GUIDE DE LA DOUBLE AUTHENTIFICATION

Activer les différentes méthodes de double authentification avec ESUP-OTP

Université de Picardie Jules Verne
Direction des Systèmes d'Information
(DiSI)

Préambule

Qu’est-ce que la double authentification avec ESUP-OTP ?

La double authentification, également appelée authentification à deux facteurs (2FA), est un mécanisme de sécurité qui ajoute **une couche supplémentaire de protection** à l’accès à un compte ou à un système.

Avec ESUP-OTP, la double authentification implique **l’utilisation de deux éléments** pour vérifier l’identité d’un utilisateur. Le premier élément est généralement quelque chose que l’utilisateur connait, comme un mot de passe. Le deuxième élément **est généré dynamiquement**, souvent par une application mobile ou un dispositif physique comme un token, et change à chaque tentative d’authentification. Cette combinaison rend plus difficile pour une personne non autorisée d’accéder au compte, même si le mot de passe est compromis.

Ainsi, la double authentification avec ESUP-OTP utilise un **système de génération de codes à usage unique** (OTP : One Time Password) pour renforcer la sécurité de l’authentification.

Dans notre cas l’UPJV met en place cette solution pour l’ensemble de ses agents. Nous allons voir, à travers ce guide, comment configurer ESUP-OTP pour **activer une ou plusieurs méthodes** de génération de code à usage unique (OTP). L’UPJV **vous recommande d’activer ou moins deux méthodes** (en cas de perte de votre portable, vol, etc…).

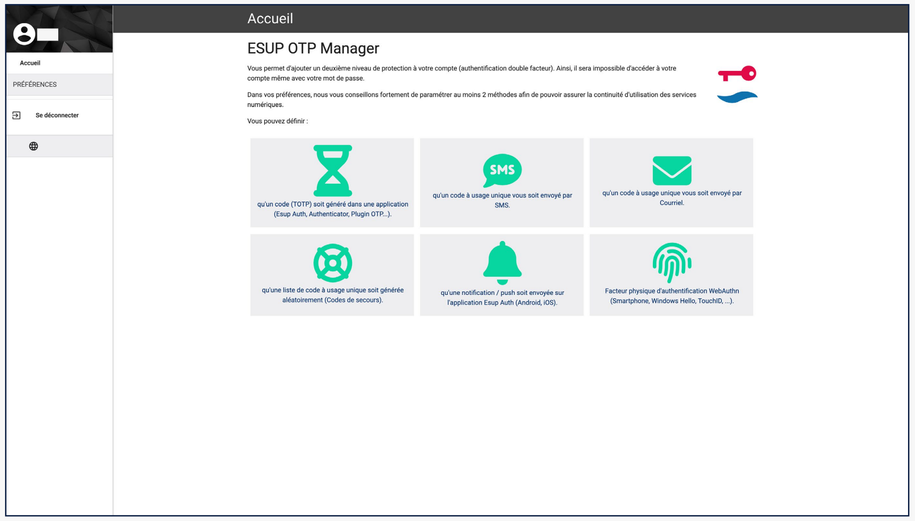
Il est **nécessaire de configurer la méthode de génération du code OTP** afin d’activer la double authentification sur votre compte. Vous avez **la possibilité de modifier ce paramétrage** à tout moment depuis l’interface ESUP-OTP.

Veuillez noter que la double authentification ne **sera requise qu’une seule fois tous les sept jours.** Ainsi, chaque semaine, en plus de votre mot de passe UPJV, vous devrez saisir le code à usage unique généré à l’aide de l’une des méthodes que nous allons détailler ci-après.

L’application « Authentification renforcée »

1. Accédez au service : depuis votre ENT, rendez-vous dans le bloc « Préférences » et cliquez sur « **Authentification renforcée** », ou accédez directement via ce lien : https://otp-manager.u-picardie.fr/preferences. Dans les deux cas, vous devez être **connecté au réseau de l’UPJV pour y accéder** (pensez à activer votre VPN si vous êtes en dehors du réseaux WiFi ou filaire). Si ce n’est pas le cas, veuillez contacter l’assistance téléphonique au 03.22.82.59.29.

2. Vous êtes à présent sur la page d’authentification renforcée de l’UPJV, appelée « ESUP-OTP Manager ». Cette page vous permet de fournir **les informations nécessaires pour la double authentification et de configurer les différentes méthodes.**



Méthode N°1
Code temporel (TOTP)

Recommandée par la DiSI

La méthode « Code temporel (TOTP) »

Recommandée par la DiSI

Qu’est-ce que la méthode « Code temporel (TOTP) ? »

La méthode « Code temporel » fait référence à l’algorithme d’authentification à deux facteurs appelé TOTP, qui signifie «Time-Based One-Time Password» **(Mot de passe à usage unique basé sur le temps)**.

