Authentification à deux facteurs :
Sécurisation de votre compte informatique

Une authentification à deux facteurs va devenir obligatoire pour sécuriser votre compte informatique :

- Le premier facteur reste le couple **identifiant / mot de passe de votre compte Lyon 2 ;**
- Le second facteur prendra la forme d'un **code TOTP** qui sera indispensable pour vous connecter aux applications universitaires en ligne.

TOTP signifie "Time-based One Time Password", littéralement "mot de passe à usage unique basé sur le temps".

En pratique, c'est un code à 6 chiffres changeant et valide seulement 30 secondes qu'il faut saisir après votre mot de passe universitaire, quand il vous est demandé.

Créer votre second facteur TOTP

La création initiale (ou « enrôlement ») du second facteur est une étape que vous ferez une seule fois. Cette opération doit être obligatoirement effectuée à partir de votre ordinateur professionnel Lyon 2.

Prérequis :

- Votre ordinateur doit être strictement à l'heure (à la seconde près)
- Votre navigateur doit disposer de l'extension Authenticator

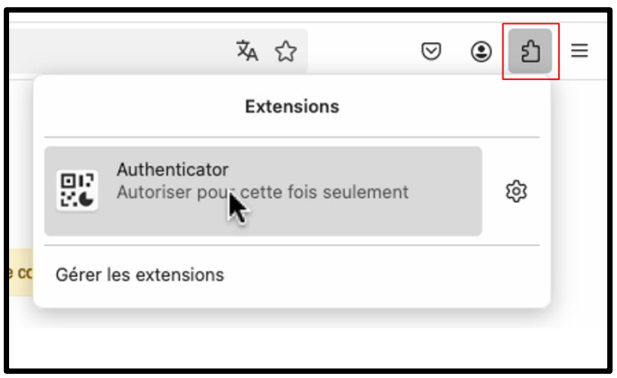
L'extension *Authenticator* pour Firefox et Chrome est installée sur tous les postes gérés par la DSI. Elle permet la **création initiale puis l'utilisation d'un code TOTP** à chaque nouvelle connexion. Pour les postes non gérés par la DSI, l'extension est téléchargeable à l'adresse https://authenticator.cc

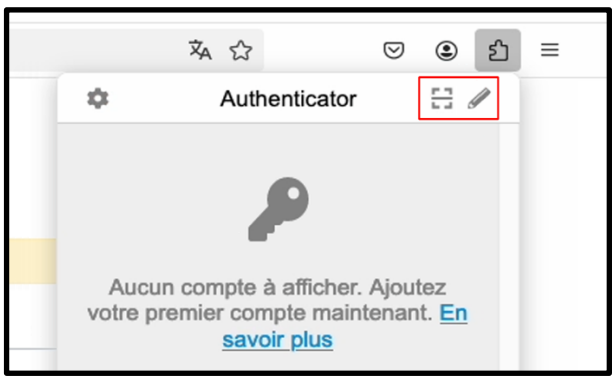
Après son installation, les étapes qui suivent sont identiques.

Vous aurez un temps limité pour effectuer les 7 étapes suivantes, ainsi prenez bien le temps de les lire avant de démarrer.

1. Connectez-vous à https://casl2.univ-lyon2.fr, saisissez votre identifiant et votre mot de passe habituels Lyon 2, puis rendez-vous sur https://casl2.univ-lyon2.fr/2fregisters
2. La page suivante s'affiche, lisez simplement le texte sur fond jaune et passez à l'étape suivante

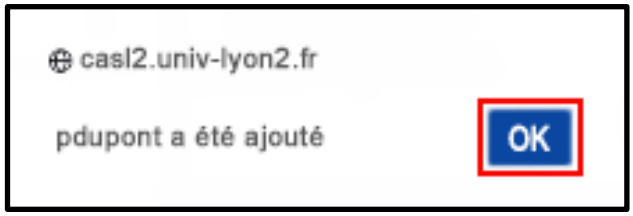
3. Ouvrez l'extension *Authenticator* dans la barre du navigateur, et cliquez sur l'icône d'acquisition de QR Code :





