



ESUP-OTP

# Activer les différents modes de double authentification

Afin de pouvoir accéder à certains services numériques nécessitant l'authentification double facteur, il convient de paramétrer l'application ESUP-OTP

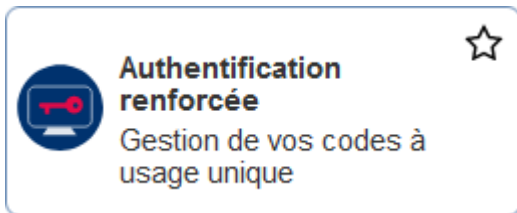


## SOMMAIRE

<b>Méthode 1 : <u>Notification (Esup Auth)</u></b>	<b>p. 4</b>
<b>Méthode 2 : <u>Code Temporel (TOTP)</u></b>	<b>p. 12</b>
<b>Méthode 3 : <u>Code par SMS (seulement pour les personnels de l'université)</u></b>	<b>p. 15</b>
<b>Méthode 4 : <u>Facteur physique (WebAuthn) pour appareil Android</u></b>	<b>p. 21</b>
<b><u>Facteur physique (WebAuthn) pour appareil iOS</u></b>	<b>p. 26</b>
<b><u>Facteur physique (WebAuthn) pour appareil Windows</u></b>	<b>p. 30</b>
<b><u>Facteur physique (WebAuthn) pour appareil Mac OS</u></b>	<b>p. 33</b>
<b>Méthode 5 : <u>Grille de codes (Grille imprimée par l'assistance de la DSIUN)</u></b>	<b>p. 36</b>



# L'application « Authentification renforcée »




Accueil

## ESUP OTP Manager

Vous permet d'ajouter un deuxième niveau de protection à votre compte (authentification double facteur). Ainsi, il sera impossible d'accéder à votre compte même avec votre mot de passe.

Dans vos préférences, nous vous conseillons fortement de paramétrer au moins 2 méthodes afin de pouvoir assurer la continuité d'utilisation des services numériques.

Vous pouvez définir :

-  qu'une notification / push soit envoyée sur l'application Esup Auth (Android, iOS bientôt).
-  qu'un code (TOTP) soit généré dans une application (Esup Auth, Authenticator, Plugin OTP..).
-  qu'un code à usage unique vous soit envoyé par SMS.



UNIVERSITÉ PARIS  
PANTHÉON SORBONNE

🏠 | Mentions légales | Contacts | Aide

1

Depuis l'ENT, rendez-vous sur l'application « **Authentification renforcée** »

2

Vous êtes dirigé vers la **page d'authentification renforcée** de Paris 1 « **ESUP OTP Manager** »

Cette page vous permet de renseigner les informations nécessaires à la double authentification

# 1<sup>ère</sup> Méthode

**NOTIFICATION (ESUP AUTH)**



# Activation de la méthode notification / Push dans l'ENT



ENT | Authentification renforcée

Accueil

Préférences

Notification (Esup Auth)

Code temporel (TOTP)

Code par SMS

Manager

Préférences

Notification (Esup Auth)

Désactiver  Activer

Méthode permettant de se connecter via les notifications c

**1**

Sélectionnez le menu « **Notification / Esup Auth** », puis cliquez sur le bouton « **Activer** »

**2**

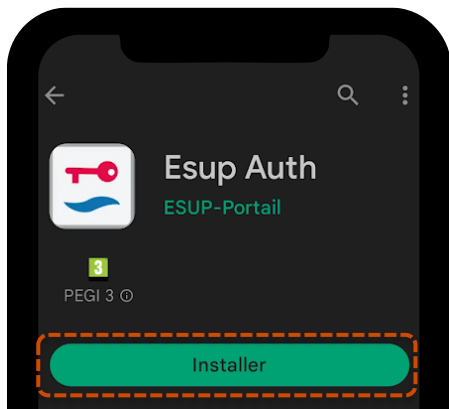
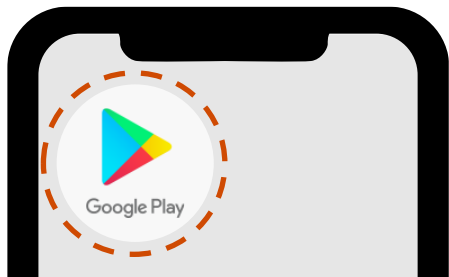
Un **Code QR** est généré et doit être scanné à l'aide de l'application « **Esup Auth** »



*Il est impératif d'avoir téléchargé au préalable l'application « Esup Auth » sur son Smartphone*



## Installation de l'application Esup Auth sur le Smartphone (Android)

**1**

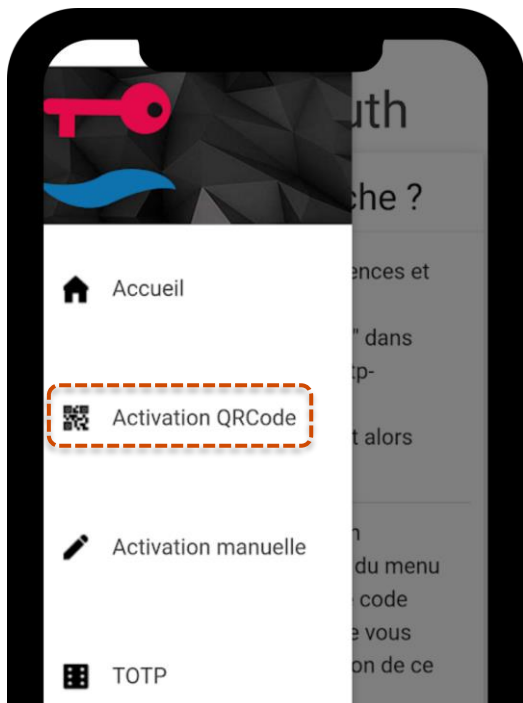
Depuis votre **smartphone**, rendez-vous sur le **Google Play Store** et saisissez « **Esup Auth** » dans la barre de recherche ou scanner le QrCode suivant :

