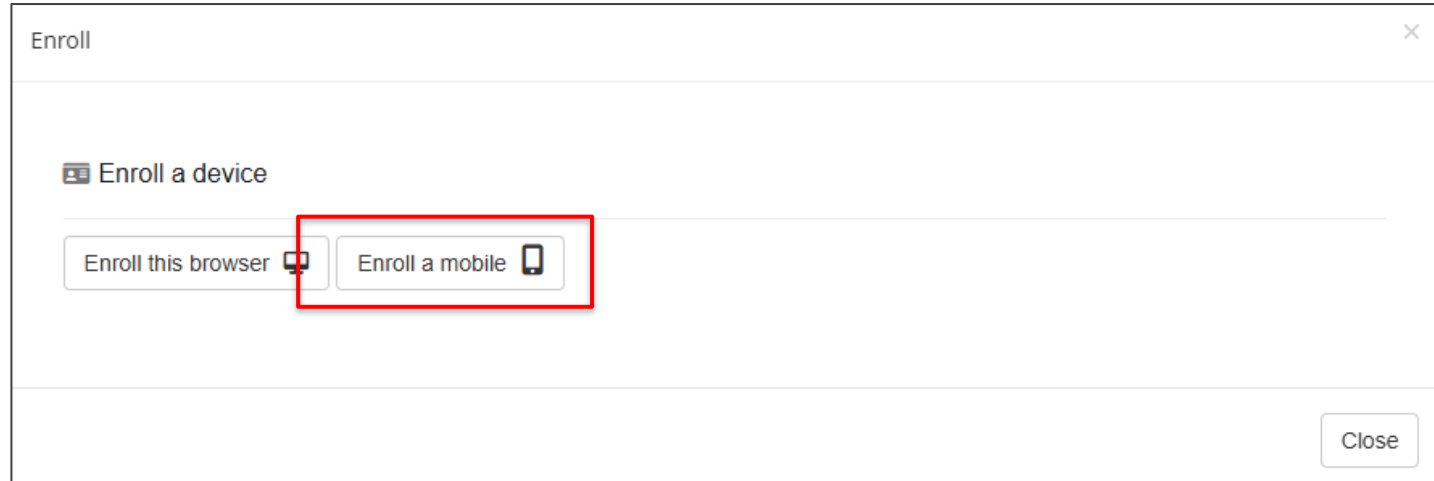
## Enroll Memory Mobile App

1. Go to « My Account » > « Security »
2. In “Enroll the Memory Mobile app or my Web Browser” section click on « **Enroll** »

The screenshot displays the SAFRAN user interface. On the left, a navigation menu shows 'My Account' and 'My Applications'. The main content area is divided into two sections. The top section, 'I enroll my key', includes options for 'Windows Hello' and 'Secure Key', and a 'Trusted devices' section with a 'Refresh' button. The bottom section, 'I enroll the Memory Mobile App or my Web Browser', includes an 'Unlock' button and a '+ Enroll' button, which is highlighted with a red box. A red arrow points from the 'Refresh' button in the top section to the '+ Enroll' button in the bottom section.

# Mobile Authentication application - Enrollment

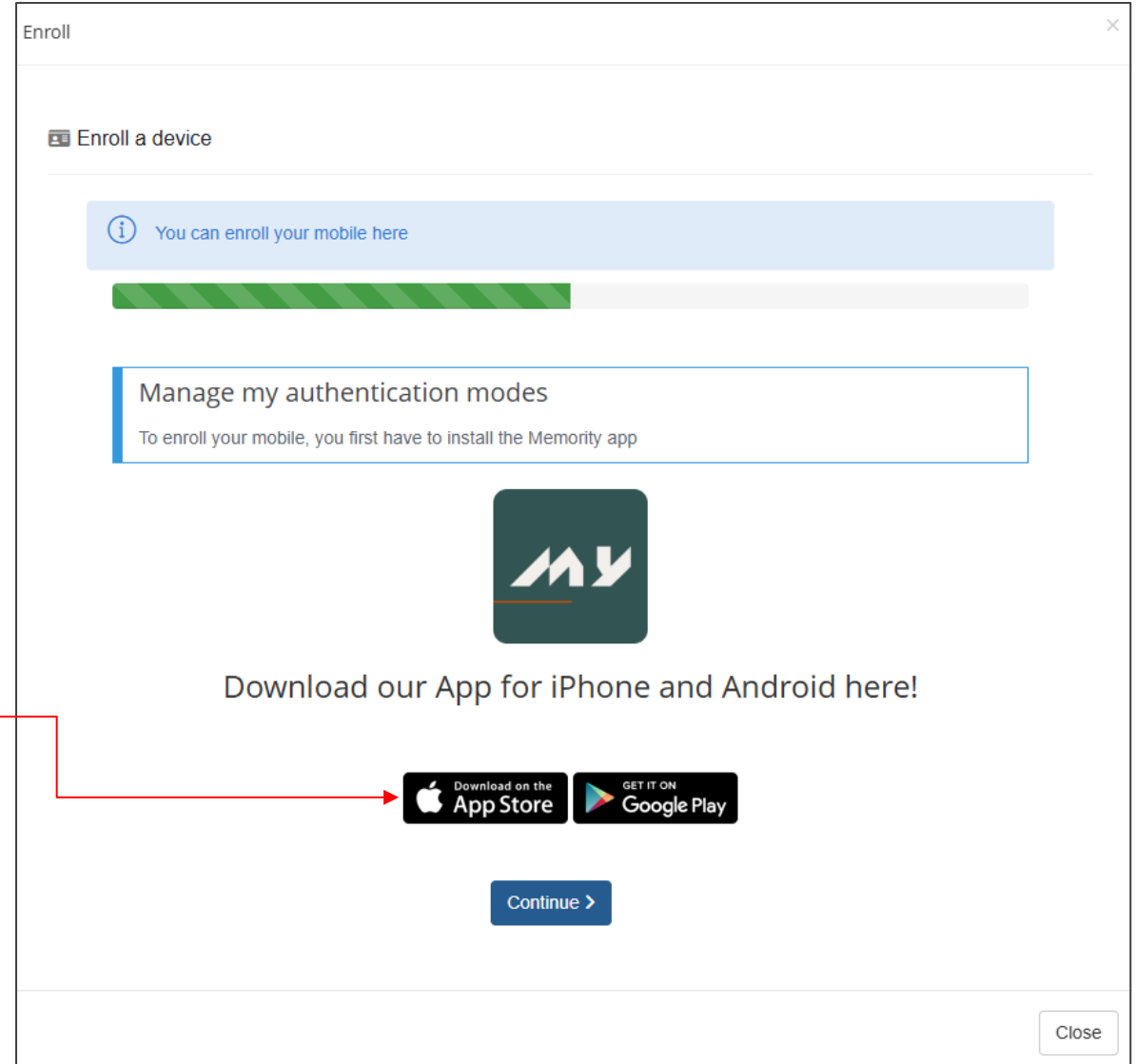
2 – Click on « Enroll a mobile»



