

Accès distants sécurisés - VPN

Accès distants sécurisés - VPN

Version : 1.0.1

Date : Janvier 2022

Éditeur : Université de Strasbourg - Direction du numérique

Auteur(s) : Rédacteurs : Cédric Freyermuth

Contributeurs : Marina Heimburger

Copyright : Université de Strasbourg

TABLE DES MATIÈRES

Introduction	3
1. Pourquoi / Comment ?	4
2. Configuration pour un PC Windows	5
3. Configuration pour un appareil Apple	13
3.1. Configuration pour MacOS Apple	13
3.2. Configuration pour iPhone, iPad	27
4. Configuration pour un appareil Android	41
5. Configuration pour un appareil Linux	53
5.1. Via le terminal de commande	53
5.2. Via l'interface graphique	57
6. Assistance	63
7. Remarques, suggestions	73

INTRODUCTION

De quoi s'agit-il ?

Le VPN, ou « Virtual Private Network » est un service qui permet à un ordinateur, depuis chez vous ou en dehors de l'université, de se connecter et d'être vu comme une machine interne au réseau universitaire.

Public concerné

Le VPN de l'Université de Strasbourg (et du réseau Osiris) est accessible pour tous ses personnels techniques, administratifs, d'enseignement et de recherche. Il est également ouvert pour les étudiants.

Objet

Ce guide a pour objectifs d'accompagner à l'installation et à la configuration du client (programme) permettant l'accès au service.

Arrêt de la plate-forme "Cisco"

À compter du 1er janvier 2022, le service VPN "Cisco" ne sera plus disponible. Le nouveau VPN, "Fortinet", proposée en complément depuis le printemps 2020, prend entièrement le relai.

Ce guide décrit l'installation et la configuration du client Fortinet.



Télécharger la version PDF de cette documentation (cf.  [guidePapier](#))

1. POURQUOI / COMMENT ?

Quand installer le VPN ?

Si vous faites partie des utilisateurs qui ont besoin d'accéder aux **espaces numériques et applications qui ne sont pas accessibles depuis une connexion extérieure à l'université.**

Les personnes prioritairement concernées sont les **utilisateurs ayant un profil spécifique** (VPN-ADM, VPN-Lab et VPN-Lab+ ...) qui **ont accès à des services ou applications particulières** (répertoire partagé de service, ADE, Apogée...).



Cependant pour accéder à la plupart des services et applications numériques de l'université (Ernest, Partage, Moodle, Seafile ...) le VPN n'est pas nécessaire.

Comment ça fonctionne ?

Nous mettons à disposition une plateforme VPN Osiris : **Fortinet**.

- Un programme (client) doit être **installé puis configuré** sur votre ordinateur pour pouvoir faire fonctionner ce service.
- Ces deux opérations sont simples, vous trouverez à la suite de ce texte un **guide de mise en œuvre**.

2. CONFIGURATION POUR UN PC WINDOWS

1. Télécharger et installer le client

Prérequis

Si votre poste est géré par la Direction du numérique, cette étape n'est pas nécessaire, le programme est déjà installé. Vous pouvez passer à l'étape 2 « Configurer votre client Fortinet Unistra »



Système d'exploitation compatible: Microsoft Windows 11 (64-bit), 10 (32-bit and 64-bit), 8.1 (32-bit and 64-bit)

1 Sur votre navigateur internet, rendez-vous sur <https://vpn.unistra.fr>.



Attention : Le navigateur Chrome n'est pas compatible avec cette procédure. Vous pouvez utiliser Firefox, Edge, Safari ou autres.