**2**

Sélectionnez l'application « **Esup Auth** » puis appuyez sur « **Installer** »



# Activation de la méthode notification Esup Auth sur Smartphone

**1**

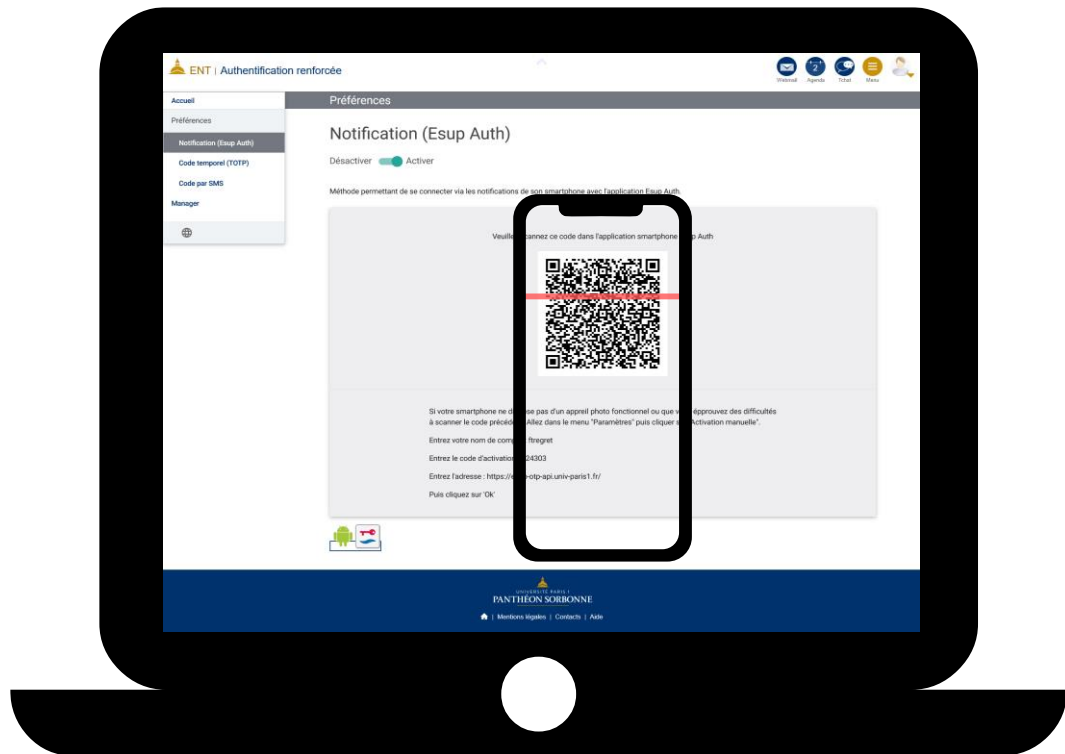
Sur votre Smartphone, depuis l'application « **Esup Auth** », sélectionnez « **Activation** » afin de procéder au scan du Code QR présent dans « **Authentification renforcée** » dans l'ENT



*Notez qu'il est possible de procéder sans scan en renseignant les informations présentes sur la page « Notifications / Esup Auth » dans l'application « Authentification renforcée »*



# Activation de la méthode notification Esup Auth sur Smartphone



2

Depuis votre **smartphone**, scannez le Code QR affiché sur la page « **Notification / Esup Auth** » que vous avez activé sur l'ENT précédemment