# Mobile Authentication application - Enrollment

**3** – Download Memory Authenticator App on the store

**4** – Click on « continue »



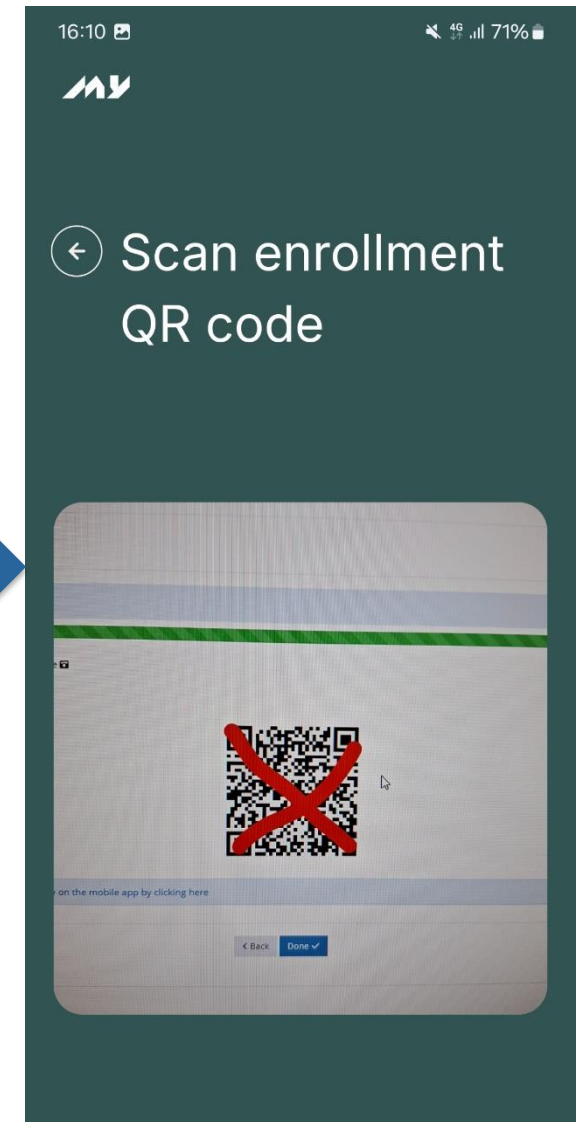
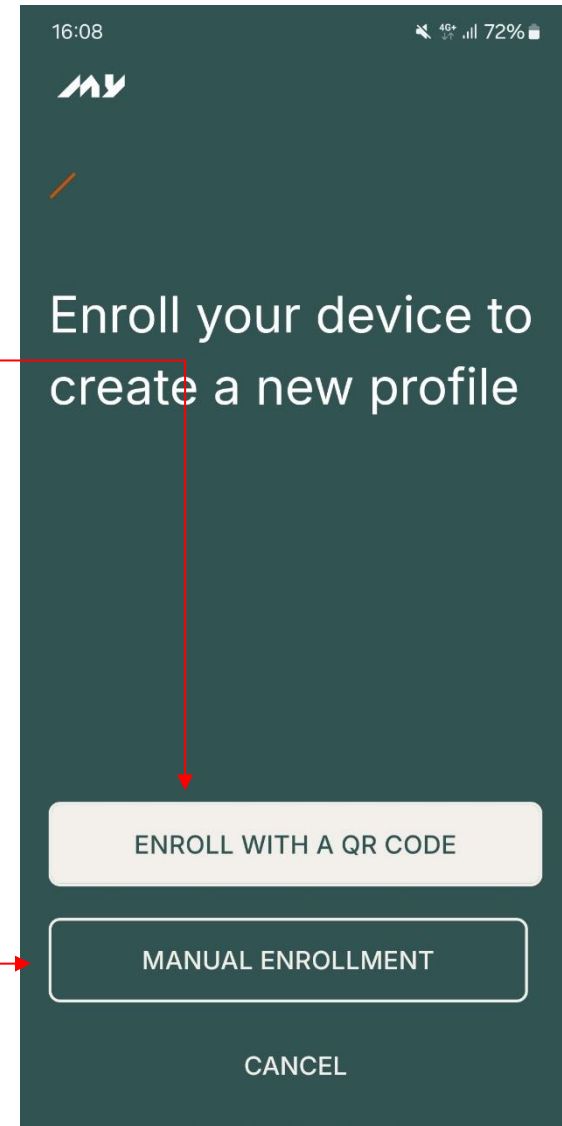
# Mobile Authentication application - Enrollment

**5** – On your smartphone open the Memory App

**6** – Click on « Enroll with a QR code »

OR

**6\*** – **If necessary**, you can manually enroll your app by clicking on “Manual enrollment”.  
You will need to fill in the tenant, which is: safran

