MINISTÈRE
DE L'AGRICULTURE,
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE
Liberté
Égalité
Fraternité

Ordre de service d'action

Secrétariat général **Service du numérique** **Département de l'environnement de travail numérique des agents** **Direction générale de l'enseignement et de la recherche** **78 rue de Varenne** **75349 PARIS 07 SP** **0149554955**	**Instruction technique** **DGER/DAT/2026-342** **19/06/2026**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction n'abroge aucune instruction.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 3

Objet : Déploiement de la double authentification pour l'accès des agents de l'enseignement agricole au BNUM et au VPN

Destinataires d'exécution
DRAAF/DAAF Etablissements de l'enseignement agricole technique (publics et privés du temps plein)

Résumé : Depuis 2025, les menaces sur la cyber-sécurité ont significativement augmenté et l'enseignement agricole est touché comme l'ensemble des organisations publiques. Afin de renforcer la sécurité, la double authentification est rendue obligatoire pour l'accès au BNUM (dont messagerie) et au VPN selon un calendrier adapté à chaque outil. Cette évolution concerne l'enseignement agricole public et dans une moindre mesure les établissements privés (pour les seuls agents utilisant le BNUM)

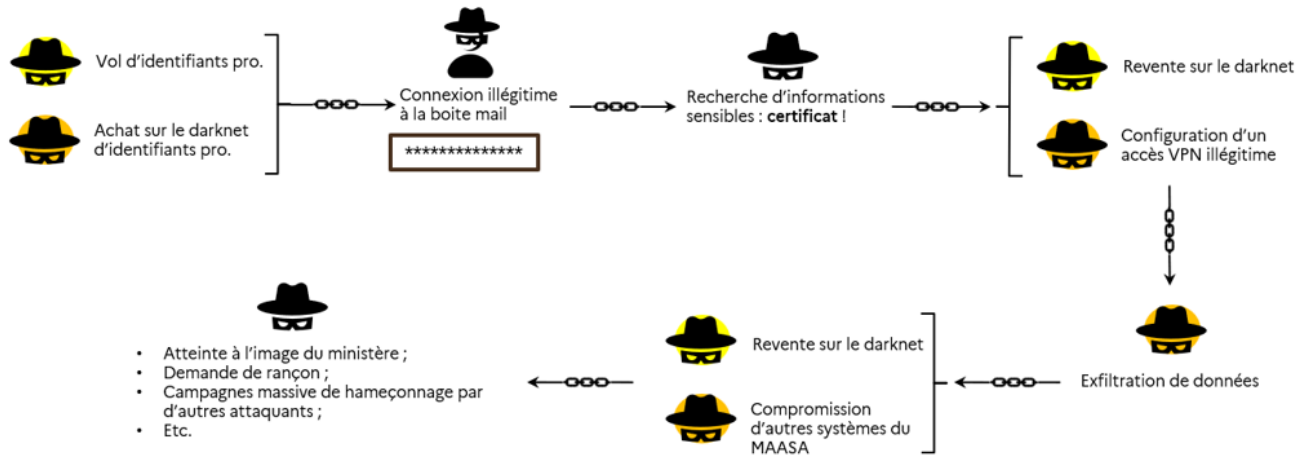
Table des matières

1. Contexte : des menaces cyber croissantes

Depuis 2025, les menaces sur la cyber-sécurité ont significativement augmenté et l'enseignement agricole est touché comme l'ensemble des organisations publiques. La sécurisation des outils et de leur accès est un enjeu majeur.

La principale modalité d'attaque relève de l'usurpation de comptes et de certificats qui rendent possible les intrusions puis des fuites de données. L'ensemble des agents est invité à la plus grande vigilance concernant tout évènement anormal dans le champ numérique (mails ou appels suspects, alertes antivirus, etc.).

Mode opératoire d'une attaque cyber



Dans ce contexte, la sécurité des accès aux VPN et au BNUM (messagerie, agenda…) va être renforcée grâce à la mise en place de l'authentification à deux facteurs, également appelée « double authentification ».

L'ensemble des agents du MAASA, en administration centrale, services déconcentrés et dans les établissements de l'enseignement agricole doivent ainsi activer la double authentification, selon le calendrier présenté en infra, pour pouvoir accéder aux VPN Mercure et Demeter ainsi qu'au BNUM (accès en ligne).

S'agissant de l'enseignement agricole, les personnels concernés sont quasi exclusivement ceux des établissements publics mais quelques agents dans l'enseignement agricole privé du temps plein peuvent être concernés :

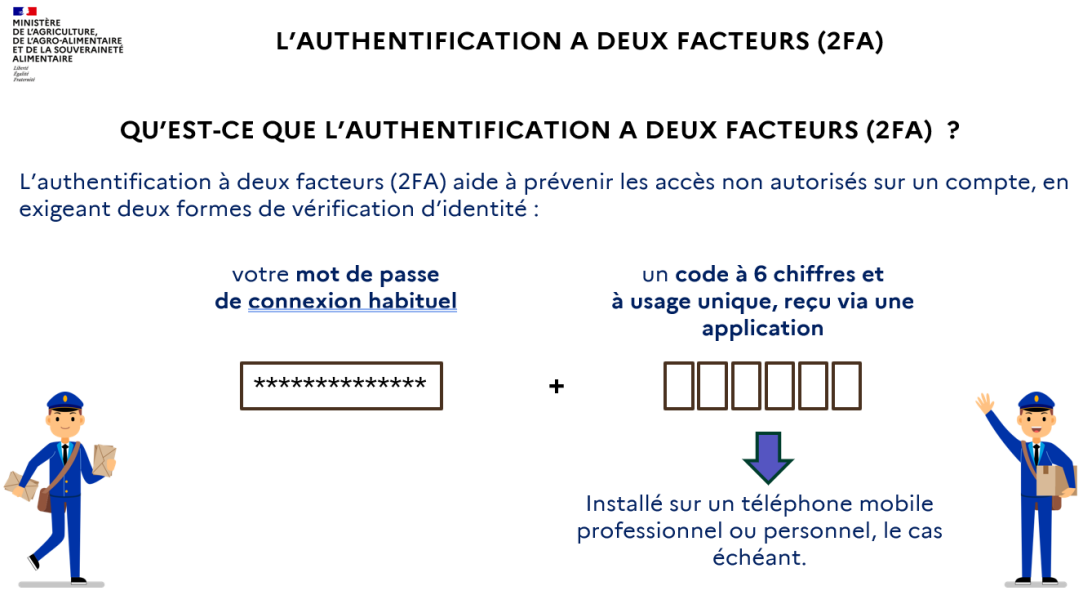
- VPN : l'utilisation des VPN Mercure et Demeter est fourni aux seuls agents en établissement public ;
- BNUM : la très grande majorité des agents publics en établissement privé utilisent la messagerie fournie par leur fédération. Les quelques agents d'établissements privés qui utilisent une adresse en « educagri » fournie par le ministère, à laquelle ils accèdent *via* le BNUM, doivent également passer à la double authentification pour maintenir cet accès.

2. Qu'est que la double authentification ?

Afin de renforcer la sécurité, le principe de la double authentification est de demander deux techniques de vérification de l'identité : lorsque vous vous connectez à un outil à partir d'internet (avec votre ordinateur ou votre smartphone), l'application vous demande, en complément du couple « identifiant/mot de passe » habituel, de saisir **un code de vérification**. Ce code est généré à partir d'une application dédiée que vous aurez préalablement installé sur votre smartphone.