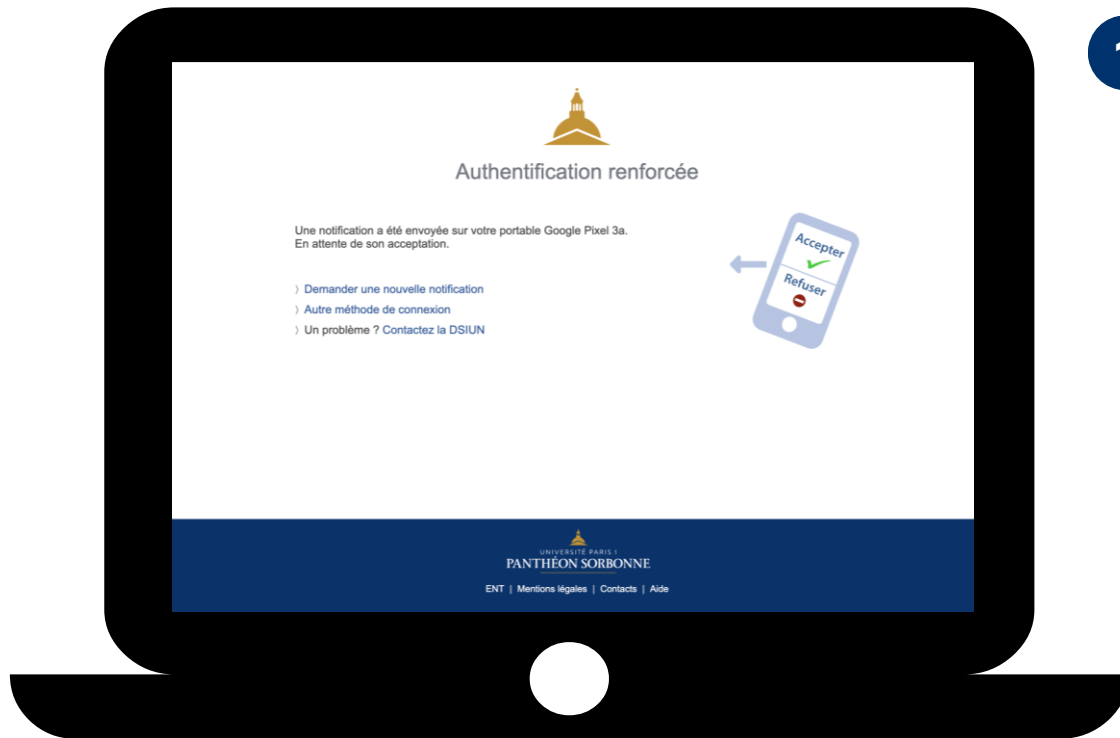


*Cette étape n'est à réaliser qu'une seule fois.*





# Se connecter avec la notification Esup Auth

**1**

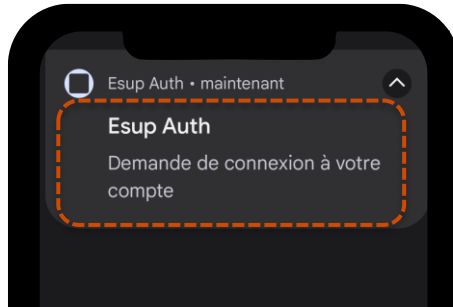
Désormais pour accéder à des services nécessitant la double authentification, vous voyez cette page lors de l'accès à ce service

Pour y accéder, il suffit **d'accepter la connexion depuis votre Smartphone**



## Se connecter avec la notification / Esup Auth

2



Pensez à activer les notifications sur votre **Smartphone** afin de recevoir les **notifications Esup Auth** vous demandant de valider la connexion

3



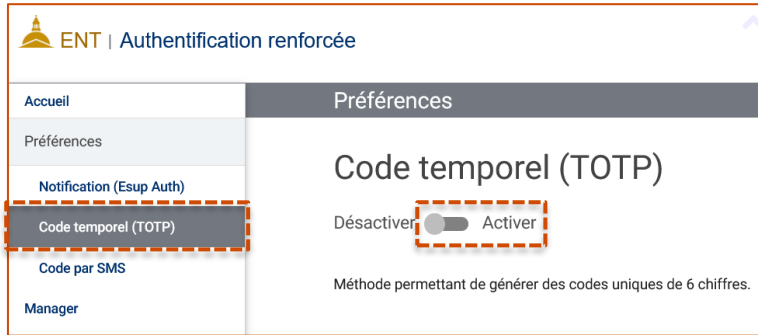
Si vous êtes à l'origine de la demande de connexion, sélectionnez « **Accepter** » pour accéder au service, sinon refusez

# 2<sup>ème</sup> Méthode

**CODE TEMPOREL (TOTP)**



# Activation de la méthode code Temporel (TOTP) (1)

**1**

Sélectionnez le menu « **Code Temporel (TOTP)** », puis cliquez sur le bouton « **Activer** ».

**2**

Une fois activé, il est demandé de **scanner un Code QR** (une seule fois) à l'aide d'une **application TOTP** (Esup Auth, FreeOTP, Google Authenticator, Microsoft Authenticator, ...).

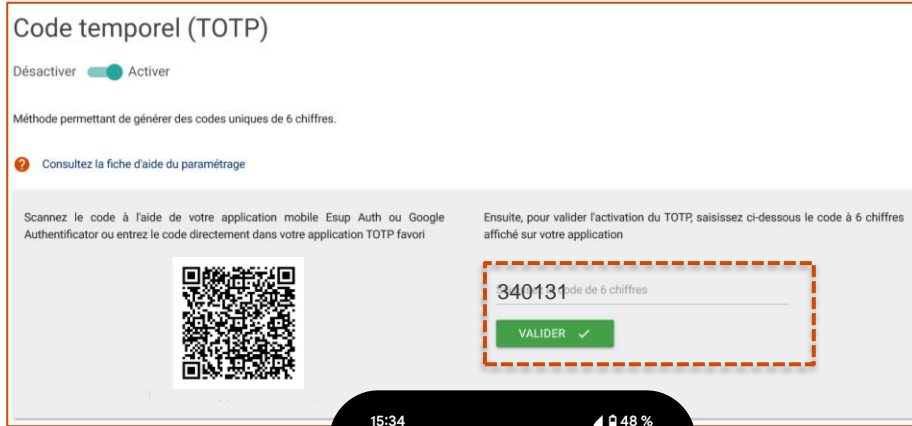
Sur votre Smartphone, appuyez sur « **TOTP** » puis sur « **Scan** » afin de créer l'association.