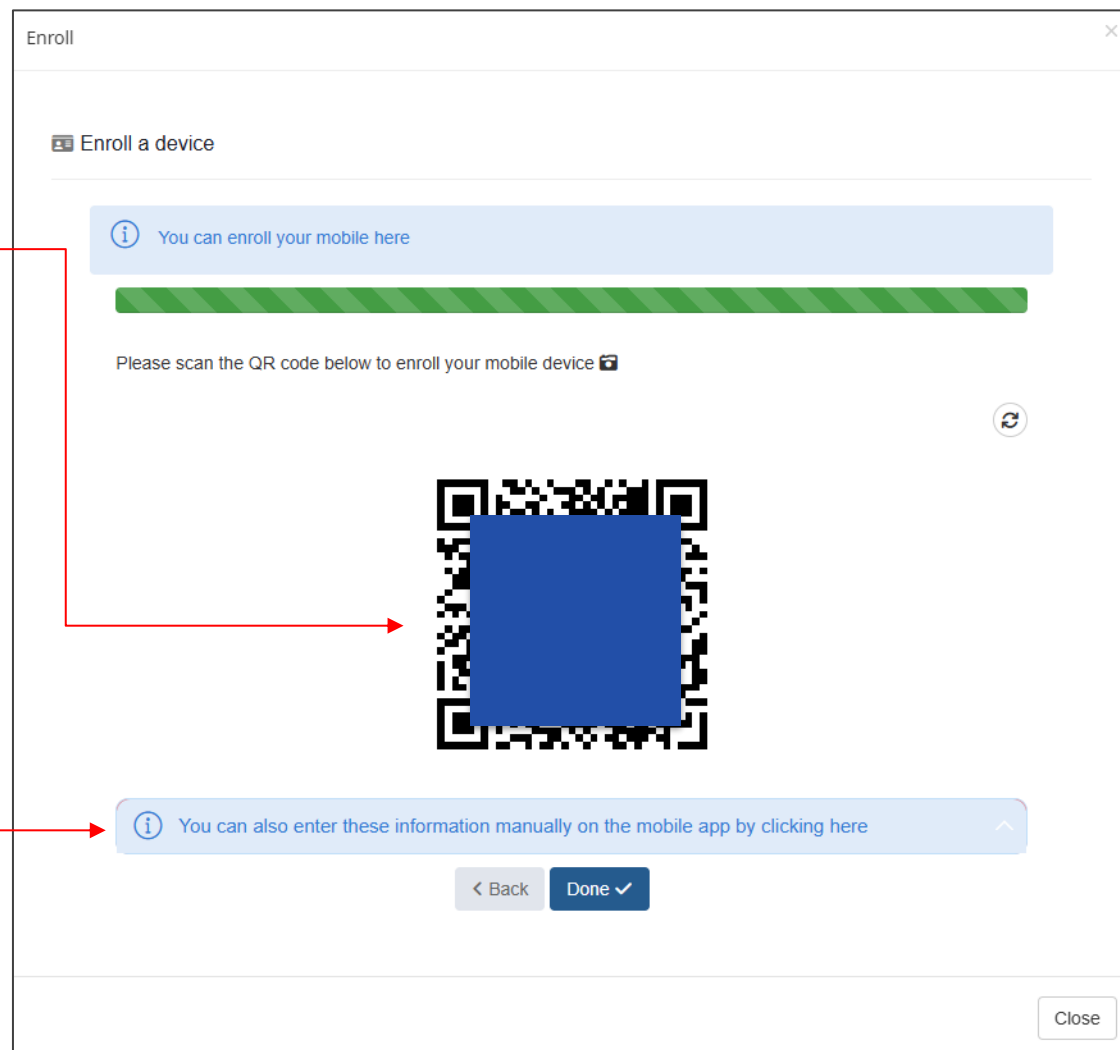


# Mobile Authentication application - Enrollment

**7** – From the app, Flash the QR code to enroll your device

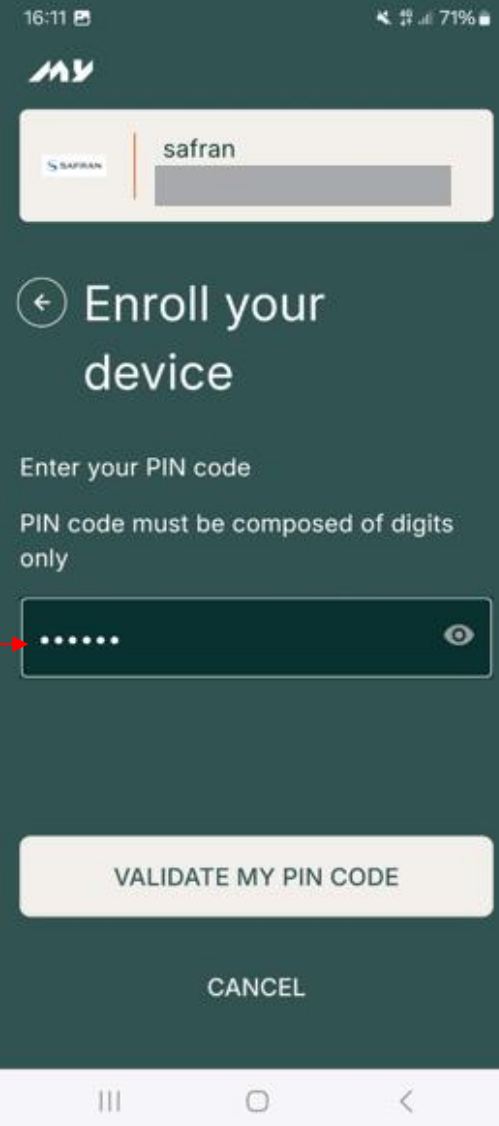
**OR**

**7\*** – **If necessary**, you can manually enter your authentication details by clicking here. You will need to fill in the tenant, which is: safran



# Mobile Authentication application - Enrollment

8 – Set a PIN code for the app



16:11 71%

SAFRAN safran

← Enroll your device

Enter your PIN code

PIN code must be composed of digits only

.....

VALIDATE MY PIN CODE

CANCEL

**i** In the event of inactivity (no connection with this method) exceeding 365 days, this method will expire.

# Mobile Authentication application – How to login

## 1 – Login page :

- Go on the **customer portal** login page
- Fill in the login field with your email address.
- Click on « Next »



## 2 – Select «Mobile Authentication»

# Mobile Authentication application – How to login

Login

[Redacted]

A notification with security code KT-IZ has been sent to your mobile. Please click on it and enter your PIN code to continue.

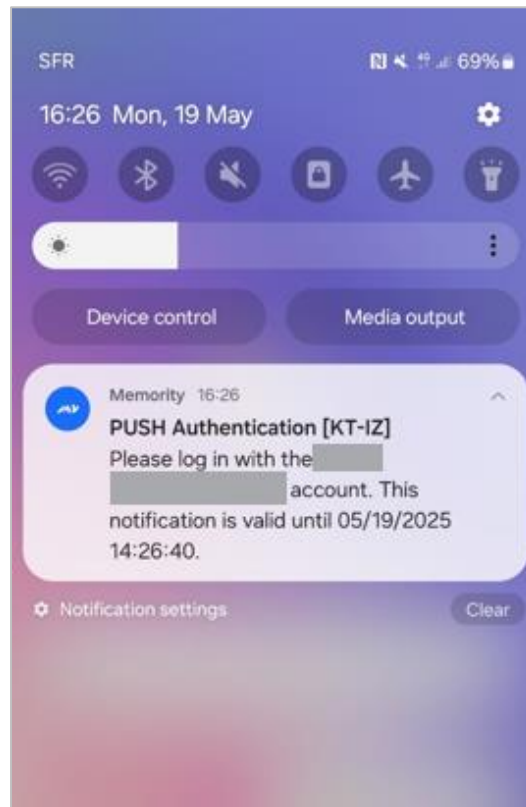
Loading ...

PUSH AUTHENTICATION

ENTER CODE

CHANGE LOGIN

Memory - © 2015-2025 Memory. All Rights Reserved.



16:26 69%

Validate Push Authentication

Only accept this authentication if you see the following code on the login page: KT-IZ

Login with your PIN code

PIN code must be composed of digits only

[Redacted PIN code]

Forgot PIN code?

VALIDATE

CANCEL

**3** – A **notification** will be sent to your smartphone, click on it.

**4** – In the app, enter your **PIN code** & validate

Go back on the Customer portal, you're logged in.



# Web Browser authentication

## Enrollment & login

---

# Web Browser authentication – Enrollment

## Enroll my Web Browser

1. Go to « My Account » > « Security »
2. In “Enroll the Memory Mobile app or my Web Browser” section click on « **Enroll** »



This is the password you use to log in to your customer portal.



The screenshot displays the SAFRAN customer portal interface. The top navigation bar includes the SAFRAN logo, a user profile icon with the name 'JD', and a 'History' dropdown menu. The left sidebar shows a 'My Account' dropdown menu with options for 'My Account' and 'My Applications'. The main content area is divided into two sections:

- I enroll my key** (Windows Hello or physical Secure Key): This section features buttons for 'Windows Hello' and 'Secure Key'. Below, there is a 'Trusted devices' section with the text 'Registered web authentication keys (FIDO2 & WebAuth)' and a 'Refresh' button. A message states 'You have no devices currently enrolled.'
- I enroll the Memory Mobile App or my Web Browser** (Browser or Memory Mobile App): This section features an 'Unlock' button and a '+ Enroll' button, which is highlighted with a red box. Below, there is a 'Trusted devices' section with the text 'Registered devices for multi factor authentication' and a 'Refresh' button. A message states 'You have no devices currently enrolled.'

# Web Browser authentication – Enrollment

Enroll

Enroll a device

Enroll this browser  Enroll a mobile 

Close

**2** – Choose « Enroll this browser »

**3** – Name your browser


**4** – Enter a **PIN code** for this browser & click on « Activate »

i

In the event of inactivity (no connection) exceeding 365 days, this method will expire.

ENROLL

MFA activation Enroll device

 You can enroll your browser here

**Activate TrustBuilder authentication service**

Site: AWS-Citadel-CSTAGE-S...