Avec la méthode TOTP, un utilisateur **génère des codes à usage unique** en utilisant une clé secrète partagée entre le service (la page web de connexion) et l’application d’authentification de l’utilisateur (l’application mobile). Ces codes changent à intervalles réguliers, généralement **toutes les 30 secondes**, en fonction du temps actuel.

L’utilisateur doit fournir **ce code TOTP en plus de son mot de passe lors de la connexion**. Cette approche ajoute une couche de sécurité supplémentaire en s’assurant que le code à usage unique est valide seulement pendant une courte période, renforçant ainsi la protection de l’accès au compte.

La méthode « Code temporel (TOTP) »

Recommandée par la DiSI

Activer la méthode « Code temporel (TOTP) »

1 Avant toute chose, sur votre smartphone, vous devez **télécharger une des deux applications** mobile suivantes : « Scan Auth » ou « Google Authenticator ».

App Store

Scan Auth

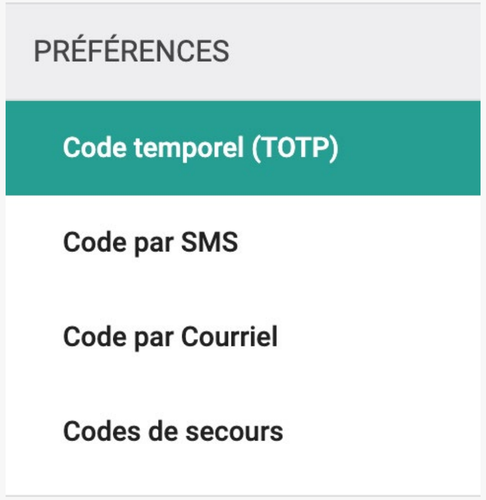
Google Authenticator

Google Play

Scan Auth

Google Authenticator

2 Rendez-vous maintenant sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Code temporel (TOTP) ». Basculez ensuite le sélecteur sur « Activer ».



3 Après activation, cliquez sur « GÉNÉRER QRCODE ». Un code QR sera créé et devra être **scanné une seule fois** à l'aide de l'application que vous avez installée lors de l'étape numéro 1.

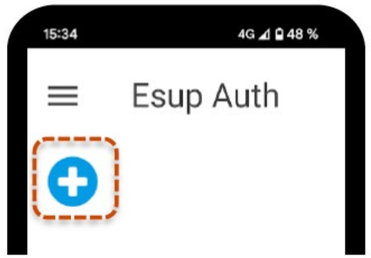
La méthode « Code temporel (TOTP) »

Recommandée par la DiSI

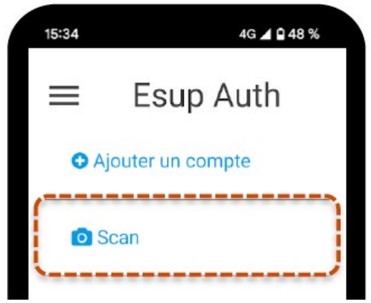
Activer la méthode « Code temporel » (TOTP)

4 Depuis votre smartphone, appuyer sur le « + » puis sur le bouton « Scan » afin de scanner le Code QR affiché sur la page « Code temporel (TOTP) » que vous avez activé sur l'ENT précédemment.

Cette étape n'est à réaliser q'une seule fois.

