TUTORIEL : AUTHENTIFICATION FORTE MULTIFACTEUR (MFA)

Vous trouverez plus d'informations sur le projet MFA à cette adresse https://dsiun.univ-tln.fr/L-authentification-forte-multifacteur-ou-MFA.html

Avant de pouvoir sécuriser vos accès avec le MFA, vous devez préalablement activer l'authentification forte en suivant les trois étapes suivantes :

- Étape 1 : Installation de l'application d'authentification forte « Authenticator » sur votre poste de travail principal
- Étape 2 : Activation de l'application d'authentification forte sur votre poste de travail principal
- Étape 3 : Choix de votre code PIN personnel

Pour une gestion autonome de vos applications d'authentification forte, et/ou pour gérer vos accès en mobilité, nous vous recommandons également une étape optionnelle :

- Étape 4 : Installation de l'application d'authentification forte sur un autre appareil : smartphone, tablette ou autre poste de travail en votre possession

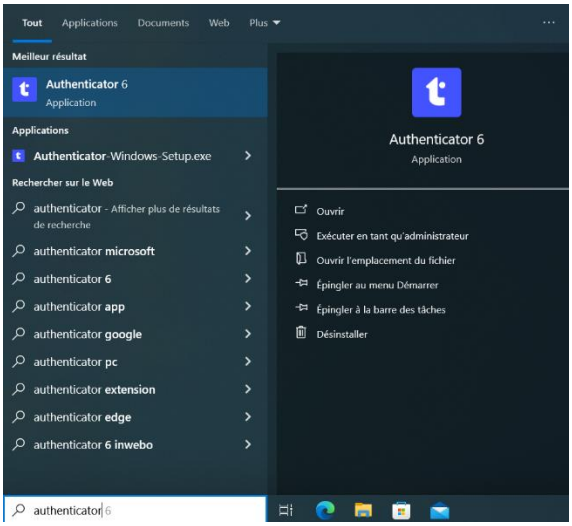
Vous pourrez alors utiliser l'authentification forte multifacteur lors de vos prochaines connexions aux services numériques de l'université de Toulon (Étape 5 : Utilisation de l'authentification forte multifacteur)

ÉTAPE 1 : INSTALLATION DE L'APPLICATION D'AUTHENTIFICATION FORTE

CAS 1 : VOTRE POSTE EST GERE PAR UN SERVICE INFORMATIQUE DE L'UNIVERSITE (DSIUN, SA2I)

L'application « Authenticator » a normalement été déployée sur votre poste.

Assurez-vous que l'application est bien installée en recherchant l'icône de l'application sur votre bureau ou en recherchant l'application sur votre poste de travail.



Si l'application n'est pas installée, vous pouvez l'installer en autonomie en vous reportant au cas 2 : Vous gérez vous-même votre poste.

En cas de souci contactez le support du service informatique qui gère votre poste.

CAS 2 : VOUS GEREZ VOUS-MEME VOTRE POSTE

Téléchargez l'application Authenticator sur votre poste de travail. L'application peut aussi être utilisée sur votre smartphone ou votre tablette.

Pour cela, rendez-vous sur le site Trustbuilder.com https://www.trustbuilder.com/app-downloads et dans la partie **TrustBuilder Desktop Authenticator,** cliquez sur Download correspondant à votre système d'exploitation (Windows, MacOs, Linux)

TrustBuilder Desktop Authenticator

TrustBuilder Desktop Authenticator is an app that generates unique passwords (OTP) including push notification. It also has an offline mode. To add a service to your authentication profile, your administrator must provide you with an activation code for this service.

Windows — Download

macOS — Download

Linux — Download

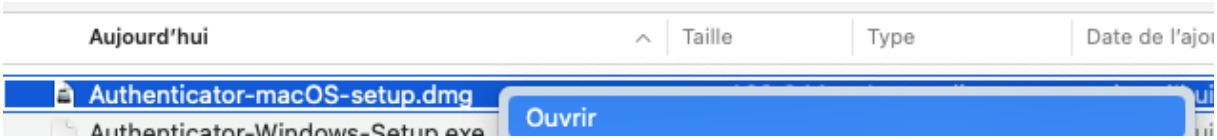
Earlier versions Windows / macOS

INSTALLATION SOUS WINDOWS

Une fois l'application téléchargée, allez dans votre dossier de téléchargement et cliquez sur le fichier pour lancer l'installation.