Name this trusted device:

Edge on Windows  
e.g. Chrome at Home, Safari at Work

Confirm your identity

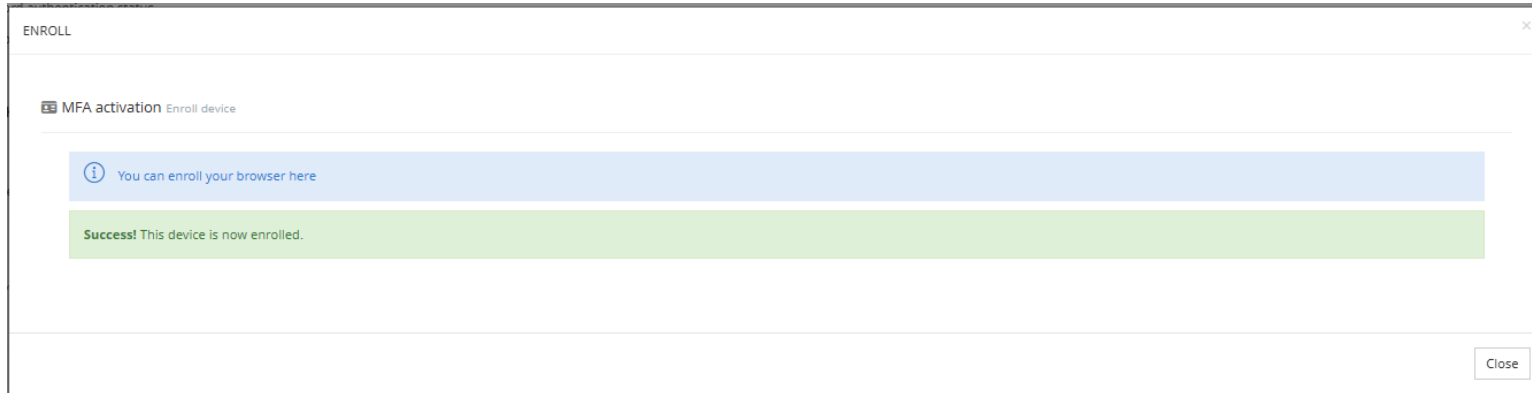
PIN code:

\*\*\*\*\*

Activate TrustBuilder

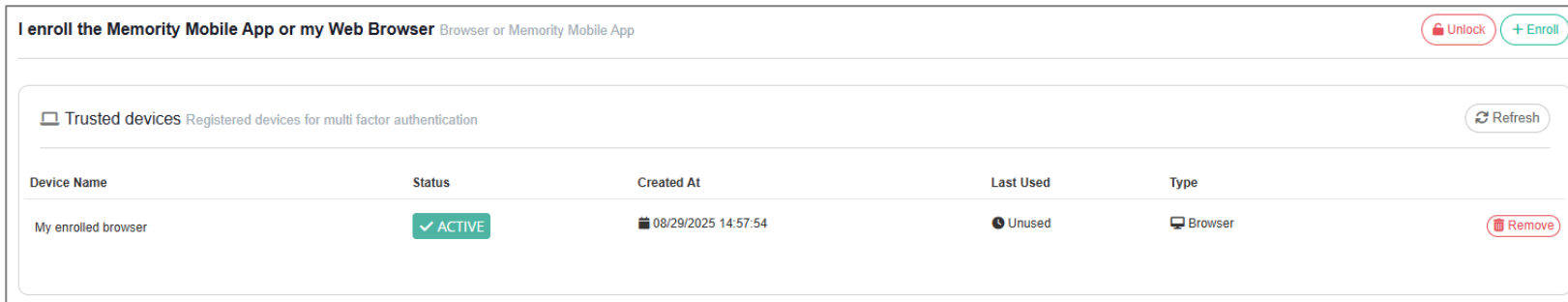
Helium - © 2025 inWebo Technologies

# Web Browser authentication – Enrollment



## Memory Confirmation

Memory message to confirm the registration of the Browser



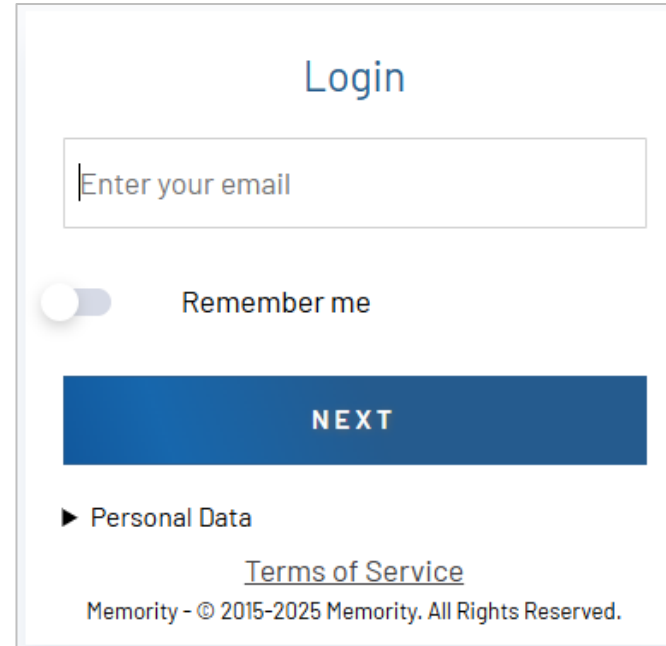
## Memory interface

The Browser is now visible in your interface (My Account > Security > « I enroll the memory mobile app or my web browser »)

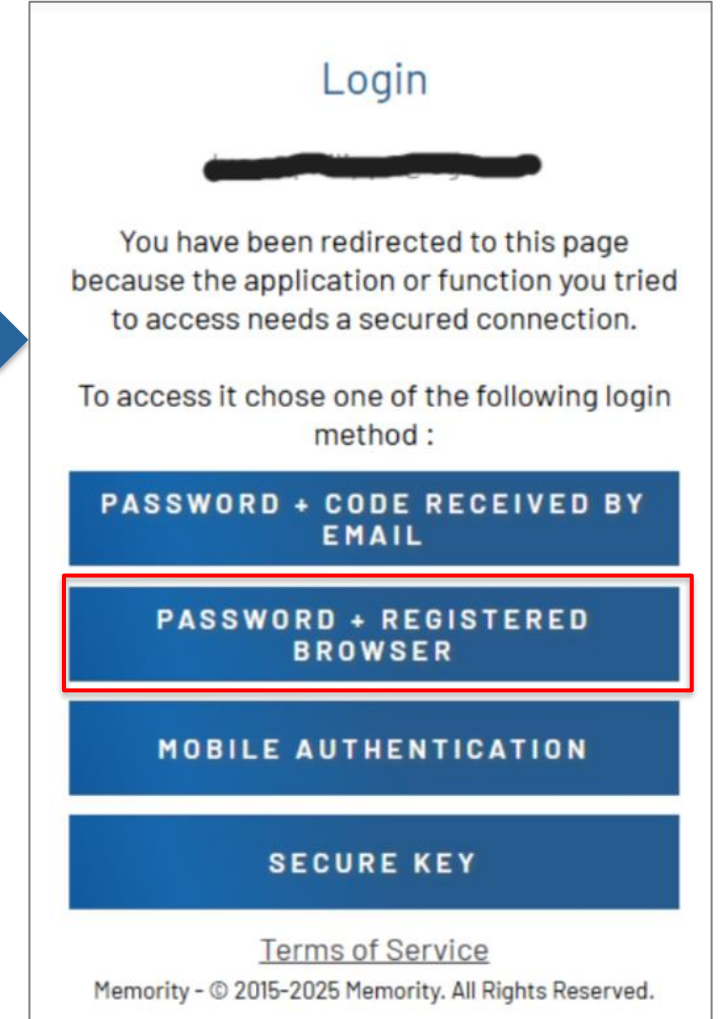
# Web Browser authentication – How to login

## 1 – Login page :

- Go on the **customer portal** login page
- Fill in the login field with your email address.
- Click on « Next »



The screenshot shows a login page titled "Login". It features a text input field with the placeholder text "Enter your email". Below the input field is a toggle switch labeled "Remember me". A large blue button labeled "NEXT" is positioned below the toggle. At the bottom of the page, there is a link for "Personal Data", a link for "Terms of Service", and a copyright notice: "Memory - © 2015-2025 Memory. All Rights Reserved."