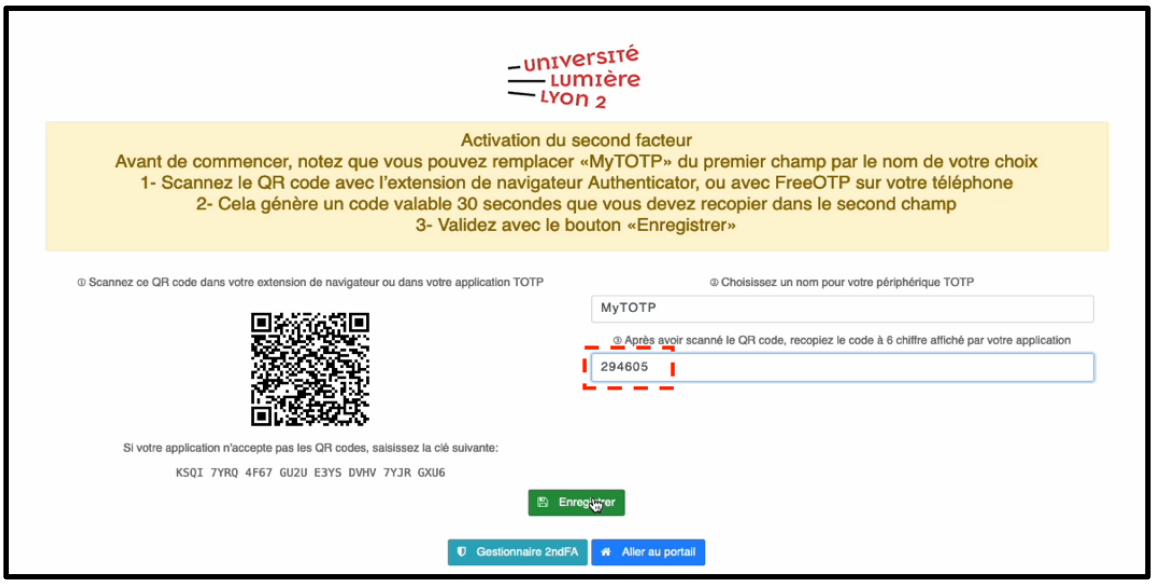
4. Avec le curseur de la souris, entourez entièrement le QR code affiché dans la page :

5. Quand le message suivant apparait (dans cet exemple « pdupont » est l'identifiant du compte), cliquez sur « **OK** » :