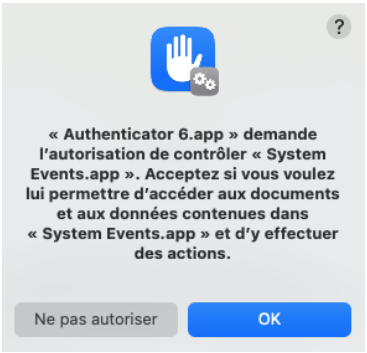
INSTALLATION SOUS MACOS

Une fois l'application téléchargée, allez dans votre dossier de téléchargement, faites un clic droit sur le nom de l'application et choisissez Ouvrir afin d'être sûr de pouvoir lancer l'installation.



Autorisez les demandes d'autorisation de contrôle si des boites de dialogues se présentent à l'écran.

Par exemple :



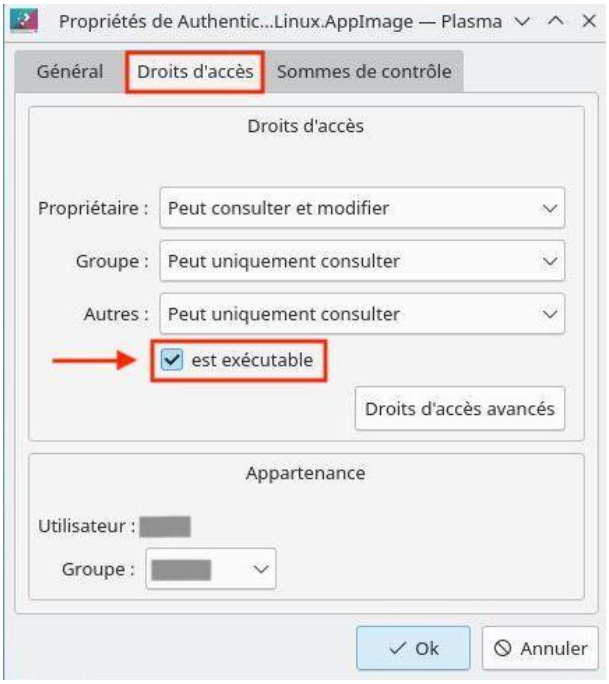
Si vous obtenez ce message :

Assurez-vous de bien installer l'application en faisant un clic-droit sur l'icône d'installation, tout en maintenant la touche Control appuyée et sélectionnez Ouvrir dans le menu déroulant. Une fois installée, il suffira de cliquer sur l'icône de l'application pour qu'elle se lance.

Procédure pas à pas :
Dans le Finder de votre Mac, repérez l'application que vous souhaitez ouvrir.
Attention n'utilisez pas Launchpad, car il ne vous permet pas d'utiliser le menu contextuel.
Faites un clic-droit sur l'icône de l'application en maintenant la touche Contrôle enfoncée, puis choisissez Ouvrir dans le menu contextuel.
Cliquez sur Ouvrir.
L'application est enregistrée en tant qu'exception dans vos réglages de sécurité et vous pourrez l'ouvrir par la suite en cliquant deux fois dessus, comme n'importe quelle application enregistrée.

INSTALLATION SOUS GNU/LINUX

Une fois l'application téléchargée, allez dans votre dossier de téléchargement, faites un clic droit sur le nom de l'application et choisissez « Propriétés ».
Dans la fenêtre qui s'affiche, rendez « **Authenticator 6** » exécutable :



En ligne de commande :

- Lancez un terminal.
- Rendez-vous dans le dossier où se trouve l'application :

```sh
user@mon-pc:~$ cd Téléchargements/
```

- Rendez l'application **exécutable** :

```sh
user@mon-pc:~/Téléchargements$ chmod +x Authenticator6-Linux.AppImage
```

- Lancez l'application :