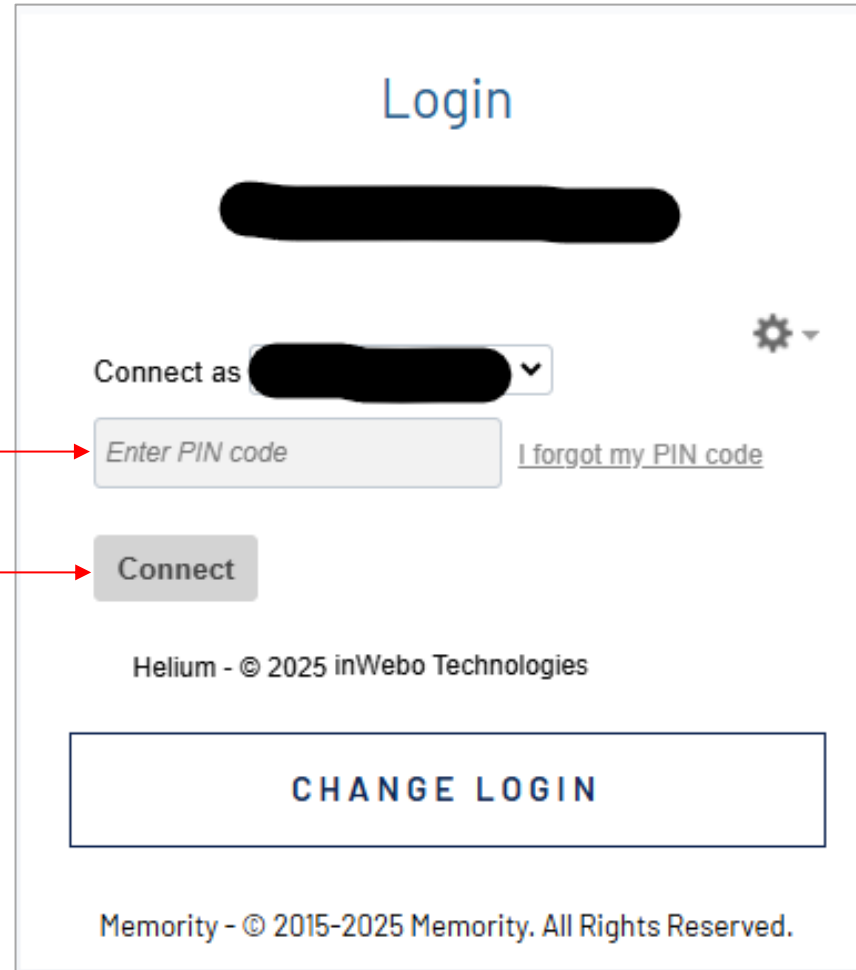
The screenshot shows a redirected login page titled "Login". The top part of the page is redacted with a black bar. Below the redaction, the text reads: "You have been redirected to this page because the application or function you tried to access needs a secured connection. To access it chose one of the following login method :". There are four blue buttons stacked vertically, each representing a login method: "PASSWORD + CODE RECEIVED BY EMAIL", "PASSWORD + REGISTERED BROWSER" (highlighted with a red border), "MOBILE AUTHENTICATION", and "SECURE KEY". At the bottom, there is a link for "Terms of Service" and a copyright notice: "Memory - © 2015-2025 Memory. All Rights Reserved."

- ## 2 – Select « Password + Registered browser»

# Web Browser authentication – How to login

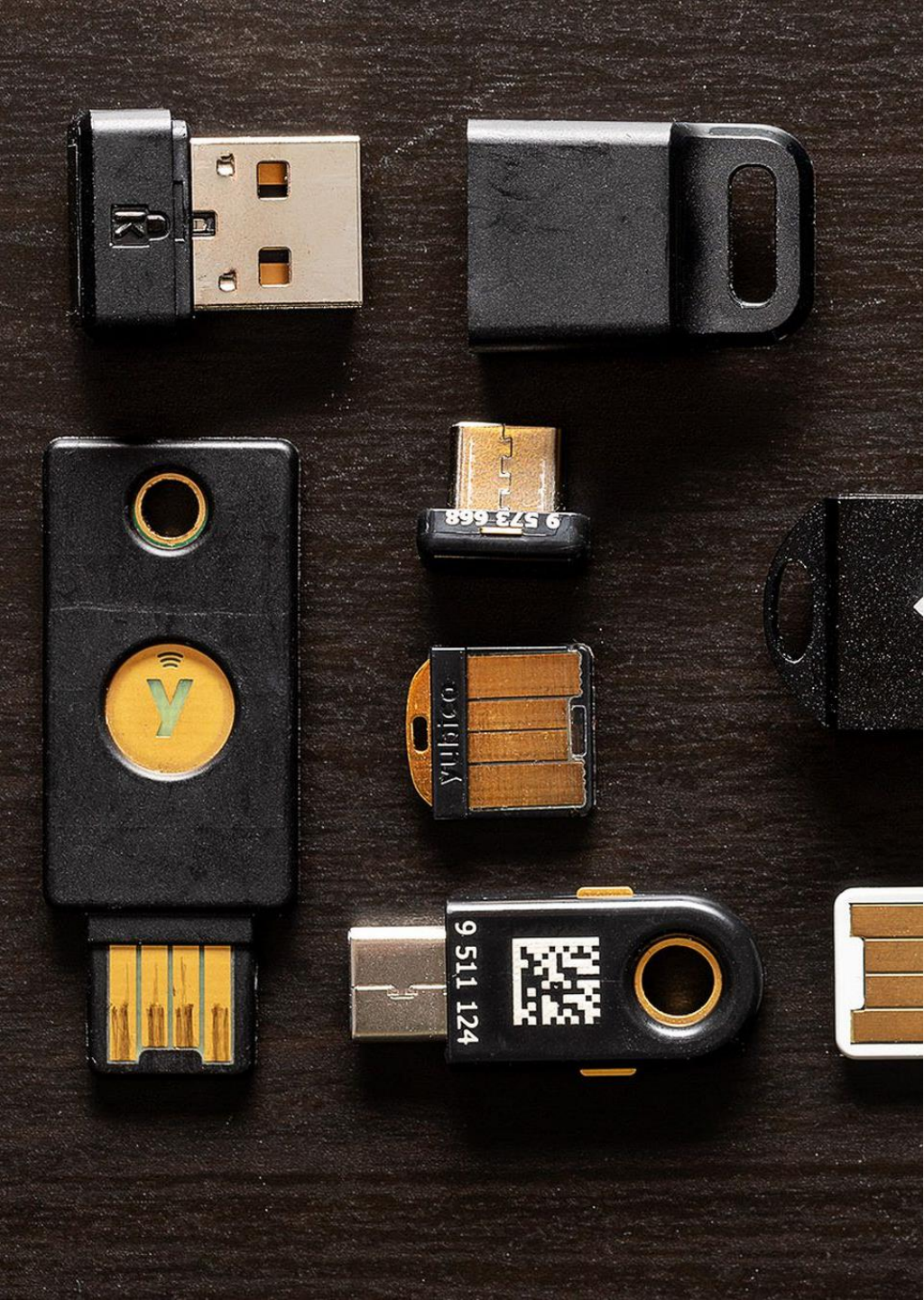
**3** – Enter the PIN code that you defined for this browser