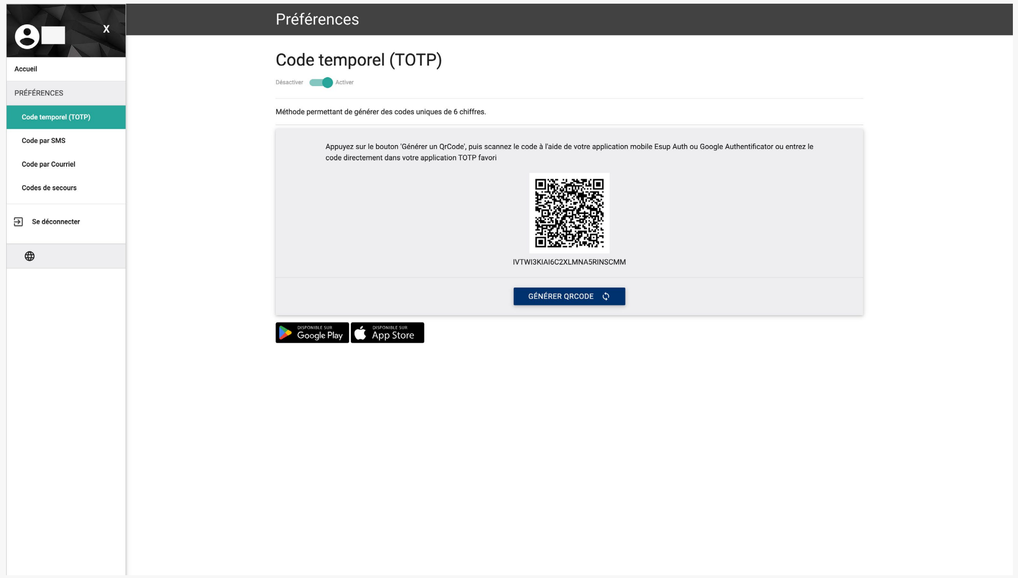


Exemple réalisé avec l'application Esup Auth



Exemple réalisé avec l'application Esup Auth

5 Depuis votre smartphone, **scannez le Code QR** affiché sur la page « Code temporel (TOTP) » que **vous avez activé sur l'ENT précédemment.**

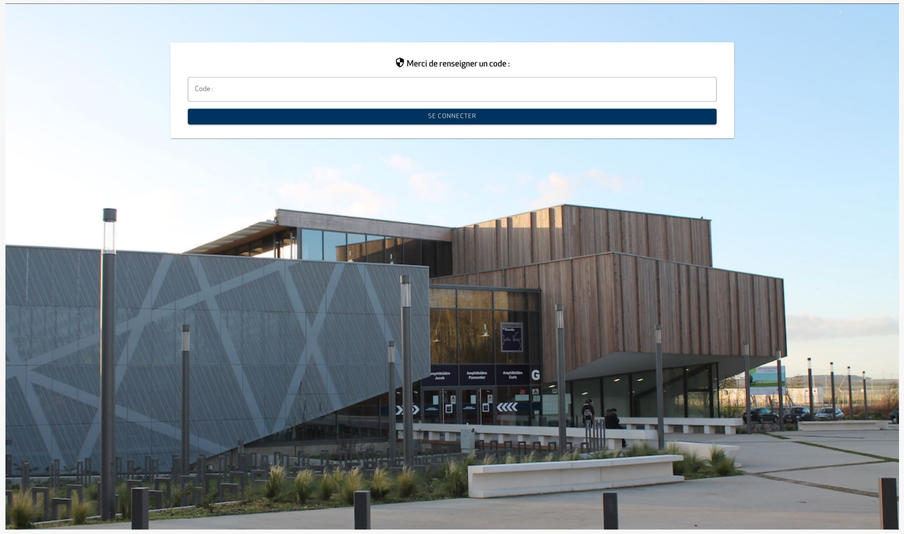


La méthode « Code temporel (TOTP) »

Recommandée par la DiSI

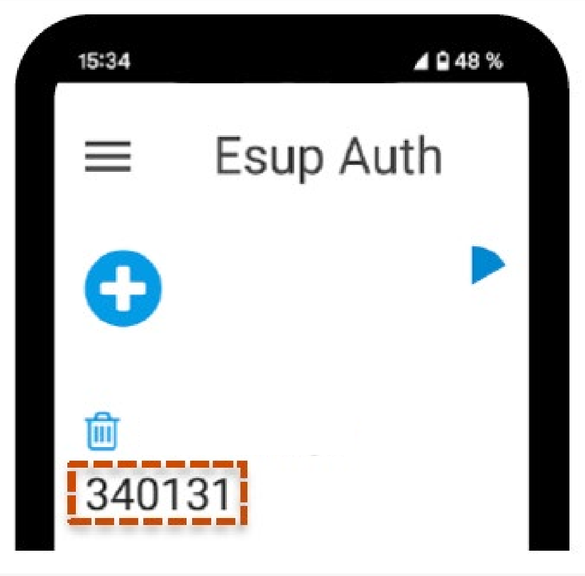
Se connecter avec la méthode « code temporel (TOTP) »

1 Lors de 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 secondes.



Méthode N°2
Code par SMS

La méthode « Code par SMS »

Qu’est-ce que la méthode « Code par SMS »

La méthode du «Code par SMS» pour la double authentification implique **l’envoi d’un SMS contenant un code à usage unique** sur le numéro mobile de l’utilisateur.