L'application à installer sur votre portable est une application gratuite disponible dans les magasins d'application de tous ces téléphones. A titre d'illustration, « Free OTP » et « Google Authenticator » sont des applications gratuites très répandues.

Ce dispositif de double authentification devient progressivement la norme pour tous nos usages numériques et chacun d'entre nous l'utilise quotidiennement pour accéder à des services sensibles (Améli, site des impôts, accès à sa banque, sites de commerce en ligne, etc.).



L'application de double authentification est installée sur le téléphone professionnel de l'agent ou, s'il n'en possède pas, sur son téléphone personnel. Votre numéro personnel ne sera en aucun cas récupéré.

Le téléphone permet uniquement d'**ATTESTER VOTRE IDENTITE** et aucun autre usage n'est possible. **Une fois que la clé de sécurité a été créée lors de la première utilisation, plus aucun échange de données n'existe entre le téléphone et un quelconque autre dispositif.** Ainsi aucune connexion réseau n'est nécessaire : le code pourra même être fourni par le téléphone en « mode avion ».

L'utilisation de la double authentification est ainsi parfaitement respectueux de la vie privée : aucune donnée personnelle n'est échangée et le numéro de téléphone n'est pas utilisé. La CNIL recommande ainsi l'utilisation de la double authentification pour sécuriser les accès personnels.

Pour plus d'informations sur la double authentification, vous pouvez consulter les sites publics suivants :

- Site public « Cybermalveillance » : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification
- Article « Sécurité : utilisez l'authentification multifacteur pour vos comptes en ligne » sur le site de la CNIL

3. Calendrier de déploiement de la double authentification

La double authentification est déployée progressivement pour les VPN Mercure et Demeter ainsi que pour le BNUM selon le calendrier fourni ci-après.

L'interface du VPN ou du BNUM demandera à l'agent de fournir un code de vérification à usage unique qui sera disponible dans l'application de double authentification. A titre d'illustration, « Free OTP » et « Google Authenticator » sont des applications gratuites très répandues qui ont été testées et validées préalablement par le SNUM.

Les modes opératoires pour activer la double authentification sont fournis en annexe de la présente note :

- Annexe 1 : mode opératoire pour activer la double authentification sur le VPN Mercure
- Annexe 2 : mode opératoire pour activer la double authentification sur le BNUM.

Le mode opératoire pour activer la double authentification sur le VPN Demeter sera transmis dans le courant de l'été.

Si au terme du délai de déploiement vous n'avez pas installé la double authentification, vous devrez passer par votre assistance informatique de niveau 1 pour l'activer (cf. § 4 *« Accompagnement et assistance »*).

3.1. Le VPN Mercure

La double authentification sur le VPN Mercure est mise en place progressivement selon le calendrier suivant :

- **Lundi 8 juin 2026** : activation obligatoire de la double authentification pour les utilisateurs de la phase de test : agents du SNUM (au sein du secrétariat général MAASA) et de la DRAAF PACA ;
- **Lundi 22 juin 2026** : généralisation à l'ensemble des utilisateurs du service VPN Mercure (administration centrale, DRAAF/DAAF et enseignement agricole).

Les agents disposent d'un délai d'un mois à compter du 22 juin pour procéder à cette activation.

A compter de cette activation, la connexion nécessitera systématiquement, en complément du certificat, la saisie du code de vérification à usage unique fourni par l'application d'authentification installée sur le téléphone.

Jusqu'au 22 juillet 2026, vous pourrez continuer de vous connecter via votre mot de passe Agricoll si vous n'avez pas activé la double authentification. Ensuite, la connexion via la double authentification sera obligatoire. **Nous vous conseillons donc de la mettre en place sans attendre cette échéance**.

3.2. Le VPN Demeter

L'activation de la double authentification sur le VPN Demeter doit être activée par l'ensemble des utilisateurs à compter du lundi 21 septembre 2026. A compter de cette activation, la connexion nécessitera systématiquement, en complément du certificat, la saisie du code de vérification à usage unique fourni par l'application d'authentification installée sur le téléphone.

Les agents disposent d'un délai d'un mois pour procéder à cette activation.

Jusqu'au 21 octobre 2026, vous pourrez continuer de vous connecter via votre mot de passe Agricoll si vous n'avez pas activé la double authentification. Ensuite, la connexion via la double authentification sera obligatoire. **Nous vous conseillons donc de la mettre en place sans attendre cette échéance**.

3.3. Le BNUM

La double authentification sur le BNUM est mise en place progressivement selon le calendrier suivant :

- **Lundi 22 juin 2026** : activation obligatoire de la double authentification pour les utilisateurs des établissements de Nouvelle Aquitaine. Vous pourrez continuer de vous connecter via votre mot de passe Agricoll jusqu'à 22 juillet. Les agents qui n'auront pas activé la double authentification à cette date devront obligatoire basculer le 20 septembre, en même temps que ceux de l'ensemble des régions.
- **Jeudi 20 août 2026** : généralisation à l'ensemble des utilisateurs du BNUM (administration centrale, DRAAF/DAAF et enseignement agricole).

A compter de cette activation, la connexion nécessitera systématiquement, en complément du certificat, la saisie du code de vérification à usage unique fourni par l'application d'authentification installée sur le téléphone.

Jusqu'au 20 septembre 2026, vous pourrez continuer de vous connecter via votre mot de passe Agricoll si vous n'avez pas activé la double authentification. Ensuite, la connexion via la double authentification sera obligatoire. **Nous vous conseillons donc de la mettre en place sans attendre cette échéance.**

4. Accompagnement et assistance

Le déploiement de la double authentification dans l'enseignement agricole technique a fait l'objet d'une préfiguration avec un groupe utilisateur constitué de représentants des établissements et du niveau régional. Un accompagnement des agents sera assuré à chaque niveau.

Le passage à la double authentification s'appuie également sur :

- La réalisation de webinaires (disponibles ensuite en ligne) et de tutoriels à destination de l'ensemble des intéressés. Les dates des webinaires feront l'objet d'une communication par courriel.
- La mise à disposition de modes opératoires détaillant les modalités d'installation et d'usage de la double authentification (cf. annexes de la présente note)
- L'élaboration d'un circuit d'assistance dédié.

Les ressources mises à disposition seront mises à jour et compléter en fonction des retours terrain consécutives au déploiement de la double authentification.

4.1. Les référents en établissements

Chaque établissement de l'enseignement agricole public désigne un référent « double authentification ». Ce référent peut être, par exemple, un enseignant TIM, un technicien TFR identifié comme relai informatique en interne, un GLA ou toute autre personne désignée par la direction de l'établissement.

Le nom du référent désigné est transmis par l'établissement au DRTIC de la région.

En l'absence d'agent identifié, les enseignant TIM, les technicien TFR et les GLA de chaque établissement seront rendus destinataires des actualités sur la double authentification.

4.2. Le groupe utilisateur

Un groupe utilisateur « double authentification » a été constitué pour préparer ce déploiement. Il est composé de représentants des directeurs d'établissement, des secrétaires généraux, d'enseignants, de DRTIC, sous pilotage de la DGER avec l'appui du SNUM.

Il sera ponctuellement réuni sur les questions relatives à la sécurisation des accès des agents des établissements et notamment sur le retour d'expérience dans le cadre du passage à la double authentification.