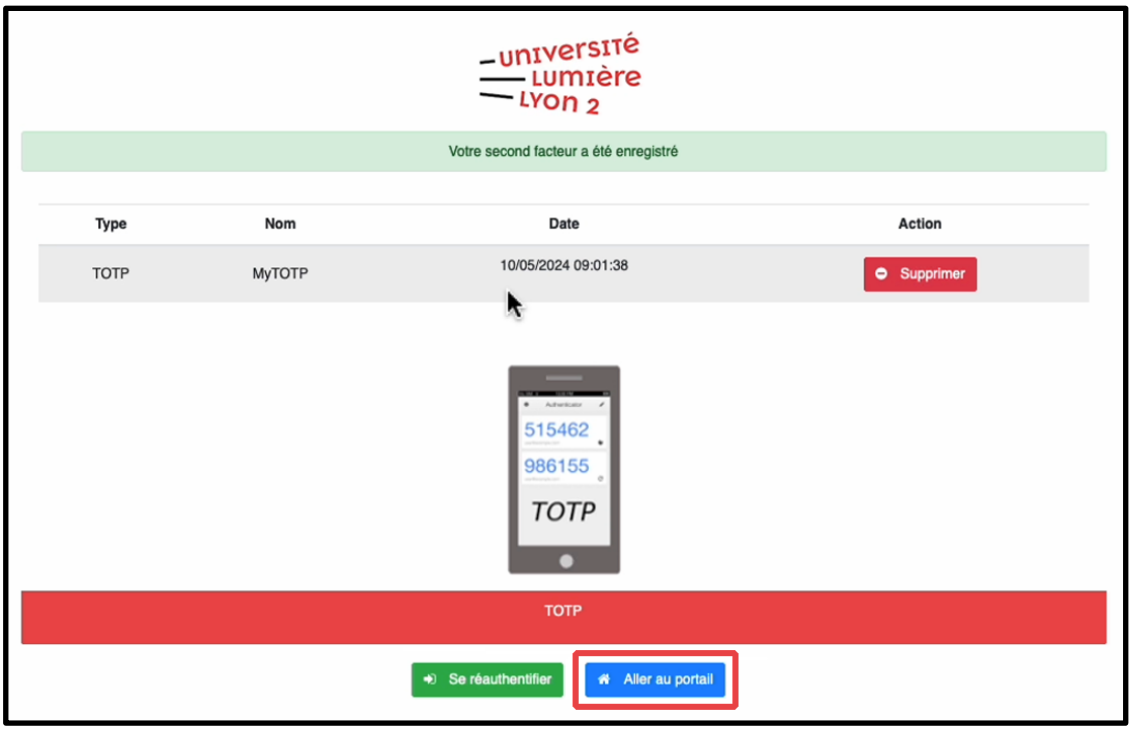


6. Revenez sur *Authenticator* et cliquez sur le code TOTP pour le copier dans le presse-papier :

7. Collez le code TOTP dans le dernier champ de formulaire puis cliquez sur « **Enregistrer** ». La création initiale de votre second facteur a été enregistrée :



À l'issue de la 7ème et dernière étape le message de confirmation suivant doit apparaître :



Cliquez sur le bouton bleu « **Aller au portail** » pour revenir à l'accueil du portail Applis.

Activer votre second facteur

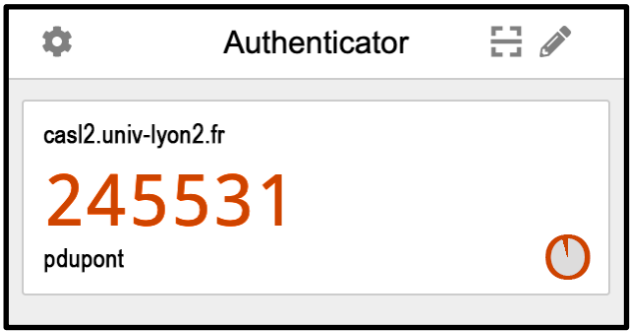
Votre second facteur TOTP a été créé mais il reste encore à l'activer pour protéger votre compte. Après cette étape, l'icône « **Validation MFA** » sera visible dans votre portail dans la section « Aide et tutoriels ». Ouvrez cette application :

Un message vous indique que cette application nécessite une authentification d'un niveau supérieur. Cliquez sur le bouton vert « **Se réauthentifier** » :

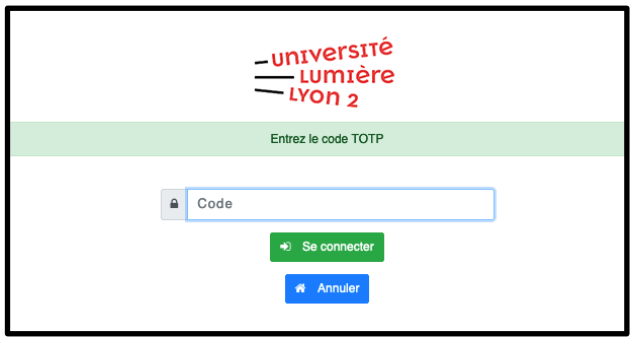
Quand vous cliquez sur le bouton vert « **Se réauthentifier** » il vous est proposé d'utiliser votre second facteur.

Le code TOTP est affiché par l'extension *Authenticator* dans votre navigateur : ouvrez l'extension et cliquez sur le code à usage unique pour le copier.