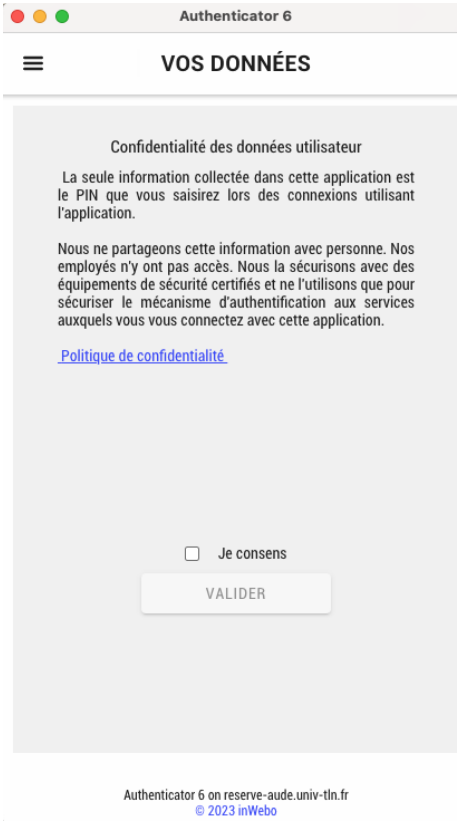
```sh
user@mon-pc:~/Téléchargements$ ./Authenticator6-Linux.AppImage
```

ÉTAPE 2 : ACTIVATION DE L'APPLICATION D'AUTHENTIFICATION FORTE

Une fois l'application installée et ouverte, vous devez consentir à la politique de confidentialité de vos données.

Pour rappel, seul le code PIN de connexion sera collecté par l'application lors de vos connexions. Aucune autre donnée personnelle n'est transmise.

Cochez la case Je consens et Faites valider.

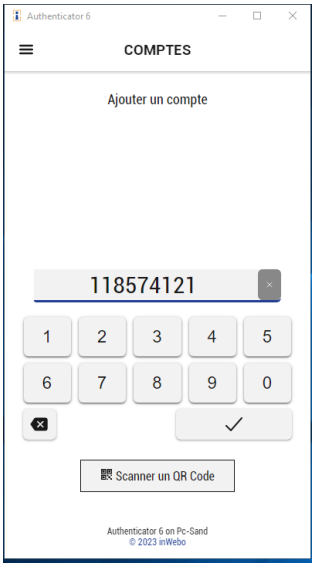


Vous devez ensuite activer l'application nouvellement installée sur votre poste de travail en saisissant un code d'activation à usage unique.

Ce code, vous a été transmis par SMS ou par courrier papier.

S'il n'est plus valide, vous pouvez demander à en recevoir un nouveau via l'interface https://assistance-mfa.univ-tln.fr. Celui-ci vous sera envoyé par SMS. Si vous n'avez pas fourni de numéro de téléphone à la DRH ou à la scolarité, veuillez envoyer un e-mail à usagesnum@univ-tln.fr pour prendre rendez-vous et venir le récupérer en présentiel.

Vous devez intégrer ce code (*ici le 118574121 pour l'exemple*) dans l'application et cliquer sur entrée ou la coche ☑.



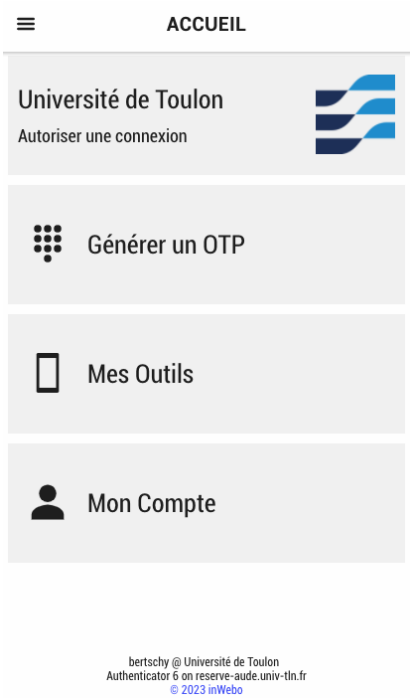
ÉTAPE 3 : CHOIX DU CODE PIN PERSONNEL

Une fois l'activation autorisée, vous devez **choisir votre code PIN personnel à 6 chiffres.** Ne le diffusez à personne et ne le perdez pas ! Il sera demandé à chaque fois que vous voudrez utiliser l'authentification forte multifacteur !!

En cas de perte du code PIN, la seule solution sera de faire appel au support de la DSIUN.

Vous pouvez saisir ce code PIN directement avec votre clavier numérique ou sélectionner les chiffres à l'écran.

Confirmez votre code PIN et validez l'opération.



Bravo vous avez activé l'authentification forte !