Contrairement à la méthode « Code temporel (TOTP) », le code SMS n’est pas généré toutes les trente secondes, offrant ainsi une durée de validité plus étendue. Cependant, il est important de noter que bien que le code SMS ne soit pas basé sur une période temporelle fixe, **sa validité reste généralement limitée à quelques minutes pour des raisons de sécurité.**

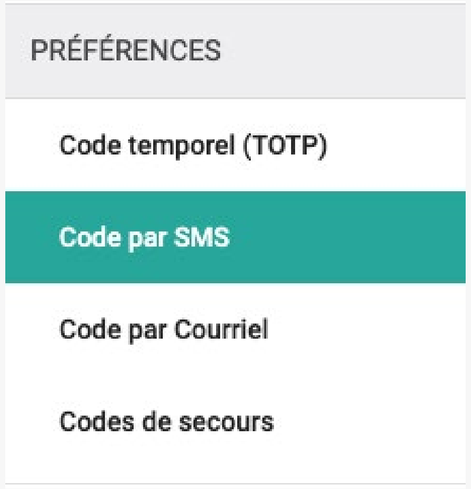
Cette approche renforce la sécurité en ajoutant un deuxième facteur au processus d’authentification, exigeant à la fois quelque chose que l’utilisateur connaît (le mot de passe) et quelque chose qu’il possède (le téléphone mobile pour recevoir le code SMS).

Bien que largement utilisée, cette méthode peut présenter des vulnérabilités potentielles, notamment **la possibilité d’interception des messages SMS**, conduisant certains services à explorer des alternatives plus sécurisées.

La méthode « Code par SMS »

Activer la méthode « Code par SMS »

1 Rendez-vous sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Code temporel par SMS ». Basculez ensuite le sélecteur sur « Activer ».



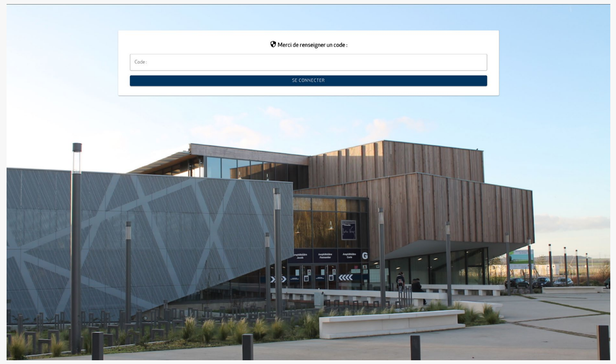
2 Saisissez le numéro de téléphone sur lequel **seront envoyés les codes par SMS**, puis cliquez sur le bouton « Enregistrer ».

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

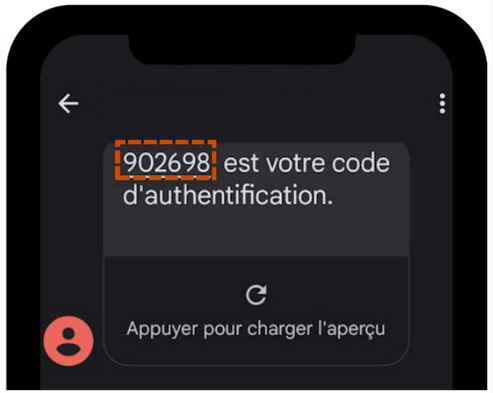
La méthode « Code par SMS »

Se connecter avec la méthode « Code par SMS »

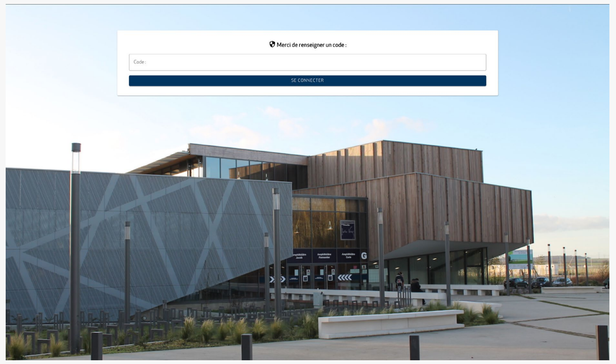
1 Lors de votre prochaine connexion nécessitant la double authentification, il vous est demandé **un code d'authentification à 6 chiffres.**



2 Lors de 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.**



Méthode N°3
Code par courriel

La méthode « Code par courriel »

Qu’est-ce que la méthode « Code par courriel »

La méthode du « Code par courriel » pour la double authentification opère en **envoyant un courriel** à l’adresse électronique fournie par l’utilisateur, **renfermant un code à usage unique.**

Contrairement à la méthode «Code temporel (TOTP)», le code par courriel n’est pas généré à intervalles réguliers, ce qui lui confère **une durée de validité plus étendue.** Toutefois, il est essentiel de noter que bien que le code par courriel ne soit pas lié à une période temporelle fixe, il reste généralement **valide pendant quelques minutes par mesure de sécurité.**