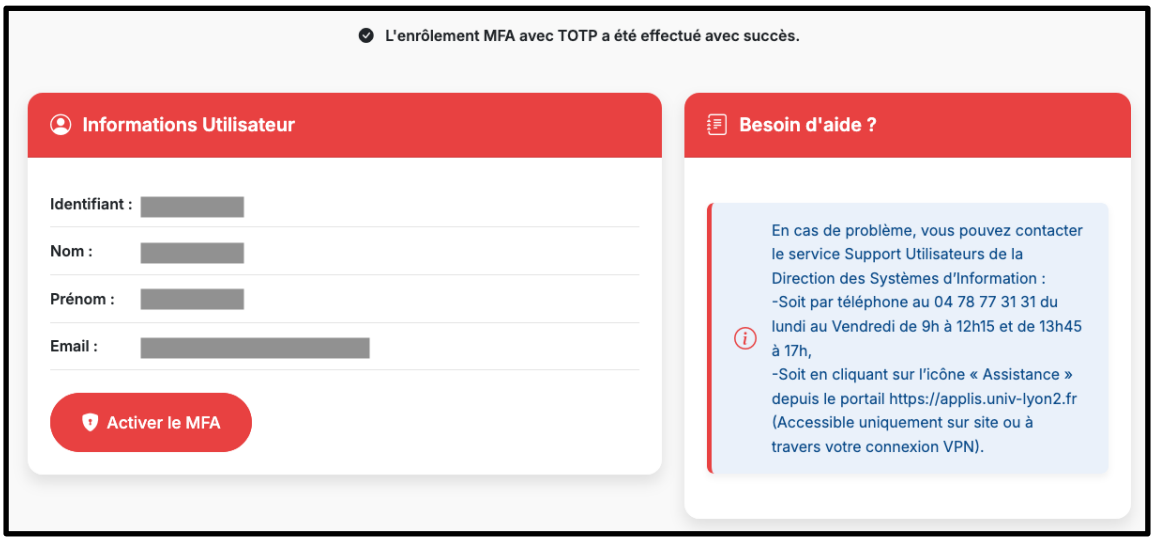
Le "minuteur" sur le côté décompte le temps restant sur les 30 secondes initiales : quand le code passe du bleu au rouge il vous reste seulement 5 secondes, dans ce cas-là attendez le code suivant :



Sur la fenêtre suivante, collez-le dans le champ « code », cliquez enfin sur « **Se connecter** » :

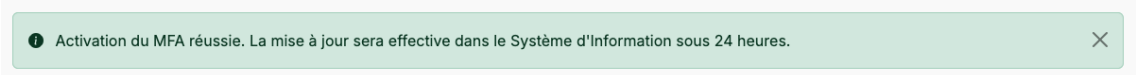


Si votre TOTP fonctionne, alors la fenêtre suivante s'ouvre :



Cette fenêtre vous indique que votre enrôlement est réussi et vous propose d'activer votre MFA pour protéger votre compte.

Après avoir cliqué sur le bouton rouge « Activer le MFA » le message suivant est affiché :



Votre compte Lyon 2 sera protégé et sous un délai de 24 maximum votre TOTP deviendra indispensable pour la connexion aux outils numériques.

Utiliser le code TOTP

Lors de vos prochaines authentifications sur le portail de l'université vous devrez fournir vos identifiant et mot de passe, puis le code TOTP généré au moment où vous vous connectez. Le code TOTP est affiché par l'extension *Authenticator* dans votre navigateur : ouvrez l'extension pour visualiser le code à usage unique quand le portail d'authentification vous le demande.

La marche à suivre est exactement la même que pour l'activation : quand le code TOTP vous est demandé, ouvrez l'extension *Authenticator* et copiez-collez le code dans la fenêtre d'authentification.

Pour des cas d'usages différents (sur smartphone, sur plusieurs navigateurs ou plusieurs ordinateurs), rendez-vous au chapitre « Compléments » de ce document.

Mon code TOTP ne fonctionne pas

- Le code TOTP étant valide seulement 30 secondes, il peut être refusé si vous l'avez saisi trop tard : **procéder par un copier-coller rapide** permet d'éviter ce problème.
- Un décalage horaire de votre ordinateur (si vous utilisez *Authenticator*) ou de votre téléphone (si vous utilisez *FreeOTP*) peut être aussi à l'origine du refus du code TOTP : **vérifiez bien que vos appareils sont à l'heure exacte, à la seconde près.**

Si votre code reste malgré tout refusé, **ouvrez un ticket en tapant directement l'adresse de l'assistance sans passer par applis.univ-lyon2.fr** : https://assistance.univ-lyon2.fr