Dans quelques minutes (maximum 1h) vous pourrez désormais l'utiliser lors de vos prochaines connexions aux services numériques.

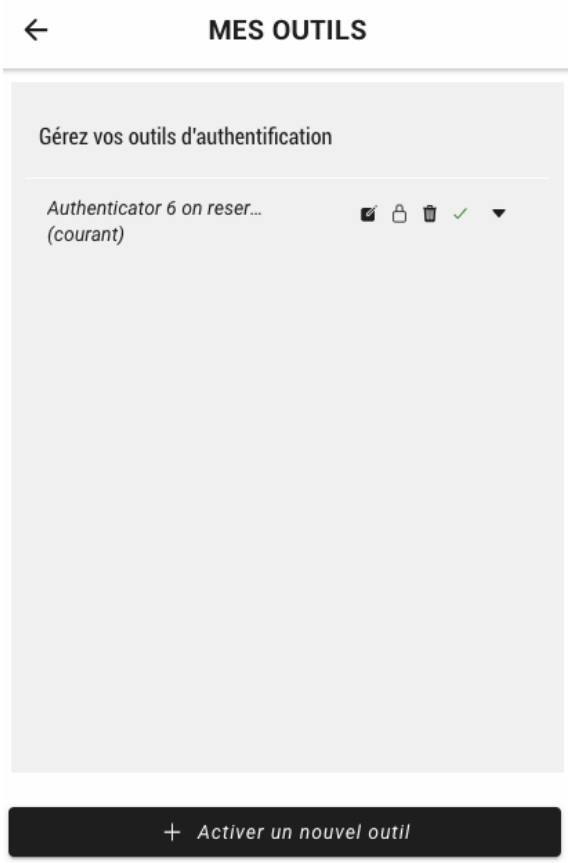
ÉTAPE 4 OPTIONNELLE : INSTALLATION DE L'APPLICATION SUR UN AUTRE SUPPORT : SMARTPHONE OU AUTRE POSTE DE TRAVAIL

Nous vous conseillons fortement d'installer l'application sur tous les postes de travail utilisés (desktop / ordinateur portable) et plus particulièrement **sur votre smartphone** afin d'être certain de pouvoir vous authentifier quel que soit le poste utilisé, même en mobilité.

Pour activer l'application sur un autre support : il faut générer un nouveau code d'activation.

Connectez-vous sur l'application Authenticator sur votre poste de travail principal (par exemple), allez dans le menu Mes Outils pour générer le code d'activation pour une nouvelle installation.

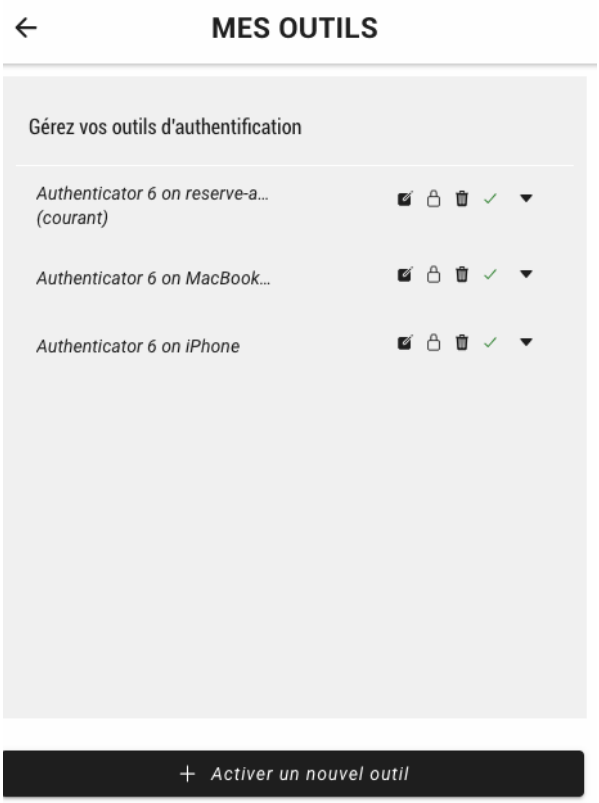
Cliquez en bas dans la barre noire sur **« + Activez un nouvel outil »**



puis **saisissez votre code PIN** pour confirmer la demande.

Vous obtenez alors **le code d'ajout d'un outil** à intégrer dans l'application installée sur un autre poste de travail ou le **QRcode à scanner** pour un smartphone (installer préalablement l'application avant de scanner le QRCode).