4.3. Le circuit d'assistance

Le circuit d'assistance dans le cadre du déploiement de la double authentification est détaillé en annexe 3 pour le VPN MERCURE et le BNUM. Le circuit d'assistance pour DEMETER sera précisé dans le courant de l'été.

5. Cas particuliers d'assistance

- ***Activation de la double authentification impossible***

Les agents qui ne pourraient pas activer la double authentification ne pourront pas accéder au dehors du réseau de l'Etat à leurs ressources.

Les agents qui n'ont pas la possibilité de se connecter aux réseaux ministériels et qui ne peuvent pas (personnels en situation de handicap ou d'illettrisme ou choix personnel) le dispositif de double authentification devront être recensés par les directeurs d'établissement et transmis à l'autorité académique (avec le motif), via le DRTIC, qui en informera la DGER.

Une solution adaptée sera recherchée dans la mesure possible avec l'établissement, l'autorité académique et la région concernée.

- ***Casse, perte, vol du smartphone***

En cas de casse, perte ou vol du téléphone équipé de l'application de double authentification, l'agent doit avertir son assistance de proximité (voir annexe 3) et, à défaut, son DRTIC, pour pouvoir activer la double authentification sur un nouveau moyen.

6. Responsabilité des agents en cas de piratage

A l'issue de la période d'activation de la double authentification, si un agent est victime d'une cyberattaque, sa responsabilité, en tant que victime, ne sera pas engagée. Cela suppose toutefois que l'agent n'ait pas délibérément contribué à l'attaque, ni commis de négligence caractérisée.

Le directeur général adjoint
de l'enseignement et de la recherche

Luc MAURER

Le chef du service numérique

Christophe BOUTONNET ID
2026.06.19 11:27:28
+02'00'

Christophe BOUTONNET

MINISTÈRE
DE L'AGRICULTURE,
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

Mode opératoire

Mise en place de l'authentification à deux facteurs pour le VPN Mercure V2 pour les agents des établissements agricoles techniques publics

Secrétariat général
Service du Numérique

Version 1.0 du 17/06/2026

Objet du document :

Ce mode opératoire détaille la procédure afin de mettre en œuvre l'authentification à deux facteurs (ou double authentification) pour se connecter à partir de son ordinateur au VPN Mercure V2 du MAASA.
Ce mode opératoire est adapté pour les agents en établissements agricoles techniques publics.

Contexte :

Dans un contexte de risque accentué en matière de cybersécurité, le ministère souhaite renforcer la sécurité de ses systèmes d'information, et en particulier les accès via VPN.

Pour cela, les connexions au VPN Mercure V2 devront s'appuyer sur deux facteurs :
- le certificat installé sur le poste de travail,
- un code d'accès à 6 chiffres qui est envoyé sur un équipement de confiance différent : le smartphone. En cas de difficulté rencontrée dans la mise en place de cette modalité, et **pour une durée limitée**, il sera possible d'utiliser son mot de passe Agricoll.

Le déploiement de ces modalités est prévu en 2 phases :
- 22/06/2026 : une expérimentation en région Nouvelle-Aquitaine.
- 20/08/2026 : la généralisation à l'ensemble des établissements agricoles techniques publics.

Prérequis :

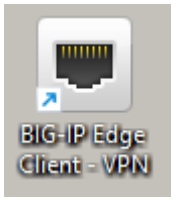
Pour pouvoir mettre en place la double authentification par mot de passe à usage unique, basé sur le temps, et généré automatiquement (TOTP – Time based One Time Password), il est nécessaire d'avoir installé sur son équipement de confiance une application dédiée.

Google Authenticator, **FreeOTP** *ou* ***FreeOTP+*** sont les plus communément utilisées et ont fait l'objet de tests préalables. Nous vous conseillons d'utiliser l'une ou l'autre de ces applications.
NB : Vous pouvez utiliser la même application d'authentification pour plusieurs usages (Resana, BNum, etc…).

Pour télécharger une application de double authentification : rendez-vous sur *Goople Play* pour Androïd ou l'*App Store* pour iOS, et procédez à l'installation en suivant les instructions.
Cf en Annexe si besoin de précisions pour cette installation.

Mode opératoire :

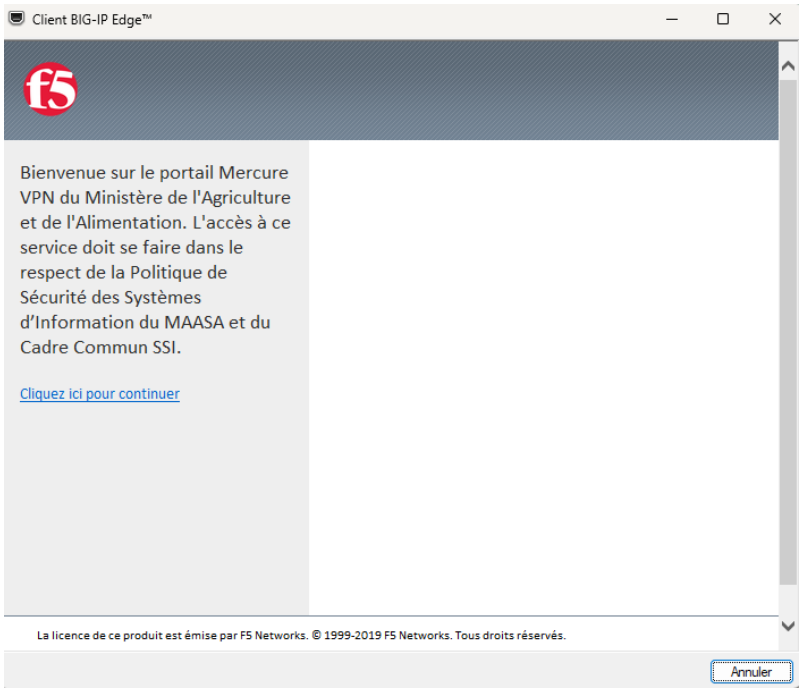
Pour se connecter au VPN, double-cliquez sur le client BIG-IP installé sur le poste de travail.



La fenêtre d'invitation à se connecter apparaît :

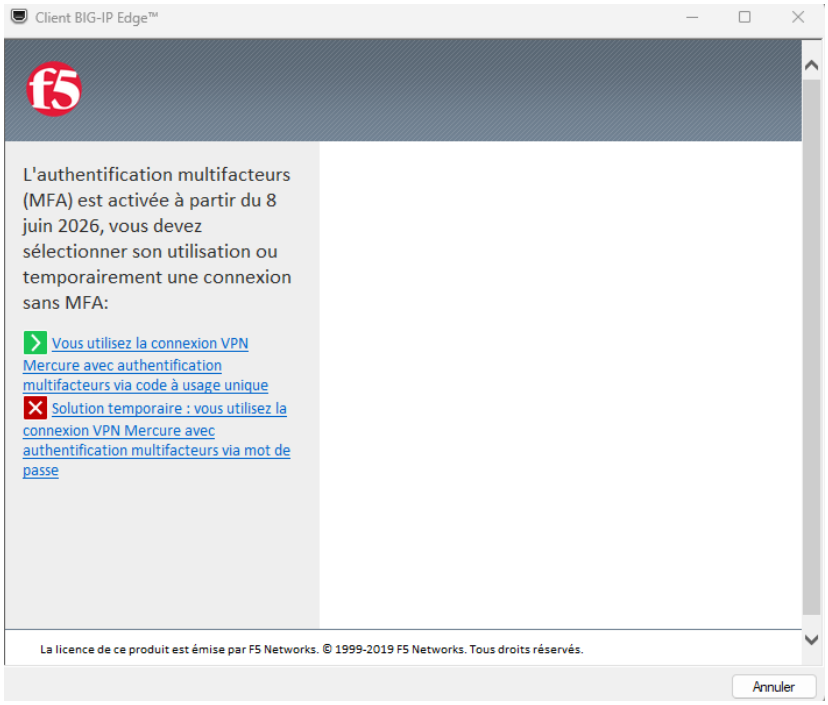
Sélectionnez « Connecter ».