Compléments

1. Application mobile *FreeOTP*

En complément de l'extension de navigateur *Authenticator*, il est possible d'utiliser une application sur votre téléphone Android ou iOS **notamment pour vous authentifier quand vous utilisez un autre ordinateur que votre ordinateur professionnel Lyon 2.**

La DSI recommande fortement FreeOTP » publiée par RedHat. C'est une application sûre, libre (open source) et gratuite.
Pour l'installer, rendez-vous sur la page officielle https://freeotp.github.io/ ou scannez ce code :

Avec cette application vous pourrez enregistrer votre second facteur TOTP en scannant un QR Code.

FreeOTP vous demande, au premier lancement, de choisir un mot de passe qui est utilisé pour chiffrer et déchiffrer les sauvegardes de FreeOTP. Choisissez quelque chose de facile à mémoriser.

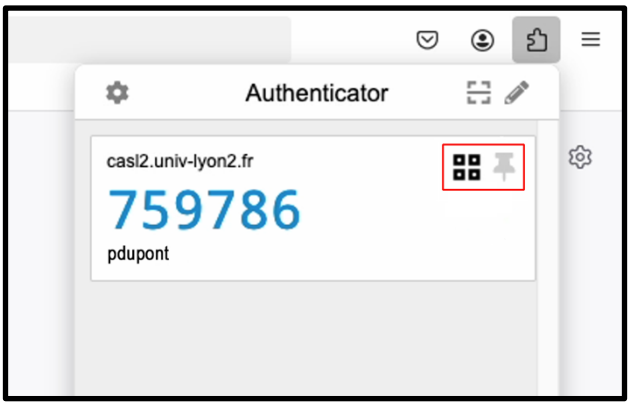
Pour faire l'ajout par QR Code vous pouvez :

- Soit scanner le QR Code au même moment qu'avec l'extension *Authenticator* (dans un temps limité donc) ;
- Soit scanner le QR Code affiché dans l'extension *Authenticator* (n'importe quand, sans limite de temps), nous vous conseillons cette méthode.

La copie de votre second facteur entre l'extension *Authenticator* et l'app *FreeOTP* se fait en deux étapes.

Étape 1 :

Dans le navigateur sur votre ordinateur, ouvrez l'extension *Authenticator* et tout à droite de la mention « casl2.univ-lyon2.fr » cliquez sur l'icône qui représente un petit QR Code :



Étape 2 :

Sur votre téléphone, lancez l'app *FreeOTP* et cliquez sur le (+) puis sur le symbole du scanner de QR Code. Scannez le QR Code affiché par l'extension *Authenticator* sur votre ordinateur :

Désormais, votre ordinateur et votre téléphone doivent afficher le même code TOTP toutes les 30 secondes. Vous pourrez utiliser indifféremment l'un ou l'autre pour votre authentification sécurisée sur le SI Lyon 2. Si les codes sont différents, vérifiez bien que les deux appareils sont bien à l'heure exacte : un code TOTP généré par un appareil qui n'est pas à l'heure a de forte chance de ne pas fonctionner.

2. Supprimer un enrôlement raté

Il se peut, dans de rares cas, que l'enrôlement initial de votre TOTP ne se déroule pas correctement. Le symptôme pour ce type d'incident est que le serveur d'authentification Lyon 2 vous demande d'enrôler un second facteur et/ou ne vous propose jamais de saisir votre code TOTP à 6 chiffres.

Vous aurez alors dans l'extension Authenticator de votre navigateur, ou dans FreeOTP sur votre téléphone, un enregistrement MFA inutile, voire encombrant. Pour nettoyer cet enrôlement raté, il vous suffit de le supprimer.

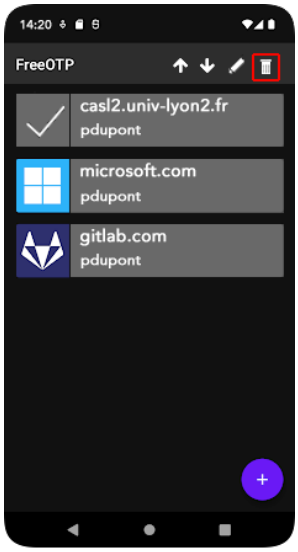
Attention, si votre TOTP fonctionne (il vous est demandé de le saisir, et quand vous le saisissez, vous accédez à vos applications) il ne faut surtout pas le supprimer. La suppression est irréversible.