Dans le menu Outils, vous avez la liste des outils que vous avez activés pour l'authentification forte. Vous pourrez supprimer des outils quand vous le souhaitez (important quand vous cédez votre poste de travail ou si vous perdez votre smartphone) ou en ajoutez d'autres à tout moment.



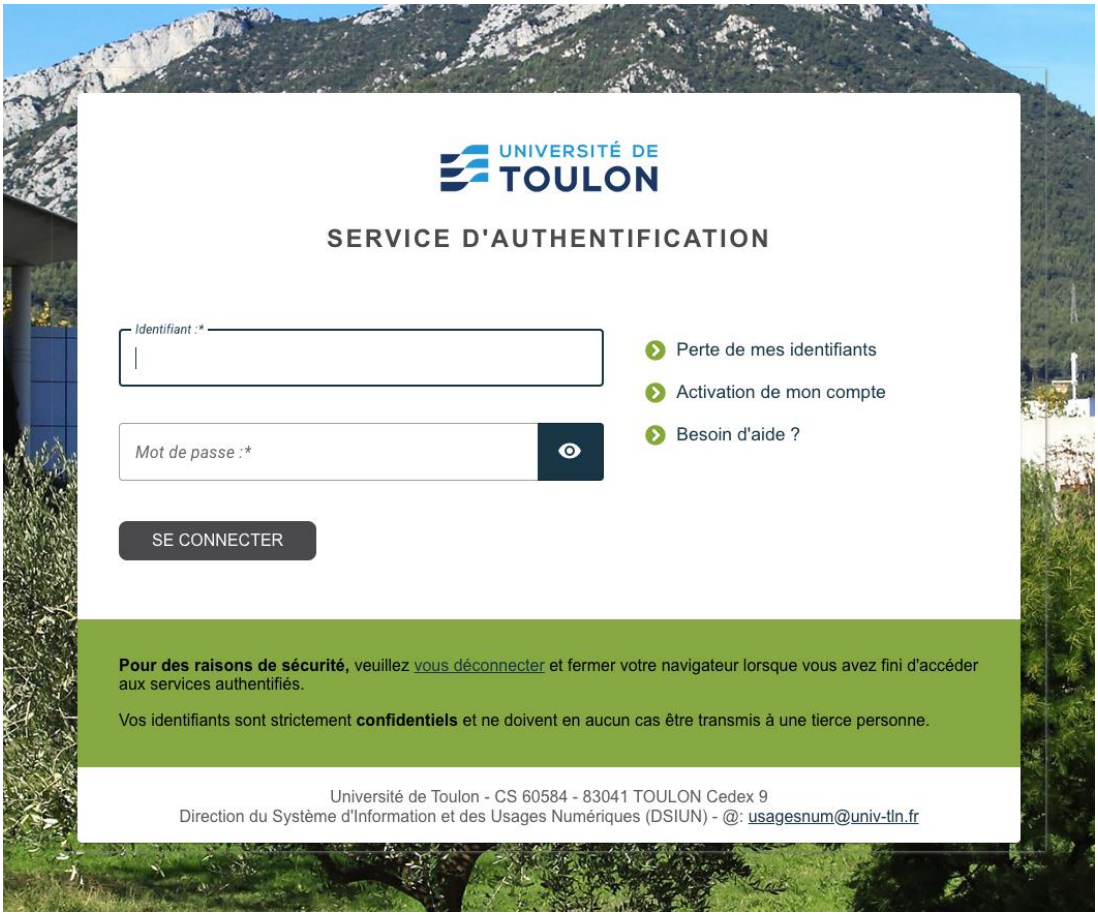
ÉTAPE 5 : UTILISATION DE L'AUTHENTIFICATION FORTE MULTIFACTEUR

CONNEXION A UN SERVICE NUMERIQUE

Dès que vous allez vous connecter à un service numérique de l'université qui exige une authentification, vous devrez valider le processus d'authentification avec l'application Authenticator.