La fenêtre ci-contre apparaît :



Vous avez alors le choix entre « Cliquez ici pour continuer » ou « Annuler », suivant que vous souhaitez poursuivre ou non, la procédure de connexion au VPN Mercure V2 (qui implique l'acceptation des conditions indiquées sur la capture d'écran ci-dessus).

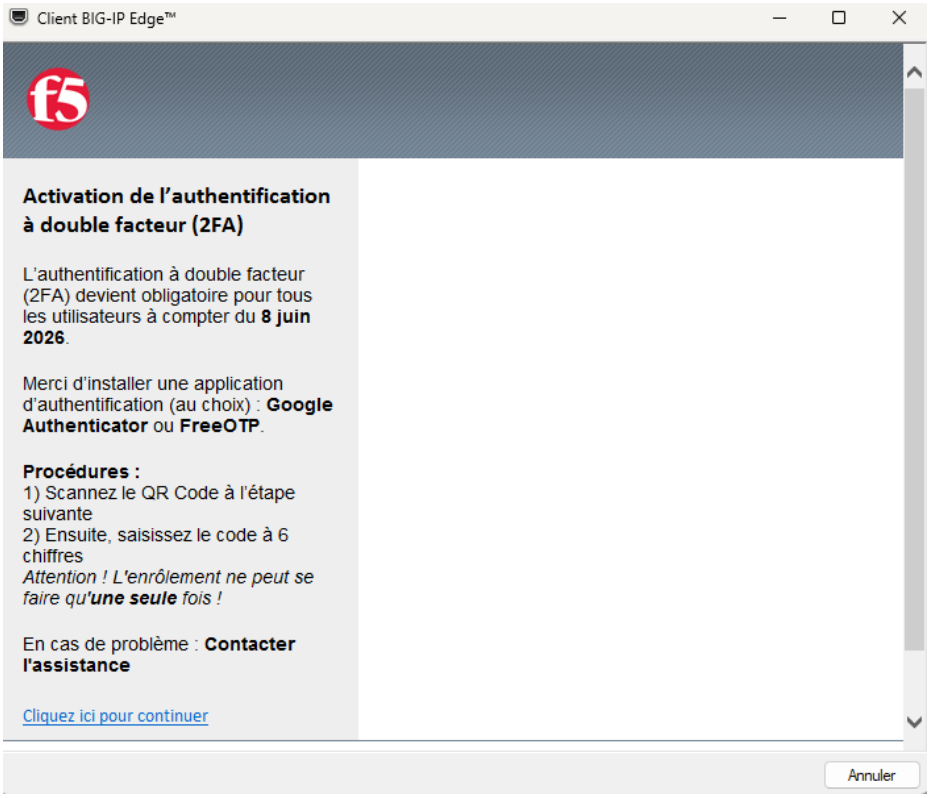
Durant la phase provisoire, la fenêtre suivante apparaitra à chaque connexion :



Elle permet de choisir le mode de connexion :

- **Si vous choisissez la 1ère option**

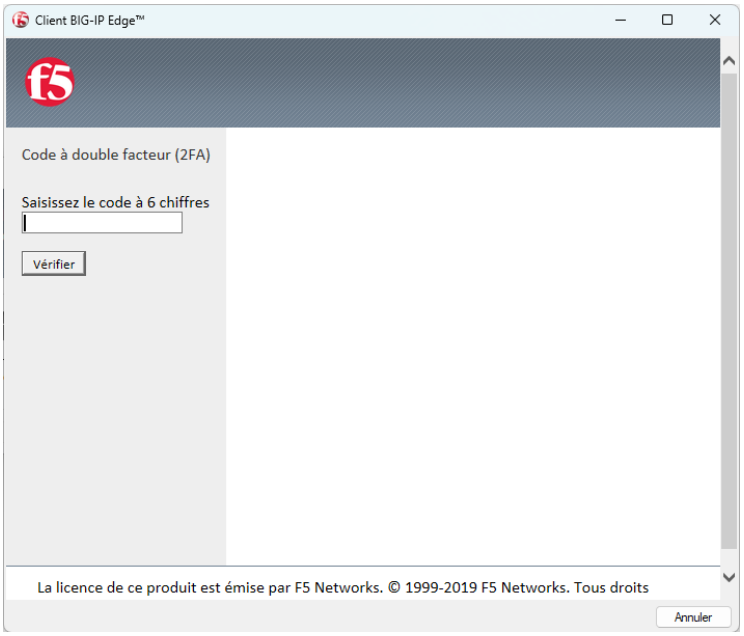
« Vous utilisez la connexion VPN Mercure avec authentification multifacteurs via code à usage unique »
La fenêtre suivante apparaît la première fois :



Après avoir choisi « cliquez ici pour continuer », scannez le QR-code qui s'affiche avec votre smartphone, ou saisissez le code secret affiché, dans l'application de TOTP :

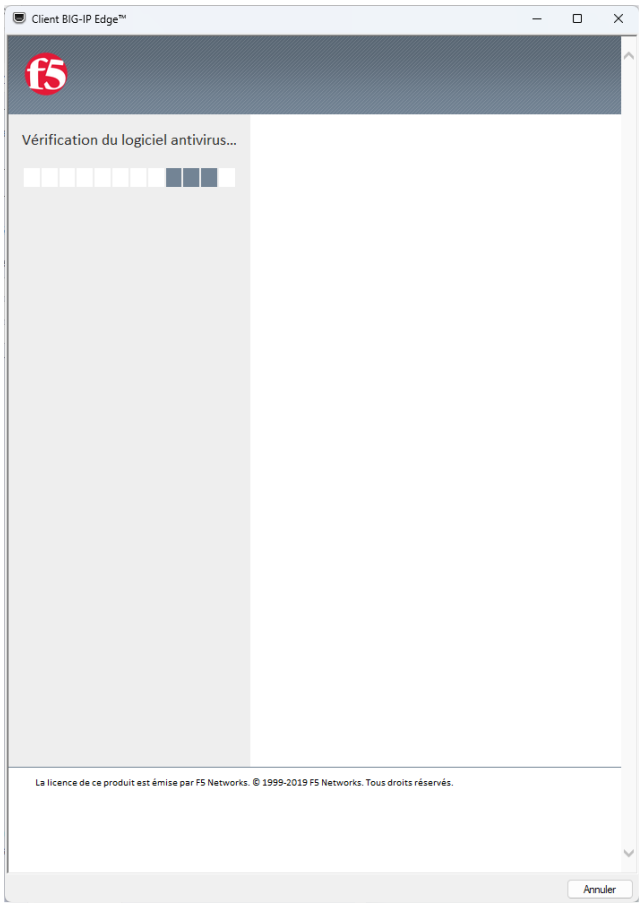
Votre smartphone est alors enrôlé, et l'application de TOTP délivre un code à 6 chiffres dédié au VPN, qui change régulièrement dans le temps.