**4** – Click on « Connect »



The screenshot shows a login interface with the following elements:

- Header: "Login"
- Redacted user information: A black bar obscuring the user's name and email.
- Settings icon: A gear icon with a dropdown arrow.
- Connect as: A dropdown menu with a redacted selection.
- Input field: A text box labeled "Enter PIN code" with a red arrow pointing to it from step 3.
- Link: A link labeled "I forgot my PIN code".
- Connect button: A button labeled "Connect" with a red arrow pointing to it from step 4.
- Footer: "Helium - © 2025 inWebo Technologies"
- Change Login button: A button labeled "CHANGE LOGIN".
- Bottom footer: "Memoryty - © 2015-2025 Memoryty. All Rights Reserved."



# Hardware Security key

## Enrollment & login

---

# Hardware Security Key - Enrollment

## Enroll Secure Key

1. Go to « My Account » > « Security »
2. Click on « **Secure Key** »

The screenshot displays the SAFRAN user interface. The top navigation bar includes the SAFRAN logo, a 'History' dropdown, a notification bell, a user profile icon, and the initials 'JD'. The main content area is titled 'My Account John DOE'. Below this, there is a user profile card with the initials 'JG', ID 'UD123', email 'john.doe@email.com', and first/last names 'John' and 'DOE'. The 'Security' tab is selected, showing options for 'Password' (with a 'Modify password' button) and 'I enroll my key' (with buttons for 'Windows Hello' and 'Secure Key'). The 'Secure Key' button is highlighted with a red box. A red line connects the 'Secure Key' button in the instructions to the 'Secure Key' button in the screenshot.

# Hardware Security Key - Enrollment

The screenshot shows a dialog box titled "Enroll Secure Key" with a "History" dropdown and a close button. The main content area is titled "Secure enrollment" and includes the text "This screen allows you to enroll a secure device." Below this is a section titled "Enter your enrollment key name" containing a text input field labeled "Key display name" and an "Enroll" button. A "Close" button is located at the bottom right of the dialog. Two callout boxes provide instructions: one points to the "Key display name" field, and the other points to the "Enroll" button.

Enroll Secure Key History ×

**Secure enrollment**  
This screen allows you to enroll a secure device.

Enter your enrollment key name

Key display name

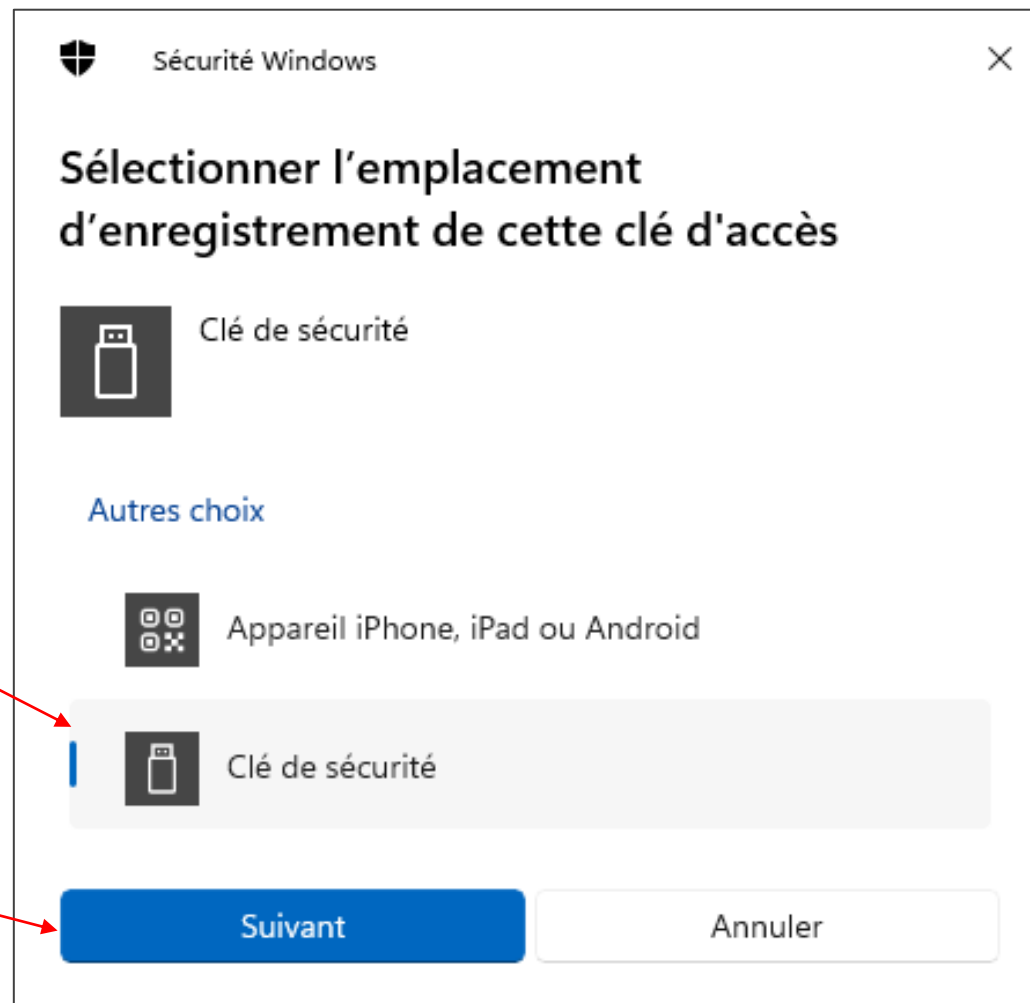
**2** – Enter the name you want for your key