Exemple réalisé avec l'application Esup Auth

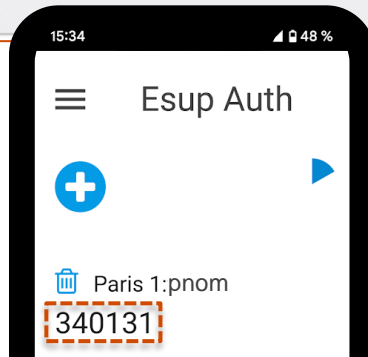


# Activation de la méthode code Temporel (TOTP) (2)



1

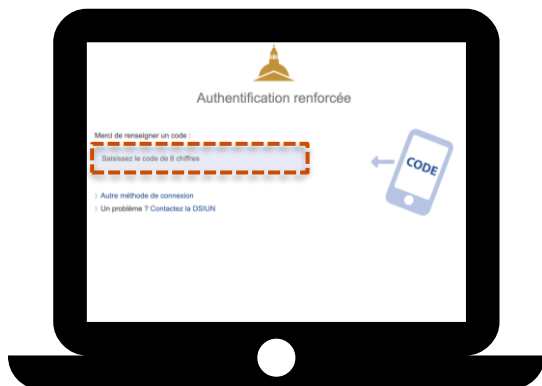
Une fois le **QrCode validé** avec votre Smartphone et afin de terminer l'association il sera nécessaire de **saisir le code à 6 chiffres** affiché sur **l'application TOTP** puis de cliquer sur le bouton « **Valider** ».





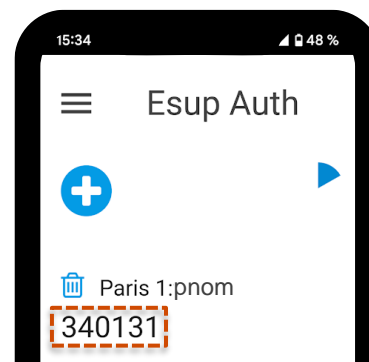
## Se connecter avec le code temporel (TOTP)

1



A votre prochaine connexion nécessitant la double authentification, il vous est demandé de **renseigner le code à 6 chiffres** généré dans votre **application de double authentification sur votre smartphone**

2



Rendez-vous dans  **votre application de double authentification**  et saisissez sur l'ordinateur le **code à 6 chiffres**



*Les 6 chiffres sont renouvelés toutes les 30 secs*

# 3<sup>ème</sup> Méthode

## CODE PAR SMS

(seulement pour les personnels de l'université)



# Activation de la méthode Code par SMS

ENT | Authentification renforcée



1

Sélectionnez le menu « **Code par SMS** », puis cliquez sur le bouton « **Activer** ».

## Code par SMS

Désactiver  Activer

Méthode permettant de s'authentifier à partir d'un code aléatoire à usage unique envoyé par SMS.

2

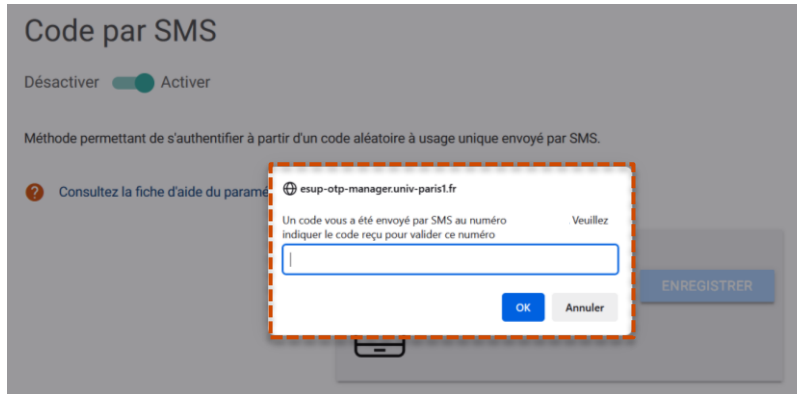
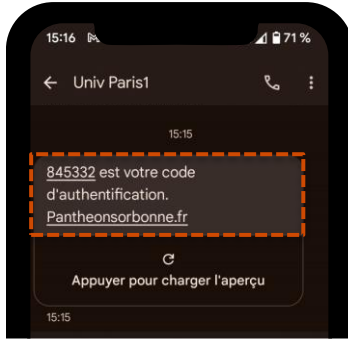
Saisissez le **numéro de téléphone** sur lequel seront envoyés les codes par SMS, puis cliquez sur le bouton « **Enregistrer** ».







## Activation de la méthode Code par SMS (2)



1

Vous allez recevoir **sur votre Smartphone** un **code à 6 chiffres** par SMS.