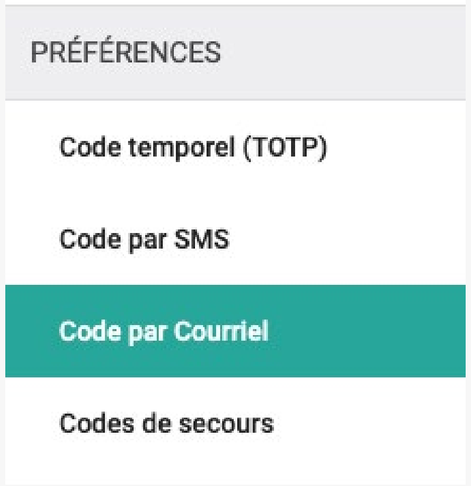
Cette approche renforce la sécurité en ajoutant **un second facteur au processus d’authentification**, exigeant à la fois quelque chose que l’utilisateur connaît (le mot de passe) et quelque chose qu’il possède (l’accès à sa boite mail pour recevoir le code).

Malgré sa large utilisation, la méthode par courriel peut présenter des vulnérabilités potentielles, notamment en termes de sécurité du courriel et de **risque d’interception des codes** par des parties non autorisées. Certains services explorent des alternatives plus sécurisées pour répondre à ces préoccupations.

La méthode « Code par courriel »

Activer la méthode « Code par courriel »

1 Rendez-vous sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Code par courriel ». Basculez ensuite le sélecteur sur « Activer ».



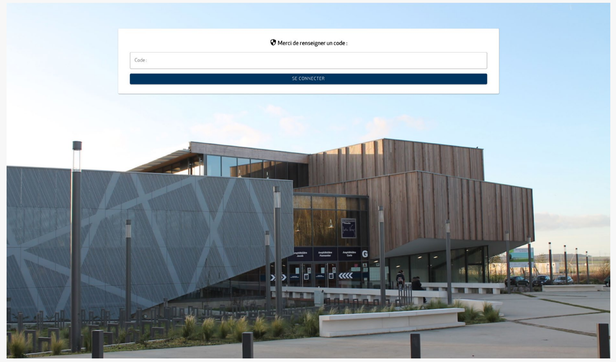
2 Saisissez l'adresse mail **(ne pas utiliser votre adresse mail professionnel en u-picardie**) sur lequel **seront envoyés les codes par courriel**, puis cliquez sur le bouton « Enregistrer ».

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

La méthode « Code par courriel »

Se connecter avec la méthode « Code par courriel »

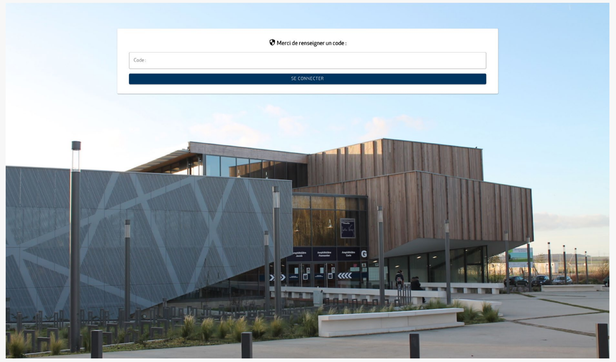
1 Lors de votre prochaine connexion nécessitant la double authentification, il vous est demandé **un code d'authentification à 6 chiffres.**



2 Lors de votre prochaine connexion nécessitant la double authentification, il vous sera demandé de **renseigner le code à 6 chiffres envoyé par mail.**

Pensez à vérifier votre dossier de Spam.

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



Méthode N°4
Code de secours

La méthode « Code de secours »

Qu’est-ce que la méthode « Code de secours »

La méthode du «Code de secours» dans le contexte de la double authentification consiste à fournir à l’utilisateur **10 codes à usage unique supplémentaires** qu’il peut utiliser **en cas d’indisponibilité de ses méthodes d’authentification habituelles**, telles que le code par SMS ou par courriel.

Ces codes de secours sont généralement générés une seule fois et peuvent être sauvegardés par l’utilisateur de manière sécurisée pour être utilisés en cas de besoin

L’utilisateur est fortement encouragé à prendre des mesures **pour stocker ces codes de secours de manière sécurisée**. Cela peut inclure **l’impression des codes et leur conservation dans un lieu sûr ou l’enregistrement sécurisé dans une application de gestion de mots de passe**. Ces codes de secours constituent une alternative cruciale en cas d’urgence où l’accès aux méthodes d’authentification principales est compromis.