**3** – Click on « Enroll »

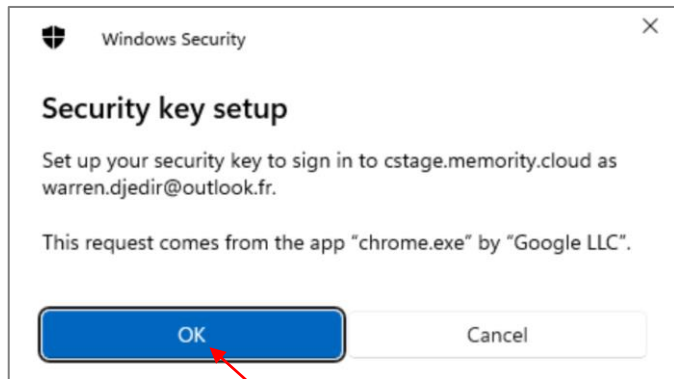
# Hardware Security Key - Enrollment

4 – Select « Security key » method

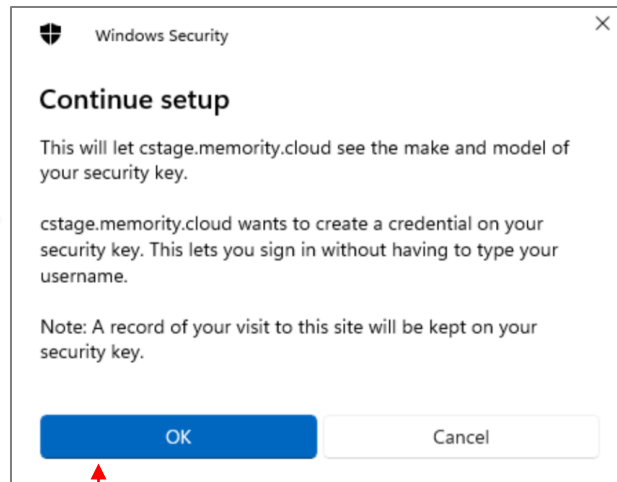
5 – Click on « Next »



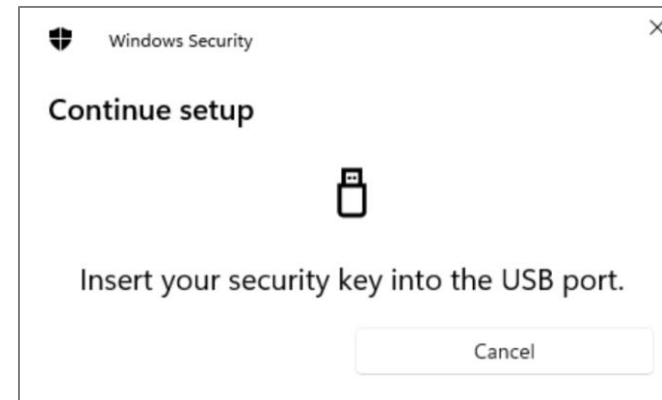
# Hardware Security Key - Enrollment



**5** - Click on « Ok » to accept

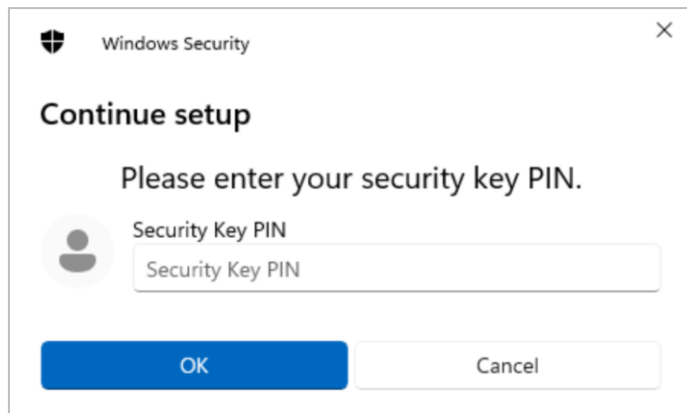


**6** - Click on « Ok » to continue



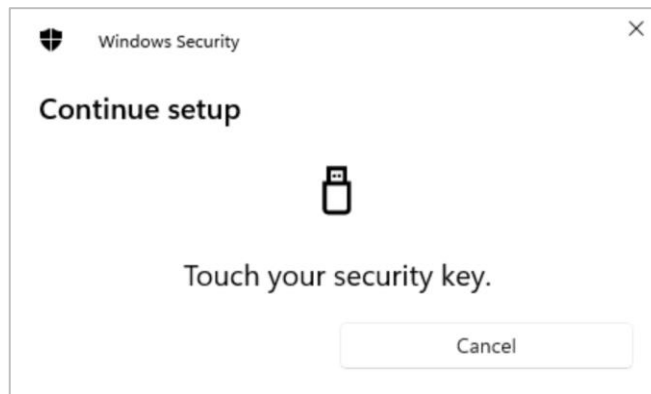
**7** - Insert your security key in your USB port

# Hardware Security Key - Enrollment

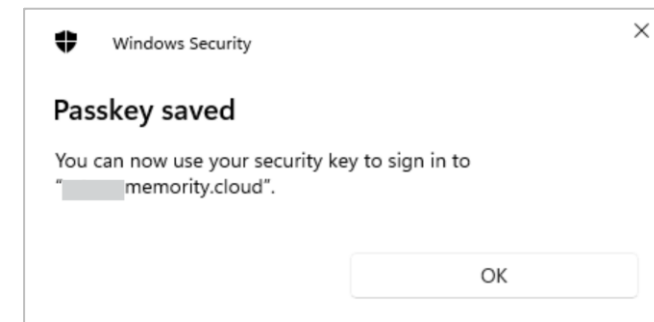


**7** – Enter the PIN of your key

**8** – Click on « Ok » to confirm

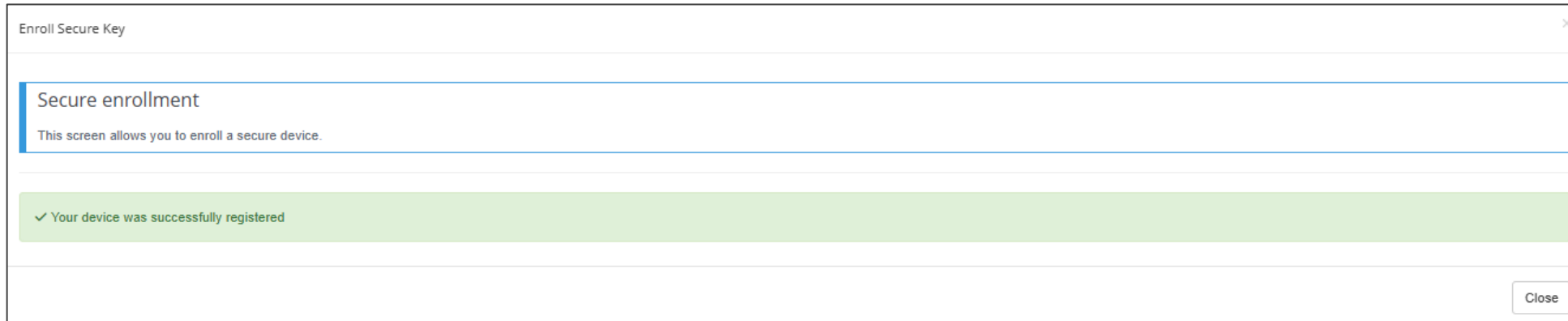


**9** – Press your security key



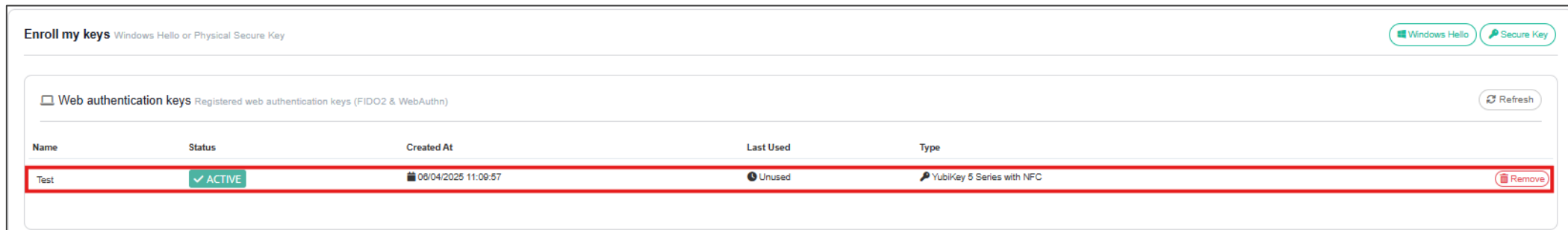
**10** – Click on « OK » to finish

# Hardware Security Key - Enrollment



## Memory Confirmation

Memory message to confirm the registration of the key



## Memory interface

The key is now visible in your interface (My Account > Security > Enroll My Keys)