2

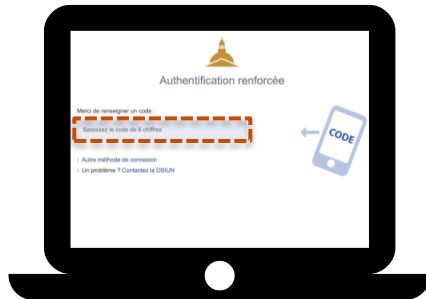
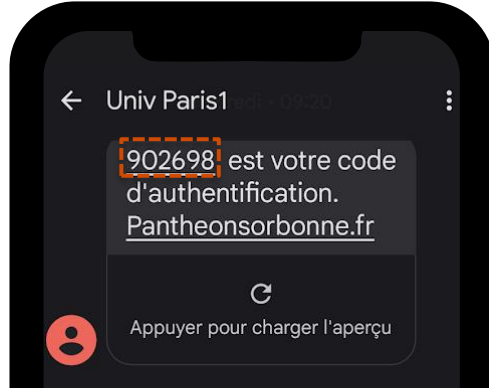
Renseignez ce **code** dans la fenêtre apparue sur votre ordinateur puis **cliquez** sur « **OK** ».



*Etape à ne réaliser qu'une seule fois*



## Se connecter avec le Code par SMS

**2**

A votre prochaine connexion nécessitant la double authentification, il vous sera demandé de **renseigner le code à 6 chiffres envoyé par SMS**

**3**

Vous devrez **renseigner ces 6 chiffres** dans la fenêtre ouverte sur votre ordinateur

# 4<sup>ème</sup> Méthode

**Facteur physique (WebAuthn)**



## Qu'est-ce que l'authentification WebAuthn ?



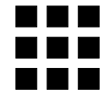
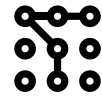
Windows



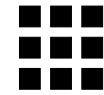
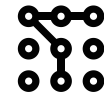
Mac Os



Android



iOS



L'authentification **WebAuthn** s'appuie sur les **dispositifs de déverrouillage intégrés aux ordinateurs, smartphones et tablettes** (reconnaissance faciale, digitale, code PIN, modèle, clé de sécurité USB/NFC,...).

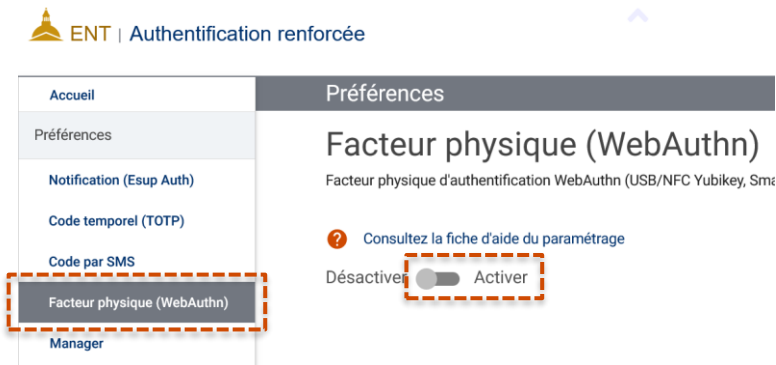
Elle se veut une option d'authentification uniforme qui ne repose plus sur des mots de passe mais sur des **authentifiants associés au matériel de l'utilisateur**.

# 4ème Méthode

**Facteur physique (WebAuthn)  
Configurer un appareil Android**



# Configurer un appareil Android (1)

**1**

Depuis l'application « **Authentification renforcée** », sélectionnez le menu « **Facteur physique** », puis cliquez sur le bouton « **Activer** ».

**2**

Une fenêtre va s'ouvrir vous demandant de **sélectionner l'emplacement d'enregistrement de la clé d'accès**.



Choisissez, « **Appareil iPhone, iPad ou Android** » un des emplacements puis cliquez sur « **Suivant** ».



## Configurer un appareil Android (2)

**3**

Un **QrCode** va s'afficher sur l'écran de l'**ordinateur**.

Vous devrez le **scanner avec votre téléphone** (application photo) afin de créer l'association pour la clé d'accès.

**4**

Sur votre **téléphone**, un message va vous demander de **créer une clé d'accès** pour univ-paris1.fr.

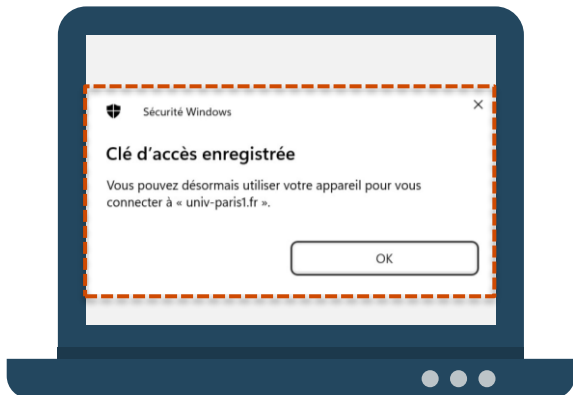
Cliquez sur « **Continuer** ».



*Afin que l'association puisse se faire il convient que le **Bluetooth** ou le **NFC** soient activés sur le Smartphone.*



## Configurer un appareil Android (3)

**5**

Afin de valider la demande vous devrez **déverrouiller votre SmartPhone** avec une des méthodes que vous avez enregistré sur votre appareil (**empreinte digitale, code pin,...**)

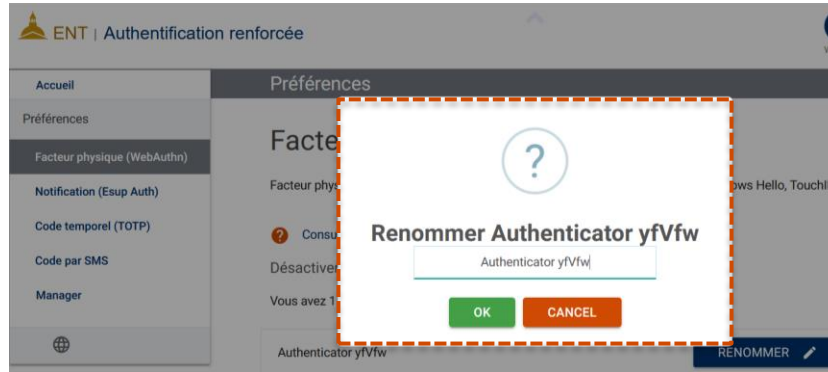
**6**

Sur votre ordinateur, un message confirmant l'**enregistrement de la clé d'accès** s'affichera et confirmera l'association.