La fenêtre suivante apparaît alors à chaque nouvelle connexion au VPN :



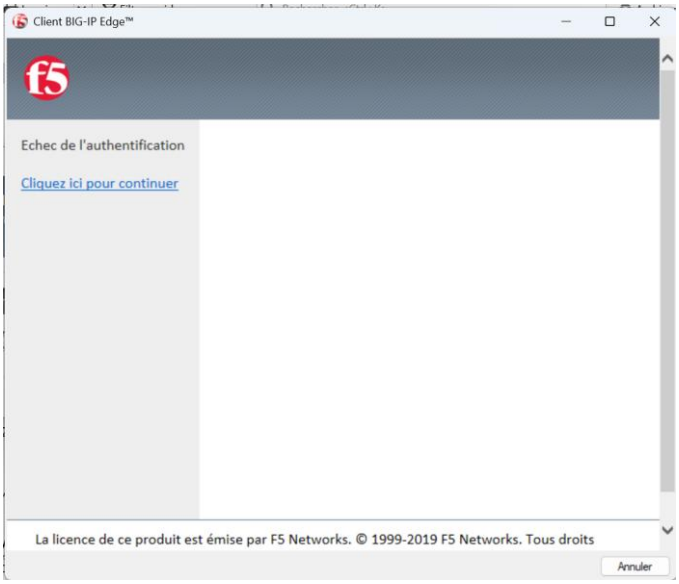
Il est nécessaire d'y saisir le code à 6 chiffres qui s'affiche dans l'application de TOTP.
Puis cliquez sur « Vérifier ».

Les fenêtres suivantes se succèdent :



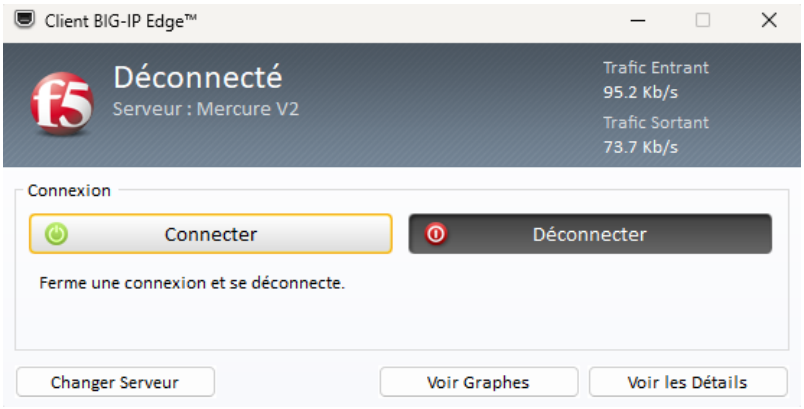
Et la connexion au VPN se finalise.

En cas de code incorrect, le message suivant s'affiche.



En ce cas, il est nécessaire de cliquer sur « Annuler ».

Et la fenêtre suivante vous informe de l'état « déconnecté »

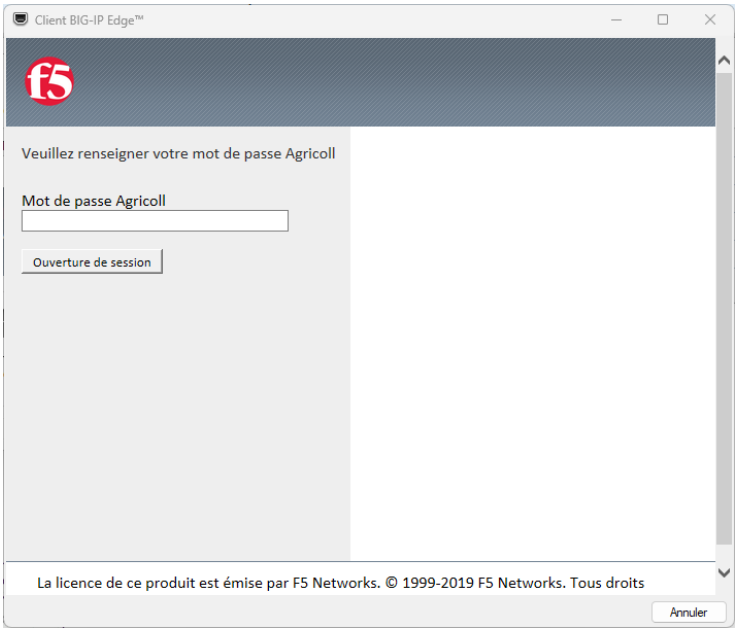


Pour faire une nouvelle tentative, il faut alors relancer le client BIG IP f5.

- **Si vous choisissez la 2ème option :**

« Solution temporaire : vous utilisez la connexion VPN Mercure avec authentification multifacteurs via mot de passe »

Alors il faudra saisir votre mot de passe Agricoll, puis cliquer sur « ouverture de session » comme ci-dessous :



Plusieurs fenêtres se succèdent, et la connexion au VPN se finalise.

Support :

En cas de difficulté dans la procédure de double authentification, contactez l'assistance utilisateurs :

- Administration centrale : Pastel au 01 49 55 59 00
- Services déconcentrés : assistance informatique de proximité.

Questions/Réponses :

Comment choisir entre FreeOTP, FreeOTP+ et Google Authenticator ?

Ces applications se valent :

- FreeOTP et FreeOTP+ imposent l'usage d'un mot de passe maître, à ne jamais oublier, mais permet de sauvegarder votre clé d'authentification à deux facteurs hors de votre smartphone et de la restaurer sur un nouvel appareil en cas de perte.
- Google Authenticator ne propose pas de sauvegarde : il permet seulement de transférer la clé vers un nouvel appareil si l'ancien est encore fonctionnel.

J'utilise déjà une autre application pour gérer des authentifications double facteurs. Suis-je obligé d'installer une des applications proposées ?

Nous proposons ces applications, pour simplifier le choix parmi toutes celles disponibles sur les stores Google, Samsung ou iPhone ; mais si vous utilisez déjà une autre application, vous pouvez la conserver pour l'authentification à deux facteurs du VPN Mercure V2.
NB : Seules les applications proposées ont été testées par le SNum pour le VPN Mercure V2.

Je n'ai pas de smartphone professionnel comment mettre en place l'authentification à double facteur ?

Si vous disposez d'un smartphone personnel, vous pouvez utiliser ce dernier. Aucun lien permanent n'est établi entre l'application d'authentification à deux facteurs de votre smartphone et le client VPN BIG IP f5.
Cependant, **si vous ne souhaitez pas utiliser votre smartphone personnel**, et **si vous ne disposez pas de smartphone professionnel**, alors vous ne pourrez pas activer la double authentification. Cela bloquera donc votre accès au VPN Mercure V2, qui vous permet d'accéder au système d'information du MAASA en télétravail.

J'ai un smartphone professionnel mais l'installation d'application n'est pas autorisée, comment mettre en place l'authentification à double facteur ?

Si vous ne pouvez pas installer d'application sur votre smartphone professionnel, nous vous invitons à solliciter votre assistance informatique de proximité pour permettre cette installation. Dans cette attente vous pouvez utiliser votre téléphone personnel.