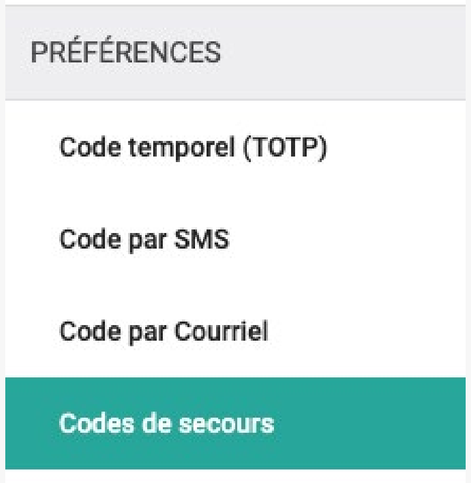
En cas de besoin, l’utilisateur peut utiliser l’un de ces codes de secours pour effectuer la double authentification. Il est important de noter **que chaque code de secours est à usage unique**, ce qui signifie qu’il ne peut être utilisé qu’une seule fois. Cette caractéristique renforce la sécurité du processus.

Il est crucial de traiter ces codes de secours avec **autant de précautions que les informations de connexion habituelles** afin d’éviter tout risque d’accès non autorisé au compte.

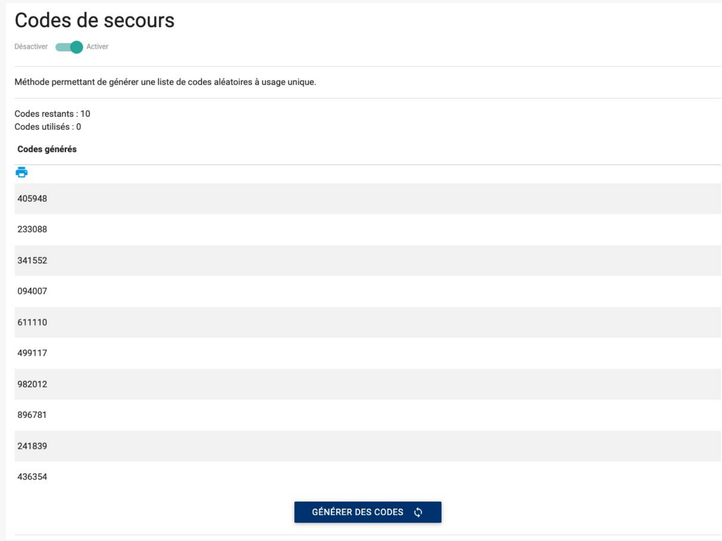
La méthode « Code de secours »

Activer la méthode « Code de secours »

1 Rendez-vous sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Code de secours ». Basculez ensuite le sélecteur sur « Activer ».



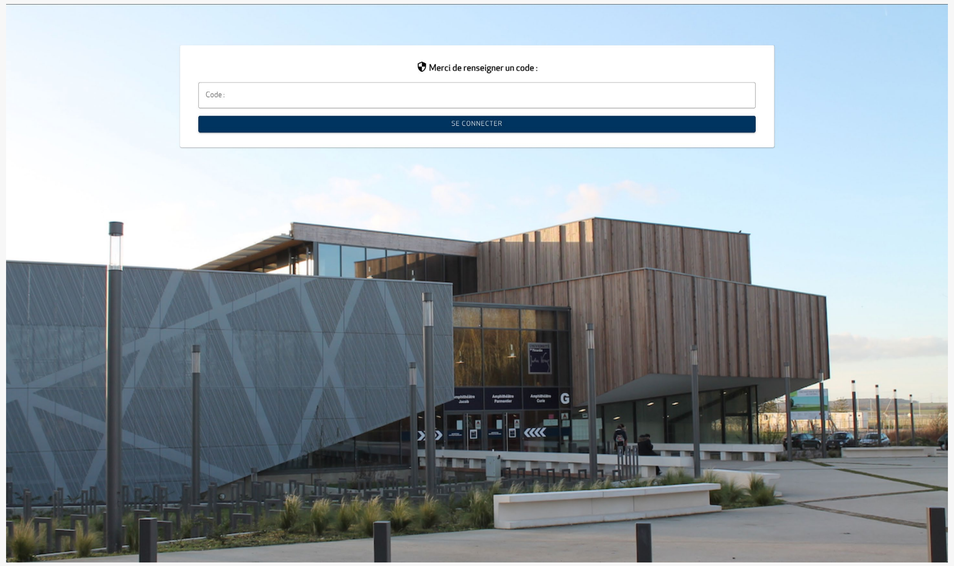
2 Cliquez ensuite sur **« Générer des codes »**. Une liste de 10 codes aléatoires à usage unique sera générée. Vous avez la possibilité **d'imprimer ces codes** directement depuis cette page. Nous vous conseillons vivement de conserver cette liste en lieu sûr et de créer **une copie dans un coffre-fort numérique.**