## Configurer un appareil Android (4)

**7**

Vous pouvez ensuite **renommer l'appareil** afin de mieux l'identifier par la suite.

Une fois renommé, **il apparaît dans la liste** des facteurs physiques d'authentification disponibles.

### Facteur physique (WebAuthn)

Facteur physique d'authentification WebAuthn (USB/NFC Yubikey, Smartphone, Windows Hello, TouchID, ...).

Consultez la [fiche d'aide du paramétrage](#)

Désactiver  Activer

Vous avez 1 moyen d'authentification.

AJOUTER +



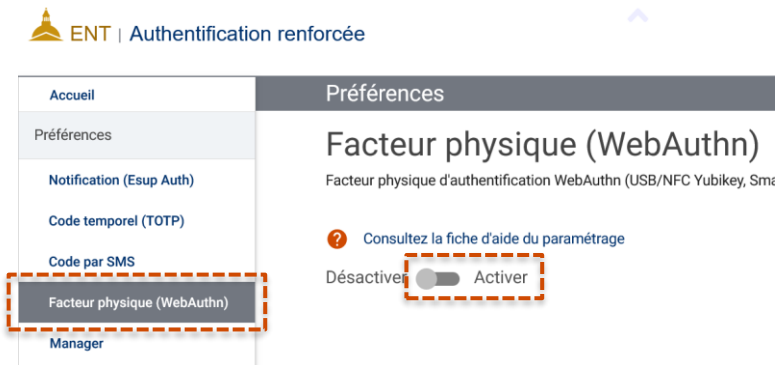
Dès lors d'une prochaine connexion demandant la double authentification, **si votre téléphone et votre ordinateur ont le Bluetooth ou le NFC d'activés et sont à proximité**, vous serez automatiquement authentifiés.

# 4ème Méthode

**Facteur physique (WebAuthn)  
Configurer un appareil iOS**



# Configurer un appareil iOS (1)

**1**

Depuis l'application « **Authentification renforcée** », sélectionnez le menu « **Facteur physique** », puis cliquez sur le bouton « **Activer** ».

**2**

Une fenêtre va s'ouvrir vous demandant de **sélectionner l'emplacement d'enregistrement de la clé d'accès**.



Choisissez, « **Appareil iPhone, iPad ou Android** » un des emplacements puis cliquez sur « **Suivant** ».



## Configurer un appareil iOS (2)

**3**

Un **QRCode** va s'afficher sur l'écran de l'**ordinateur**.

Vous devrez le **scanner avec votre téléphone** (application photo) afin de créer l'association pour la clé d'accès.

**4**

Sur votre **téléphone**, un message va vous demander d'enregistrer la clé.

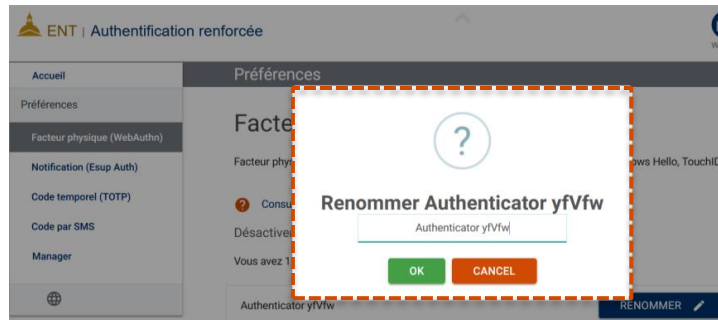
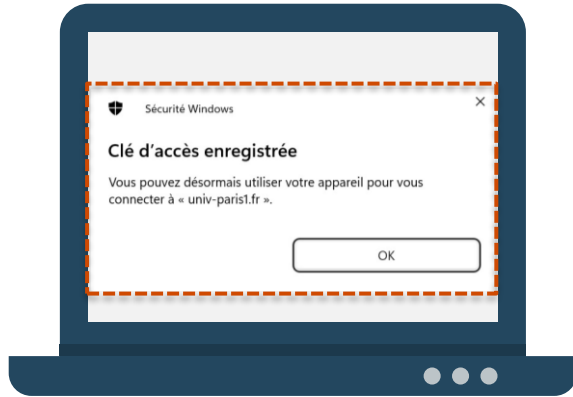
Afin de valider la demande vous devrez **déverrouiller votre appareil** (TouchID / FaceID).



*Afin que l'association puisse se faire il convient que le **Bluetooth** ou le **NFC** soient activés sur le Smartphone.*



## Configurer un appareil iOS (3)

**5**

Un fois le **QrCode** scanné avec  **votre téléphone**  un message confirmant l'**enregistrement de la clé d'accès** s'affichera.