Pour supprimer un enrôlement raté dans *Authenticator* :

- Ouvrez *Authenticator*
- Cliquez sur l'icône de crayon en haut à droite
- Cliquez sur le rond rouge barré d'un signe « moins »

Pour supprimer un enrôlement raté dans *FreeOTP* :

- Ouvrez l'application *FreeOTP*
- Sélectionnez (avec un appui long) la ligne correspondant à casl2.univ-lyon2.fr
- Pressez l'icône « poubelle » en haut à droite et validez



3. Protéger le second facteur

En fonction de votre contexte d'usage il peut être prudent de protéger l'accès à votre TOTP. Le RSSI recommande que l'accès à l'extension *Authenticator* sur votre navigateur soit protégée par mot de passe. Il n'est pas nécessaire que ce mot de passe soit complexe. Il peut s'agir par exemple des X premiers caractères de votre mot de passe Lyon 2 (mais surtout pas de votre mot de passe Lyon 2 en entier).

- Ouvrez *Authenticator*
- Cliquez la roue d'engrenage en haut à gauche
- Dans le menu, cliquez sur « Sécurité »
- Saisissez un mot de passe et validez
- Revenez au menu et cliquez « Préférences »
- Choisissez un délai raisonnable pour le verrouillage d'*Authenticator*

Pour protéger votre second facteur dans *FreeOTP*, assurez-vous simplement que votre téléphone est protégé par un verrou (code PIN, empreinte, autre).

4. Utiliser plusieurs navigateurs, sauvegarder ou exporter votre second facteur

Il peut être nécessaire dans certains contextes de faire une sauvegarde ou un export de votre second facteur. Par exemple si vous souhaitez le copier sur un autre navigateur, sur un autre appareil, etc.

L'opération est possible à partir de *Authenticator* dans votre navigateur, et à partir de *FreeOTP* sur téléphone, mais le fonctionnement est à la fois plus riche et plus souple à partir de *Authenticator* :

- Ouvrez l'extension *Authenticator*
- Cliquez la roue d'engrenage en haut à gauche
- Dans le menu, cliquez sur « Sauvegarde »
- Cliquez sur « Télécharger un fichier de sauvegarde »

Vous obtenez sur votre poste un fichier « authenticator.txt » contenant votre clé secrète TOTP. Ce fichier peut être restauré dans l'extension *Authenticator* sur un autre navigateur / une autre machine. Il suffit pour cela de cliquer sur « Importer une sauvegarde » dans le menu « Sauvegarde » puis dans la page qui s'affiche, de cliquer sur « Importer un fichier de sauvegarde ».

Pensez bien à détruire les copies de ce fichier dès que vous n'en aurez plus besoin. Certains virus spécialisés dans le vol de mots de passe savent détecter et aspirer ces fichiers. Dans *Authenticator* vous pouvez aussi très simplement afficher un QRCode permettant de recopier votre clé secrète TOTP sur un smartphone. La méthode pour afficher le QRCode est décrite à l'étape 1 du chapitre « Application mobile *FreeOTP* », page 7 de ce document.

Si vous faites une capture d'écran de ce QRCode vous pourrez aussi l'importer de nouveau plus tard dans *Authenticator* (menu « Sauvegarde » puis « Importer une sauvegarde »).

Comme pour l'export en fichier texte, la capture d'écran devra être supprimée dès que vous n'en aurez plus l'usage. Si vous souhaitez conserver durablement un export texte ou image de votre TOTP Lyon 2, faites-le sur un espace sécurisé : jamais sur un cloud public, jamais dans votre messagerie, de préférence sur un stockage externe protégé par mot de passe, comme une clé ou un disque USB chiffré. Certains gestionnaires de mots de passe peuvent stocker des fichiers, c'est aussi un bon choix.