# How to login with the security key

## 1 – Login page :

- Go on the **customer portal** login page
- Fill in the login field with your email address.
- Click on « Next »

Login

Enter your email

Remember me

NEXT

▶ Login issue?  
▶ Personal Data

[Terms of Service](#)

Memory - © 2015-2025 Memory. All Rights Reserved.



## 2 – Authentication methods page

Select « Secure Key »

Login

You have been redirected to this page because the application or function you tried to access needs a secured connection.

To access it chose one of the following login method :

PASSWORD + CODE RECEIVED BY EMAIL

PASSWORD + REGISTERED BROWSER

MOBILE AUTHENTICATION

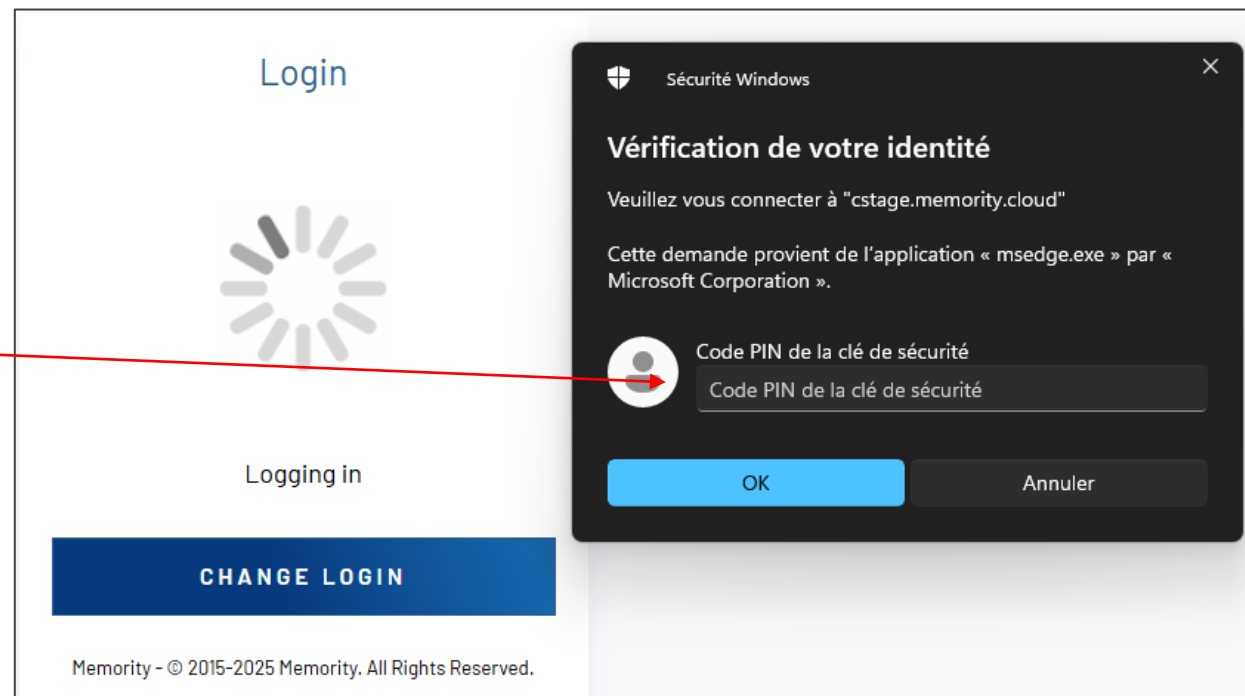
SECURE KEY

[Terms of Service](#)

Memory - © 2015-2025 Memory. All Rights Reserved.

# Hardware Security Key – How to login

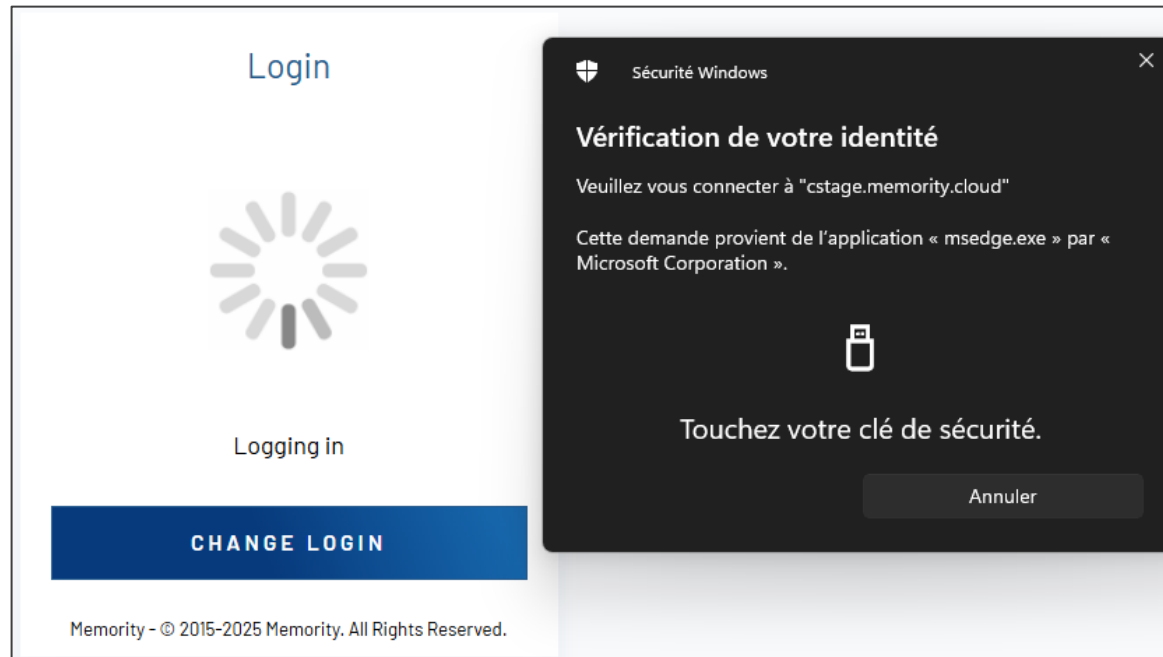
**3** – Enter the PIN of your key and click on « OK »



# Hardware Security Key – How to login

**4 – Press your key to validate**

**5 – You are logged in !**



**POWERED  
BY TRUST**