Installation de *Google Authentification* ou *FreeOTP :*

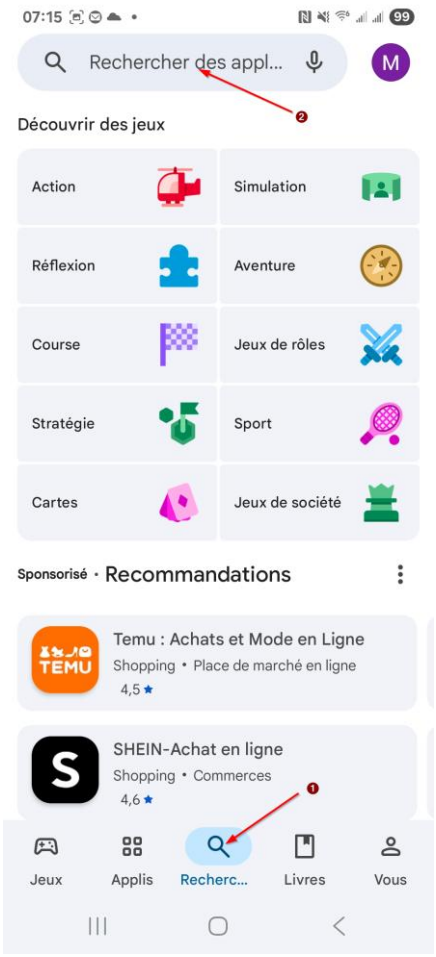
Mode opératoire pour un smartphone *Androïd*

Vous devez, dans un premier temps, installer sur votre téléphone portable, l'une des applications suivantes (cela nécessite de disposer d'un compte Google) :

- Google Authentificator
- FreeOTP.

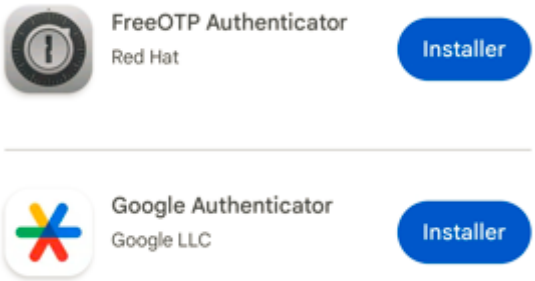
Pour ce faire, rendez-vous sur le Play Store :

Recherchez l'application FreeOTP ou Google Authentificator puis l'installer.

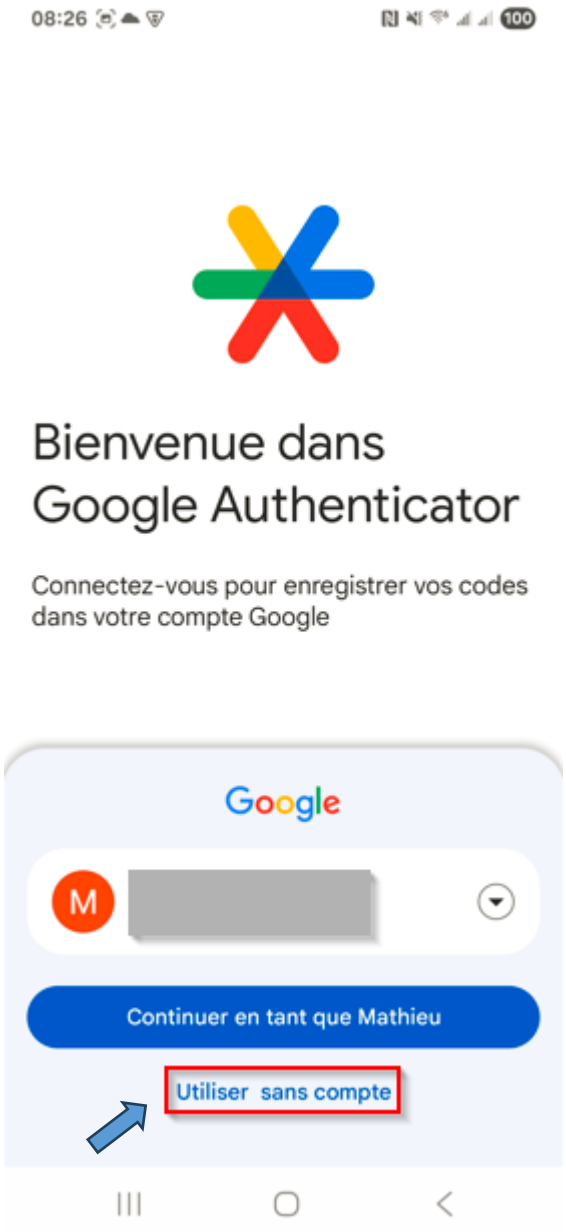


FreeOTP

Google Authentificator



Premières exécutions :

FreeOTP : un mot de passe composé que de chiffres devra être configuré	Google Authentificator
	

MINISTÈRE
DE L'AGRICULTURE,
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

Mode opératoire

Mise en place de l'authentification à deux facteurs sur le BNUM pour les agents en établissements agricoles techniques publics

Secrétariat général
Service du numérique / Département ETNA

Version 1.0 du 17/06/2026

Objet du document :

Ce mode opératoire détaille la procédure afin de mettre en œuvre l'authentification à deux facteurs (ou double authentification) lorsque l'on se connecte au BNUM directement depuis internet à partir de son ordinateur ou de son smartphone.

Ce mode opératoire est adapté pour les agents en établissements agricoles techniques publics.

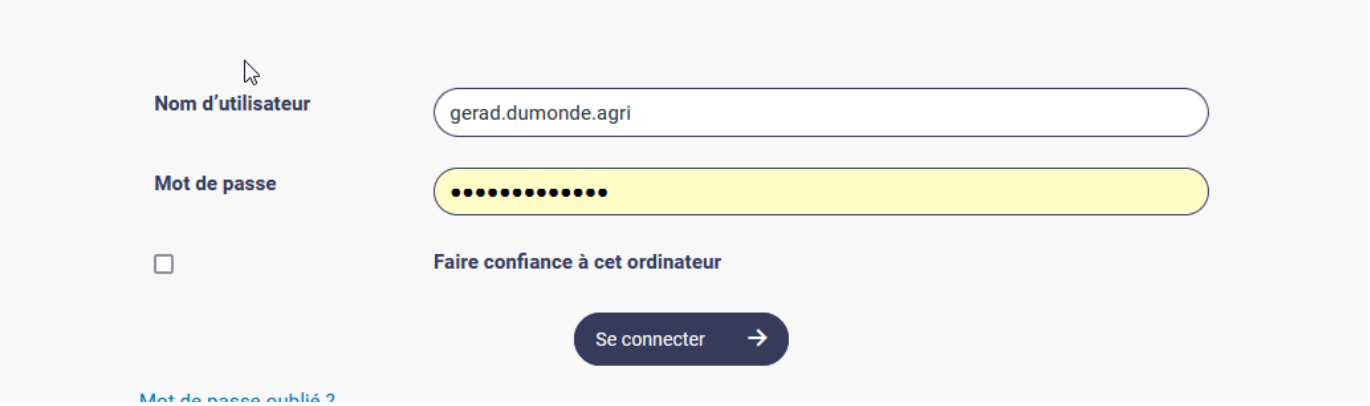
Contexte :

Dans un contexte de risque accentué en matière de cybersécurité, le ministère souhaite renforcer la sécurité de ses systèmes d'information, et en particulier les applications qui sont accessibles depuis l'internet. C'est le cas de la messagerie électronique accessible depuis n'importe quel matériel (ordinateur personnel, smartphone…) en utilisant le site appelé BNUM via un navigateur internet.