**6**

Vous pouvez ensuite **renommer l'appareil** afin de mieux l'identifier par la suite.

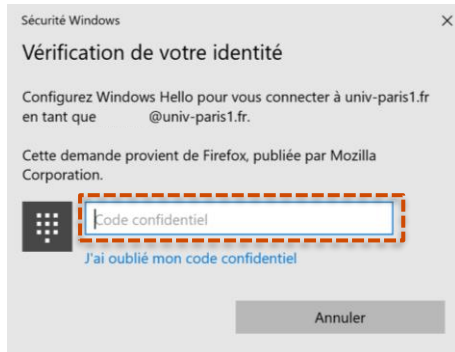
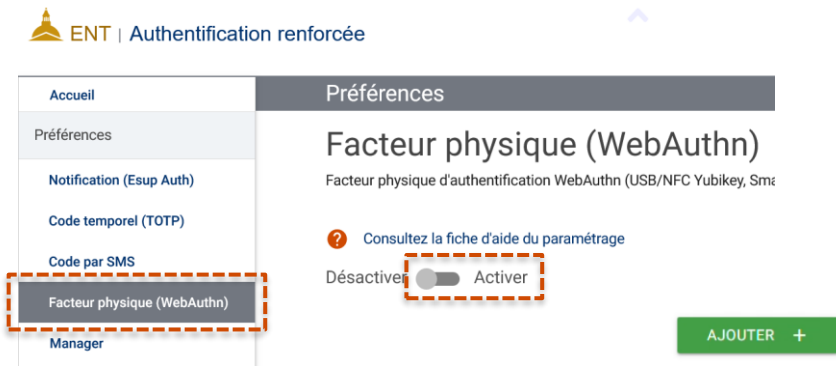
Une fois renommé, **il apparait dans la liste** des facteurs physiques d'authentification disponibles.

# 4ème Méthode

**Facteur physique (WebAuthn)  
Configurer un appareil personnel  
Windows**



# Configurer un appareil personnel Windows (1)

**1**

Depuis l'application « **Authentification renforcée** », sélectionnez le menu « **Facteur physique** », puis cliquez sur le bouton « **Activer** » et le bouton « **Ajouter** ».

**2**

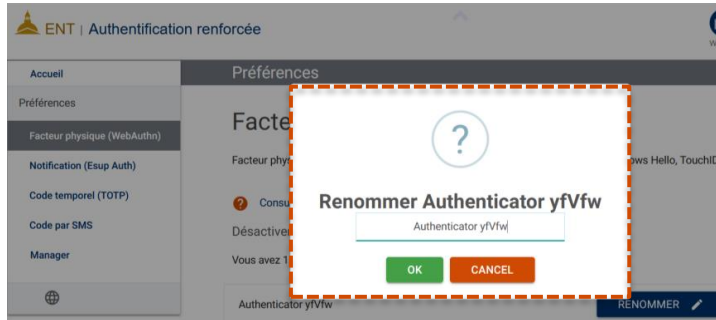
Une fenêtre va s'ouvrir vous demandant d'effectuer **votre méthode de déverrouillage Windows Hello** (reconnaissance faciale, empreinte, code PIN,...).



*Suivant votre ordinateur et votre configuration de Windows Hello, toutes les options de déverrouillage ne sont pas disponibles*



## Configurer un appareil personnel Windows (2)

**3**

Vous serez invité à **renommer l'appareil** afin de mieux l'identifier par la suite.

**4**

Une fois renommé, **il apparaît dans la liste** des facteurs physiques d'authentification disponibles.



# 4ème Méthode

Facteur physique (WebAuthn)  
Configurer un appareil personnel  
Mac OS



# Configurer un appareil personnel mac OS (1)

The screenshot shows the ESUP-OTP application interface. At the top, it says "ENT | Authentification renforcée". The main menu on the left includes "Accueil", "Préférences", "Notification (Esup Auth)", "Code temporel (TOTP)", "Code par SMS", and "Facteur physique (WebAuthn)", which is highlighted with a dashed orange box. The "Préférences" section is titled "Facteur physique (WebAuthn)" and includes a toggle switch for "Désactiver" and "Activer", with the "Activer" option selected and highlighted with a dashed orange box. A green "AJOUTER +" button is visible. Below this, there are two screens for creating a key. The first screen is titled "Créer une clé d'accès pour univ-paris1.fr" and shows the email address "@univ-paris1.fr" and a "Continuer" button highlighted with a dashed orange box. The second screen is titled "Créer une clé d'accès" and offers three options: "Trousseau iCloud", "Utiliser un téléphone, une tablette ou une clé de...", and "Votre profil Chrome". The "Trousseau iCloud" option is highlighted with a dashed orange box. An "Annuler" button is at the bottom.

1

Depuis l'application « **Authentification renforcée** », sélectionnez le menu « **Facteur physique** », puis cliquez sur le bouton « **Activer** » et le bouton « **Ajouter** ».

2

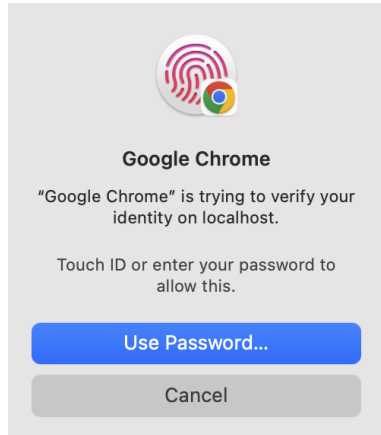
Une fenêtre va vous demander de **créer une clé d'accès**. Cliquez sur « **Continuer** ».