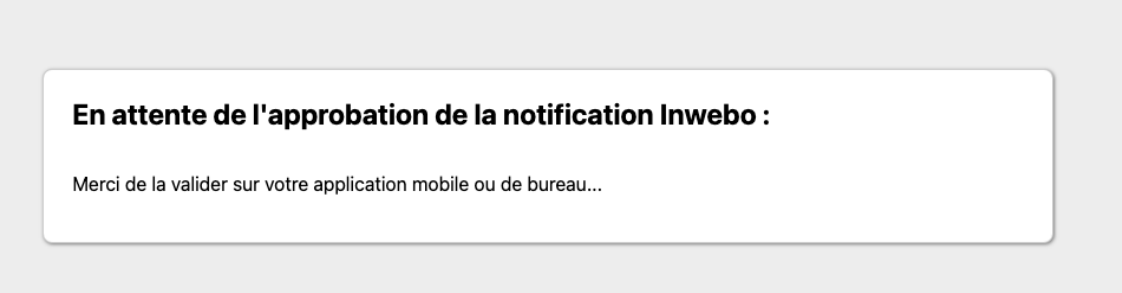
Par exemple, quand vous vous connectez au webmail : https://webmail.univ-tln.fr

Vous devez vous connecter au serveur d'authentification central de l'établissement (CAS) et mettre votre login et mot de passe :



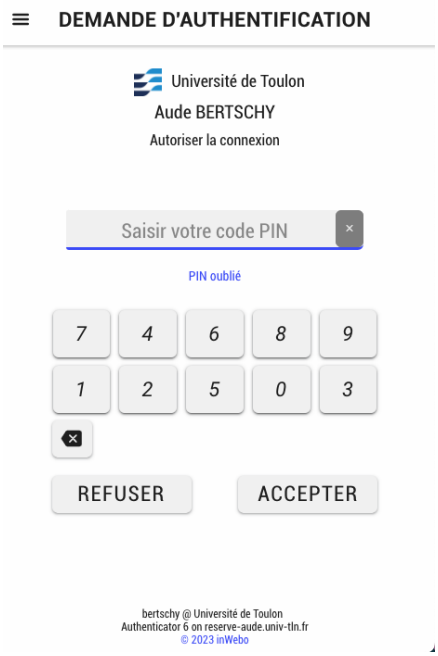
Vous cliquez sur Se Connecter, ce nouvel écran apparait : Cliquez ensuite sur « Commencer l'authentification multifacteur »

Ce message s'affiche :



Ouvrez l'application « Authenticator » (sur votre poste de travail ou votre smartphone) et Cliquez sur Autoriser une connexion tout en haut :

La demande d'authentification est faite, saisissez votre code PIN et acceptez.



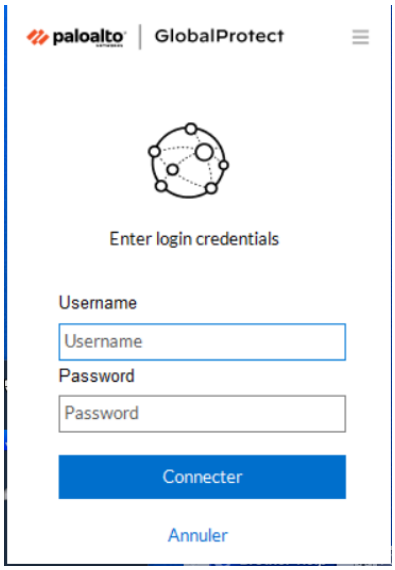
Votre authentification sur le service numérique est acceptée, vous pouvez consulter vos mails.

Si vous avez installé l'application sur votre mobile et que vous avez autorisé les notifications, vous pouvez aussi valider directement votre authentification sur votre smartphone en cliquant sur la notification et en indiquant votre code PIN.

CONNEXION AU VPN

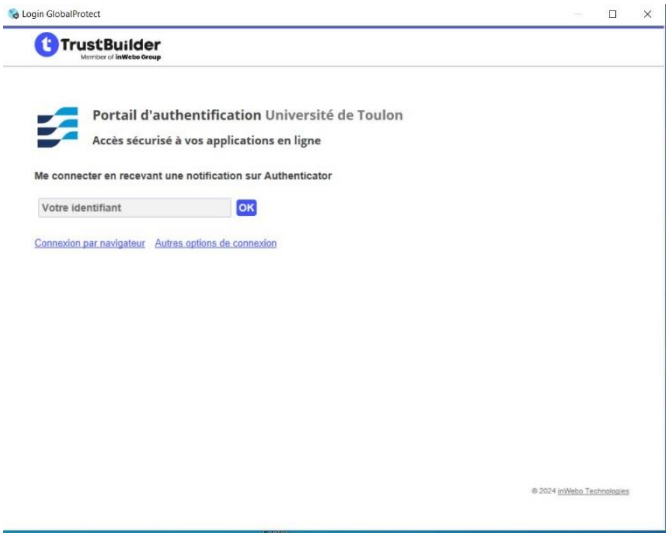
Attention : si le visuel de votre client GlobalProtect ne ressemble pas à la capture d'écran ci-dessous, merci de le mettre à jour.