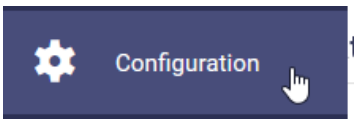
L'authentification à deux facteurs permet donc de se connecter au BNUM depuis Internet en s'appuyant sur deux facteurs :
- votre Nom d'utilisateur et mot de passe
- un code d'accès à 6 chiffres qui vous est envoyé sur un appareil différent, votre smartphone

Mode opératoire :

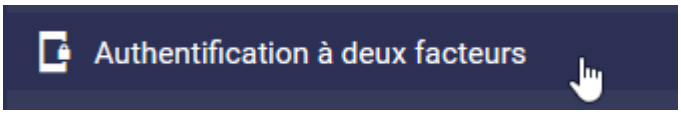
- Connectez votre ordinateur sur Internet, et ouvrez le BNUM depuis votre navigateur à l'adresse suivante : https://bnum.din.gouv.fr/
- Sur la page d'accueil, saisissez :
    - Votre nom d'utilisateur (sous la forme prenom.nom.agri ou prenom.nom@agriculture.fr)
    - Votre mot de passe : il s'agit du mot de passe Agricoll d'accès à votre messagerie



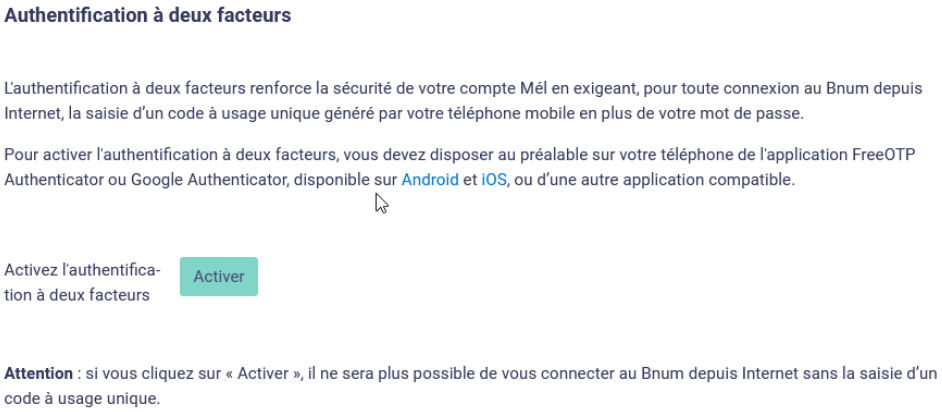
- Lorsque le BNUM est ouvert, cliquez sur l'option « **Configuration** » (en bas à gauche du Menu)



- Cliquez ensuite sur « **Authentification à deux facteurs** »



- La page suivante s'affiche :

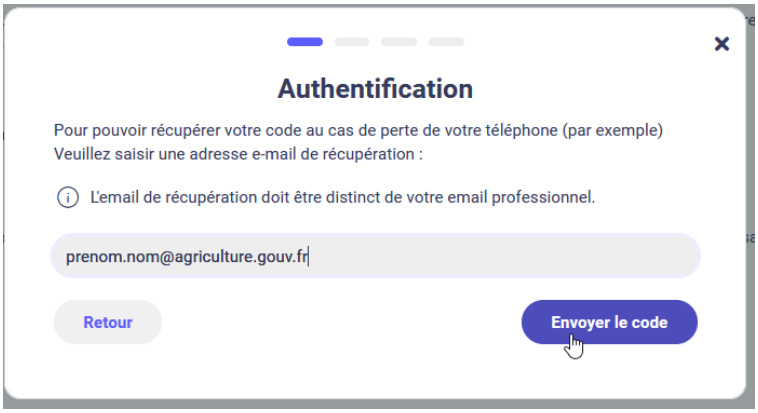


- Cliquez sur « **Activer** » pour lancer le processus de double authentification

- La page suivante s'affiche :

- Cliquez sur « **Configurer maintenant** »

- La page suivante s'affiche :



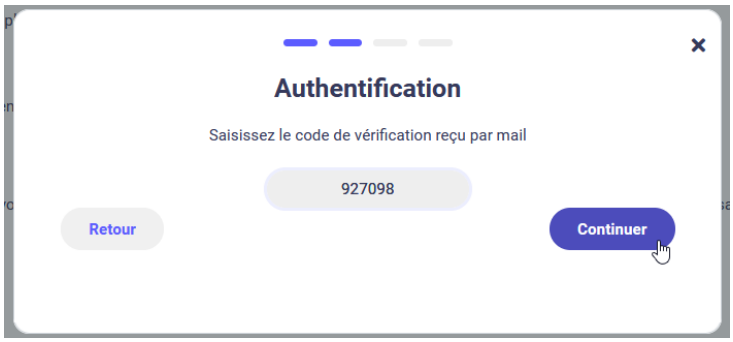
- **Contrairement au message qui est affiché, et pour des questions de sécurité,** saisissez **votre adresse mail professionnelle** sur laquelle vous pourrez récupérer votre code en cas de perte de votre téléphone.

- Cliquez sur « **Envoyer le code** »

- Connectez-vous à votre messagerie. Un mail vous est adressé contenant un code

- Saisissez ce code sur l'écran suivant

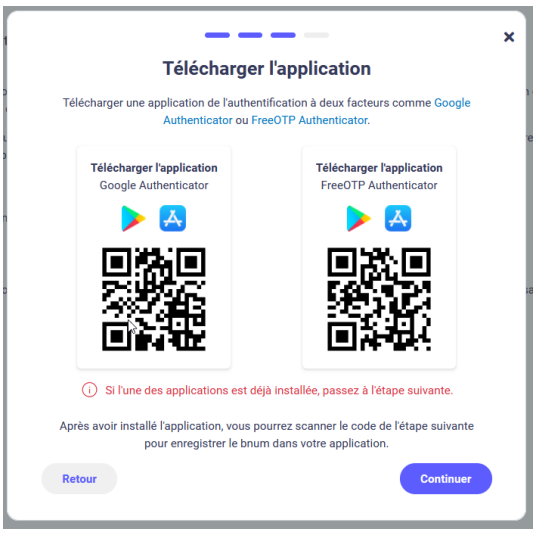
- Cliquez sur « **Continuer** »



- L'écran suivant s'affiche

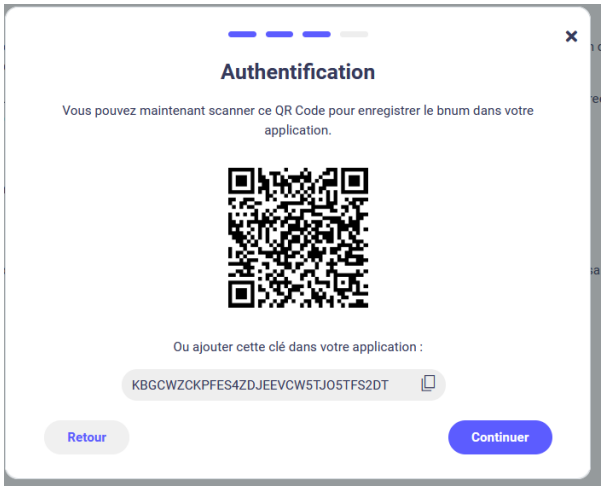
- Avec votre smartphone, scannez l'un des deux Q-R-Code afin de télécharger soit « ***Google Authenticator*** », soit « **FreeOTP Authenticator** ».
  Vous pouvez choisir toute autre application compatible.