Une seconde fenêtre va vous demander **sur quel matériel créer la clé**.

Sélectionnez « **Trousseau iCloud** » ou votre **profil de navigateur internet** (Firefox, Chrome, Safari,...).



## Configurer un appareil personnel mac OS (2)

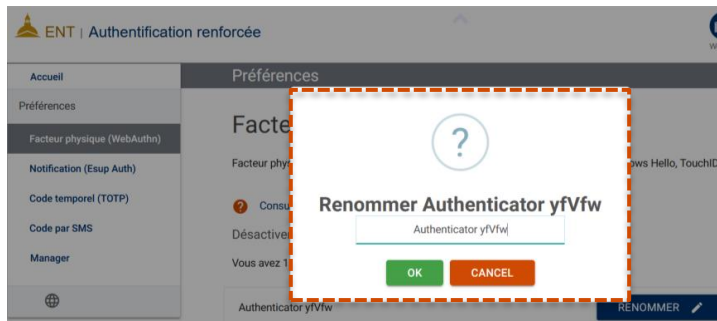
**3**

Afin de finaliser la création, votre **méthode de déverrouillage de votre Mac** (TouchID, FaceID, Code PIN...) vous sera demandé.

**4**

Vous serez invité à **renommer l'appareil** afin de mieux l'identifier par la suite.

Une fois renommé, **il apparait dans la liste** des facteurs physiques d'authentification disponibles.



# 5ème Méthode

## GRILLE DE CODES

(Grille imprimée par l'assistance de la DSIUN)



# Récupération de la Grille de codes à la DSIUN

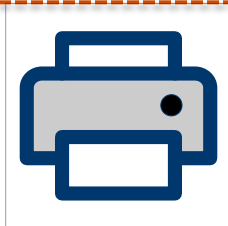
Grille de codes

Méthode permettant de générer une grille de codes aléatoires.

Consultez la fiche d'aide du paramétrage

Désactiver  Activer

	1	2	3	4	5	6	7	8
A	673027	629819	443377	605826	943775	422784	874008	209718
B	430424	705432	817314	247258	065874	470691	575107	816992
C	590079	807250	401829	038637	845428	324332	117957	447900
D	850659	535299	353453	354648	984741	123393	176818	704105
E	140853	090241	469997	505345	805080	150481	201880	236787
F	105800	589836	990201	445715	454689	800374	463520	026463
G	432447	697082	717166	381857	022267	621886	232950	957433
H	717466	885129	781079	546609	175447	954656	613061	535428

**1**

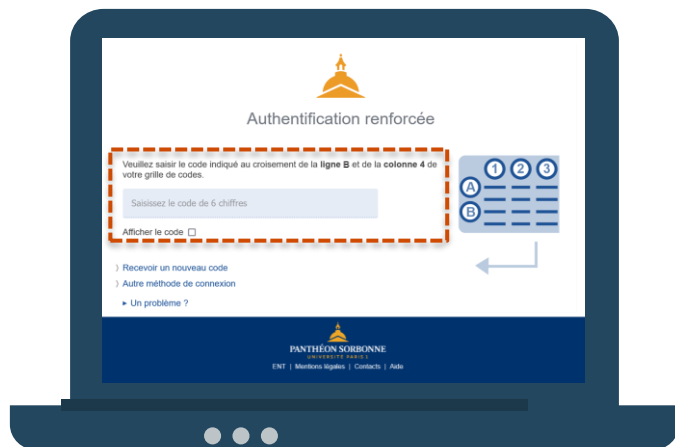
Si vous ne pouvez pas utiliser les autres méthodes, vous pouvez vous rendre à la DSIUN afin de faire imprimer une grille de codes pour votre compte.

**2**

Cette grille de code vous sera remise et vous permettra ensuite de vous connecter aux applications nécessitant l'authentification double facteur.



## Utilisation de la méthode Grille de codes



3

Dès lors, lorsque vous accéderez à une application nécessitant la double authentification, vous serez invité à **saisir le code à 6 chiffre correspondant à l'intersection ligne / colonne** de votre grille de codes.

	1	2	3	4	5	6
A	673027	629819	443377	605826	943775	4227
B	430424	705432	817314	247258	065874	4706
C	590079	807250	401829	038637	845428	3243
D	850659	535299	353453	354648	984741	1233
E	140853	090741	469997	505345	805080	1504



*Dans l'exemple ci-contre, le code demandé à l'intersection de la ligne B et de la colonne 4 correspond au code 247258*



Consultez aussi le **Guide des services numériques** de Paris 1 :

Version étudiants : [ent.univ-paris1.fr/gun](https://ent.univ-paris1.fr/gun)

Version personnels : [ent.univ-paris1.fr/gun-pers](https://ent.univ-paris1.fr/gun-pers)

Contact DSIUN pour toutes informations complémentaires :

Tél. : +33 (0) 1 89 68 55 55 | Courriel : [assistance-dsiun@univ-paris1.fr](mailto:assistance-dsiun@univ-paris1.fr)