La méthode « Code de secours »

Se connecter avec la méthode « Code de secours »

Si aucune des méthodes de connexion paramétrées au préalable ne fonctionne, vous pouvez utiliser la méthode « Code de secours ».
Entrez l'un des dix codes de secours que vous avez générés au préalable et conservés en lieu sûr.



Méthode N°5
Notifications

La méthode « Notifications »

Qu’est-ce que la méthode « Notifications »

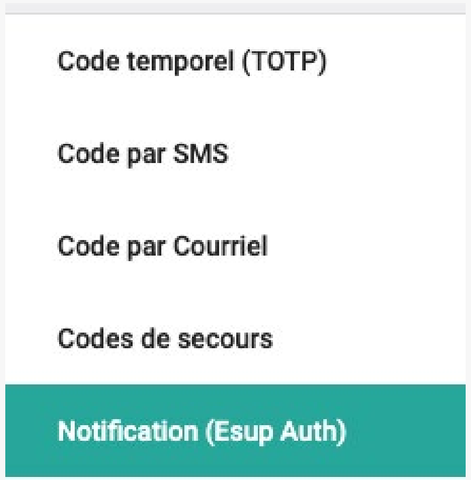
La méthode des « Notifications » pour la double authentification fonctionne en envoyant une notification à **l’appareil mobile préalablement enregistré par l’utilisateur**, généralement via une application dédiée. Cette notification contient une demande d’approbation pour confirmer l’identité de l’utilisateur.

Contrairement à la méthode « Code temporel (TOTP) », la notification n’est pas générée à intervalles réguliers. Elle est **déclenchée en temps réel lors de la tentative de connexion**, ce qui permet une validation instantanée et une interaction directe avec l’utilisateur. Bien que cette méthode dépende de la disponibilité du réseau et de l’appareil mobile, elle reste généralement très réactive.

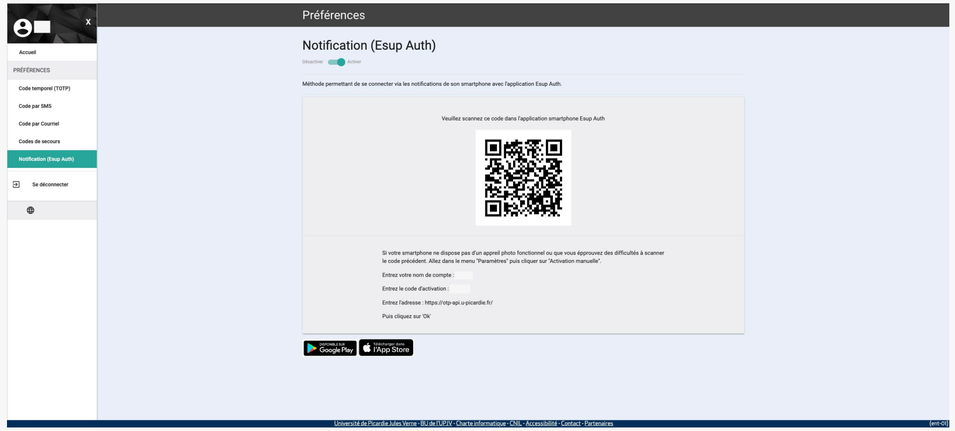
La méthode « Notifications »

Activer la méthode « Notifications »

1 Rendez-vous sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Notifications ». Basculez ensuite le sélecteur sur « Activer ».



2 Vous devez télécharger au préalable l'application «Esup Auth» sur votre smartphone. Ouvrez ensuite l'application et **scannez le QR code qui s'affiche à l'écran**. suivez ensuite la procédure indiqué sur votre smartphone.



La méthode « Notifications »

Se connecter avec la méthode « Notifications »

Lors de votre prochaine connexion nécessitant la double authentification, vous recevrez une notification sur votre smartphone. Vous devrez alors simplez cliquez dessus et **appuyer pour valider la connexion**.