Ouvrez l'application GlobalProtect, et indiquez vpn-secure.univ-tln.fr pour le nom du portail.



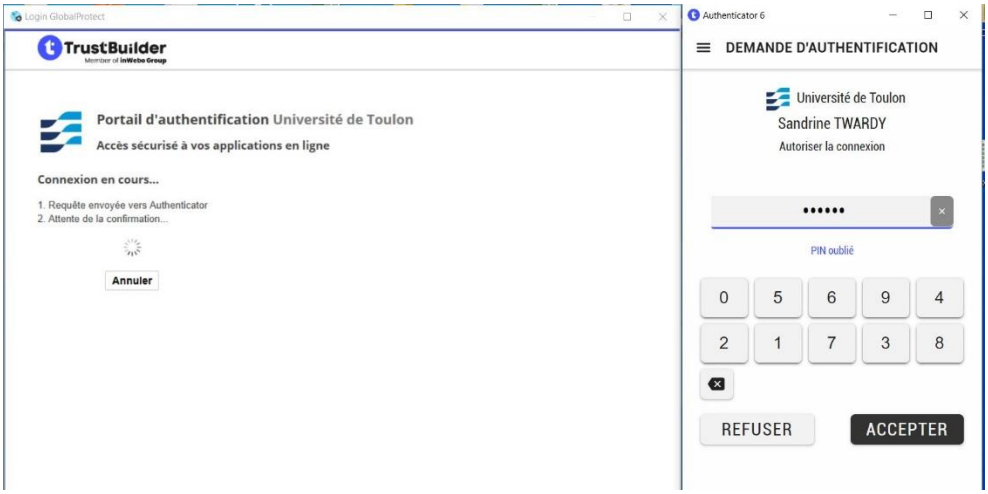
Indiquez votre login et mot de passe habituel, puis cliquez sur le bouter « Connecter ».

Attendez quelques instants qu'une fenêtre avec le logo TrustBuilder et le logo de l'université s'affiche.



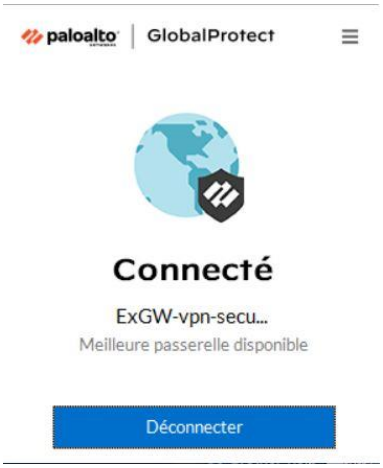
Indiquez dans cette fenêtre votre login dans le champ « Votre identifiant » et cliquez sur le bouton « Ok ».

L'application authenticator que vous avez préalablement installée et activé vous demande alors votre code PIN.



Indiquez votre code PIN et cliquez sur le bouton « Accepter »

Patientez quelques instants.



Vous êtes connecté.

INSTALLATION DU CLIENT GLOBALPROTECT SOUS LINUX

Les fichiers d'installation du client GlobalProtect pour Linux sont disponibles ici : http://nuxeo.univ-tln.fr/nuxeo/nxdoc/default/8eaba59b-baa5-44e9-be5d-807a707f0fb2/view_documents?tabIds=%3A&conversationId=0NXMAIN1

Attention : Pour les utilisateurs sous Debian, il est nécessaire d'être en version 12 et d'utiliser la version 6.1 du client GlobalProtect.

$sudo apt update

$sudo apt install libqt5webkit5

$sudo dpkg –i (chemin_de_votre_fichier)/GlobalProtect_UI_deb-6.1.4.0-711.deb

Pour toute demande de support concernant des clients Linux, veuillez-vous rapprocher de la personne responsable de la gestion de votre poste de travail.