- Procédez à l'installation de l'une de ces deux applications (ou toute autre compatible) sur votre smartphone en suivant les instructions.
- Une fois l'installation terminée cliquer sur « **Continuer** »

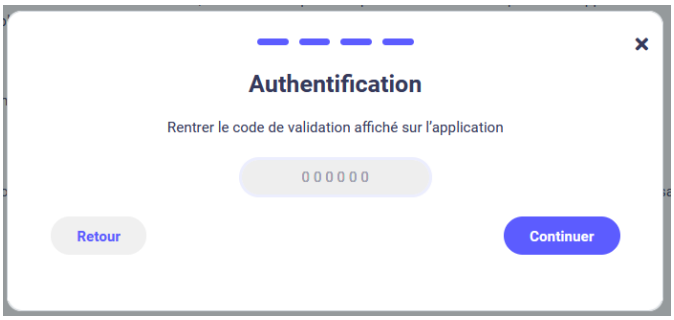


NB : Si vous disposez déjà d'une application de ce type sur votre smartphone, cliquez sur **« Continuer »**

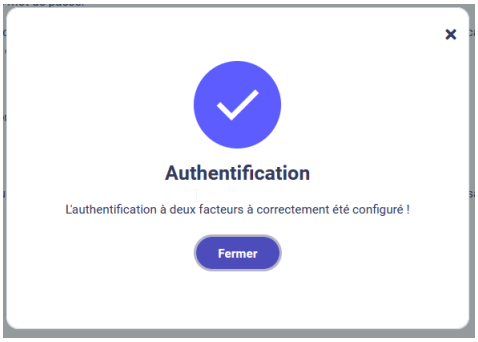
- L'écran suivant s'affiche :
- **Avec votre smartphone**, ouvrez l'application que vous venez de télécharger et Scannez ce Q-R Code (ou saisissez la clé qui s'inscrit sur l'écran de droite). L'application à double authentification va immédiatement générer un code aléatoire à 6 chiffres toutes les minutes.
- Cliquez sur le bouton « Continuer »



- L'écran suivant s'affiche :
- Saisissez le code généré par l'application de votre smartphone
- Cliquez sur « **continuer** »



- L'écran suivant s'affiche :
- Cliquez sur « **Fermer** ». Vous êtes connecté au BNUM



Questions/Réponses :

Comment choisir entre FreeOTP et Google Authenticator ?

Les deux applications se valent :

- FreeOTP impose l'usage d'un mot de passe maître, à ne jamais oublier, mais permet de sauvegarder votre clé d'authentification à deux facteurs hors de votre smartphone et de la restaurer sur un nouvel appareil en cas de perte.
- Google Authenticator ne propose pas de sauvegarde : il permet seulement de transférer la clé vers un nouvel appareil si l'ancien est encore fonctionnel.

J'utilise déjà une autre application pour gérer des authentifications double facteurs. Suis-je obligé d'installer une des deux applications proposées ?

Nous proposons deux applications pour simplifier le choix parmi toutes celles disponibles sur les stores Google, Samsung ou iPhone ; mais si vous utilisez déjà une autre application, vous pouvez la conserver pour l'authentification à deux facteurs du Bnum.

Je n'ai pas de smartphone professionnel comment mettre en place l'authentification à double facteur ?

Si vous disposez d'un smartphone personnel, vous pouvez utiliser ce dernier. Aucun lien permanent n'est établi entre l'application d'authentification à deux facteurs de votre smartphone et le Bnum : l'application mémorise seulement une clé générée par la messagerie, sans connaître ni votre identifiant de messagerie, ni votre mot de passe. Une fois initialisée, elle peut générer les codes d'authentification sans données mobiles ni Wi-Fi.

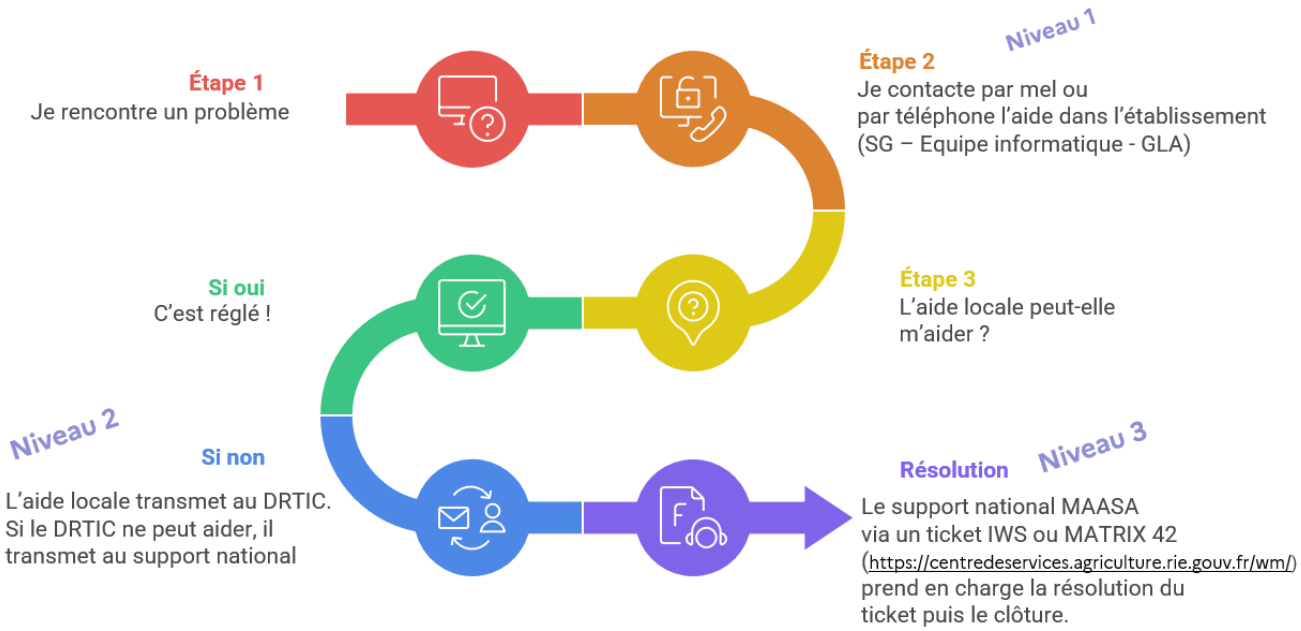
J'ai un smartphone professionnel mais l'installation d'application n'est pas autorisée, comment mettre en place l'authentification à double facteur ?

Si vous ne pouvez pas installer d'application sur votre smartphone professionnel, nous vous invitons à solliciter votre assistance informatique de proximité pour permettre cette installation. Dans cette attente vous pouvez utiliser votre téléphone personnel.

Annexe 3 – La double authentification : 3 niveaux d'assistance

Processus d'assistance VPN

En cas de difficulté dans l'activation de la double authentification et **après consultation des modes d'emploi et des webinaires en ligne**, une assistance structurée comme suit est assurée :



Processus d'assistance BNUM

En cas de difficulté dans l'activation de la double authentification et **après consultation des modes d'emploi et des webinaires en ligne**, une assistance structurée comme suit est assurée :