Méthode N°6
Facteur physique (WebAuthn)

La méthode « Facteur physique (WebAuthn) »

Qu’est-ce que la méthode « Facteur physique (WebAuthn) »

La méthode WebAuthn pour la double authentification permet à l’utilisateur de se connecter en **utilisant un dispositif physique ou biométrique déjà enregistré.** Ce dispositif peut être une clé de sécurité USB, un capteur biométrique (empreinte digitale, reconnaissance faciale), ou encore un appareil mobile compatible. Lors de la tentative de connexion, l’utilisateur **valide son identité en interagissant avec ce dispositif.**

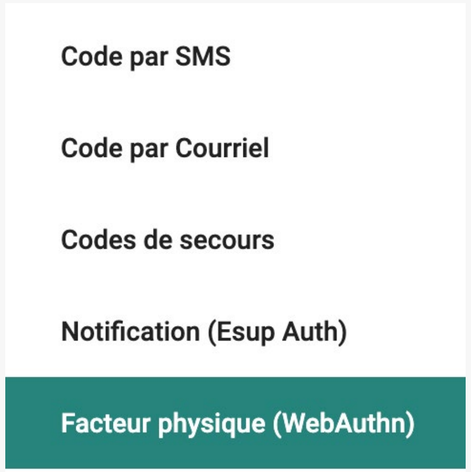
Contrairement à la méthode « Code temporel (TOTP) », qui génère des codes à intervalles réguliers, WebAuthn repose sur une validation directe via un appareil spécifique au moment de la connexion. Une fois le mot de passe saisi, le dispositif demandé s’active automatiquement, **permettant une authentification instantanée.** Cette méthode offre une sécurité renforcée en s’assurant que seul l’appareil physique enregistré peut valider l’accès, rendant toute tentative de connexion frauduleuse impossible sans cet appareil.

Bien que WebAuthn nécessite l’accès à un appareil physique, il est rapide et intuitif, offrant une protection optimale contre les attaques en ligne.

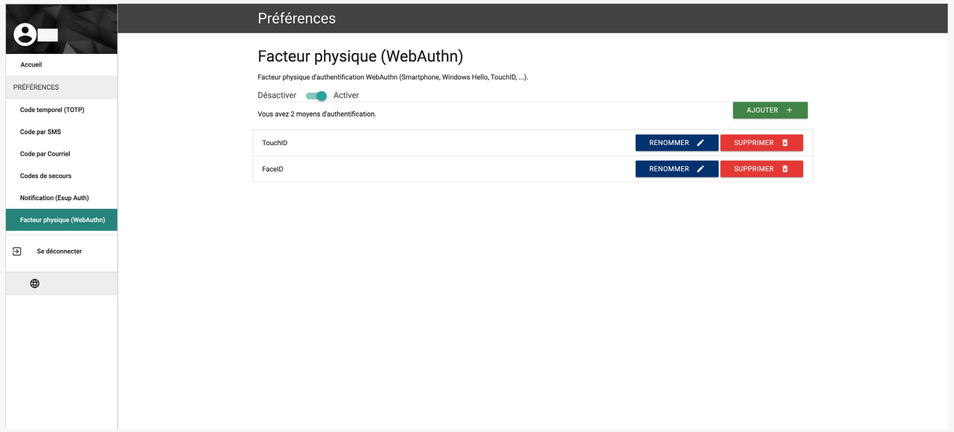
La méthode « Facteur physique (WebAuthn) »

Activer la méthode « Facteur physique (WebAuthn) »

1 Rendez-vous sur l'application **« Authentification renforcée »** de l'UPJV, sur le panneau de gauche cliquez sur « Préférence » et sur l'item « Facteur physique (WebAuthn) ». Basculez ensuite le sélecteur sur « Activer ».



2 Ajouter un dispositif en cliquant sur le bouton «Ajouter». Si vous utilisez une clé USB de sécurité, insérez-la et suivez les étapes pour l'enregistrer. Si vous utilisez un capteur biométrique, placez votre doigt ou utilisez la reconnaissance faciale pour valider l'enregistrement. Suivez les étapes qui s'affiche sur votre écran pour terminer l'ajout. Il est recommandé de renommer votre dispositif après l'avoir ajouté, afin de pouvoir l'identifier facilement lors de vos prochaines connexions.



La méthode « Facteur physique (WebAuthn) »

Se connecter avec la méthode « Facteur physique (WebAuthn) »

Lors de votre prochaine connexion nécessitant la double authentification via la méthode « Facteur physique (WebAuthn) », vous serez invité à utiliser votre dispositif enregistré. Il vous suffira **d'insérer votre clé de sécurité ou de valider via un capteur biométrique (comme une empreinte digitale)** pour confirmer la connexion.

Contact et ressources

Contact :

Centre d’assistance

Ressources :

Infographie de la double authentification