2 Authentifiez-vous avec votre compte Unistra.

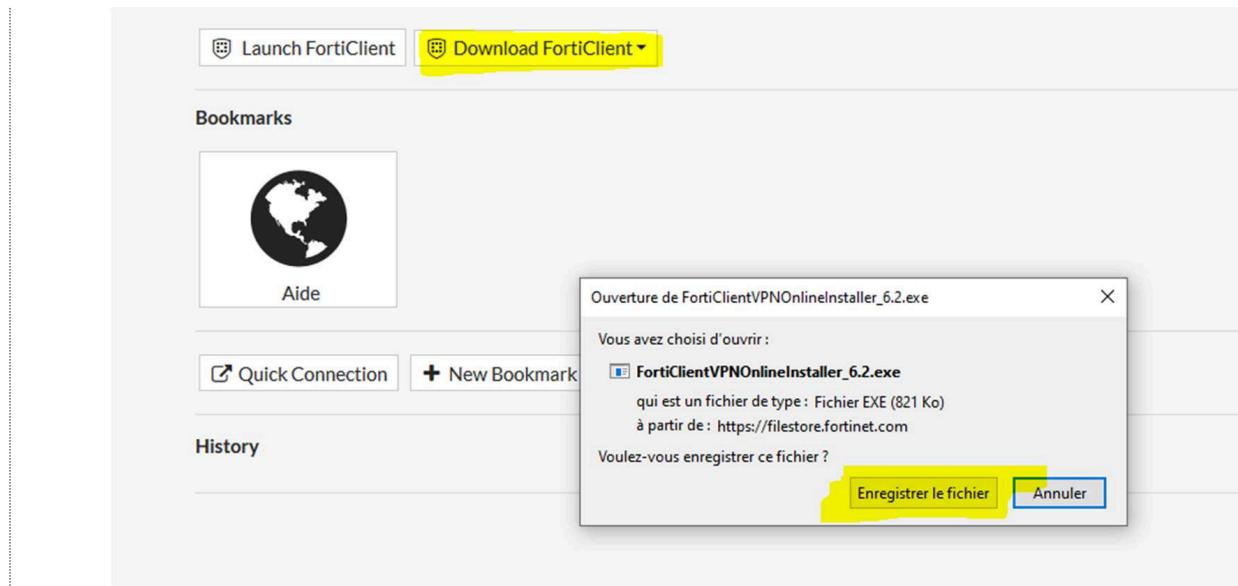


Vous pouvez retrouver votre compte unistra sur <https://quisuisje.unistra.fr>

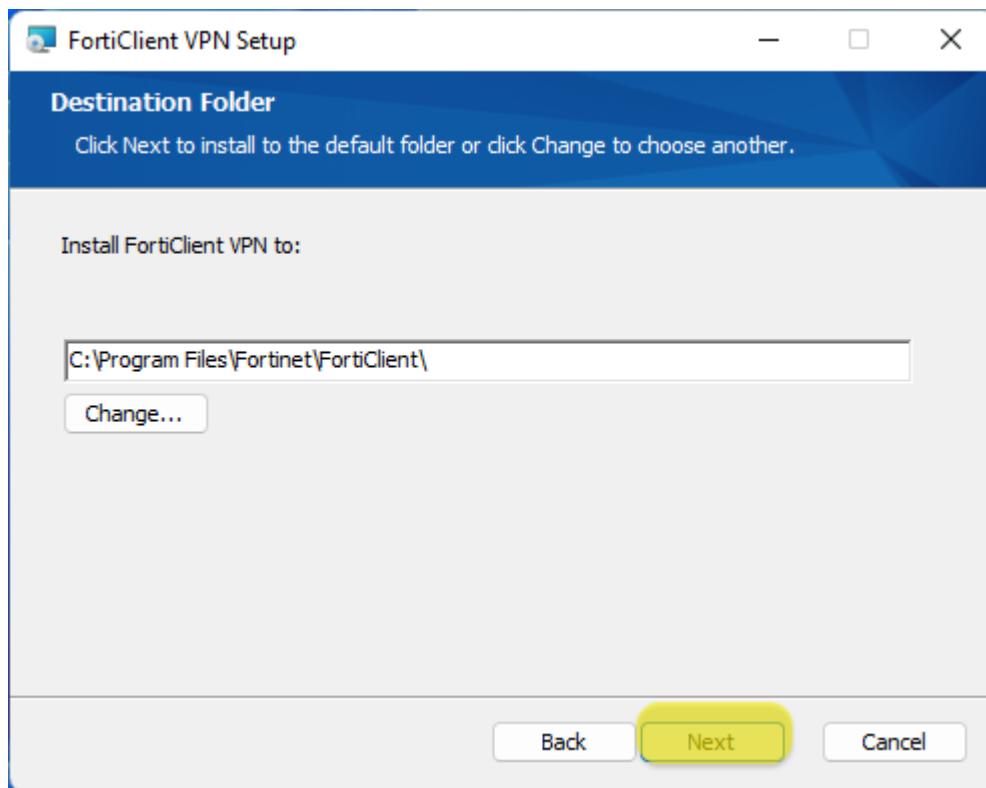


Vous arrivez sur le portail Fortinet Unistra, il vous permettra de télécharger le fichier d'installation du client.

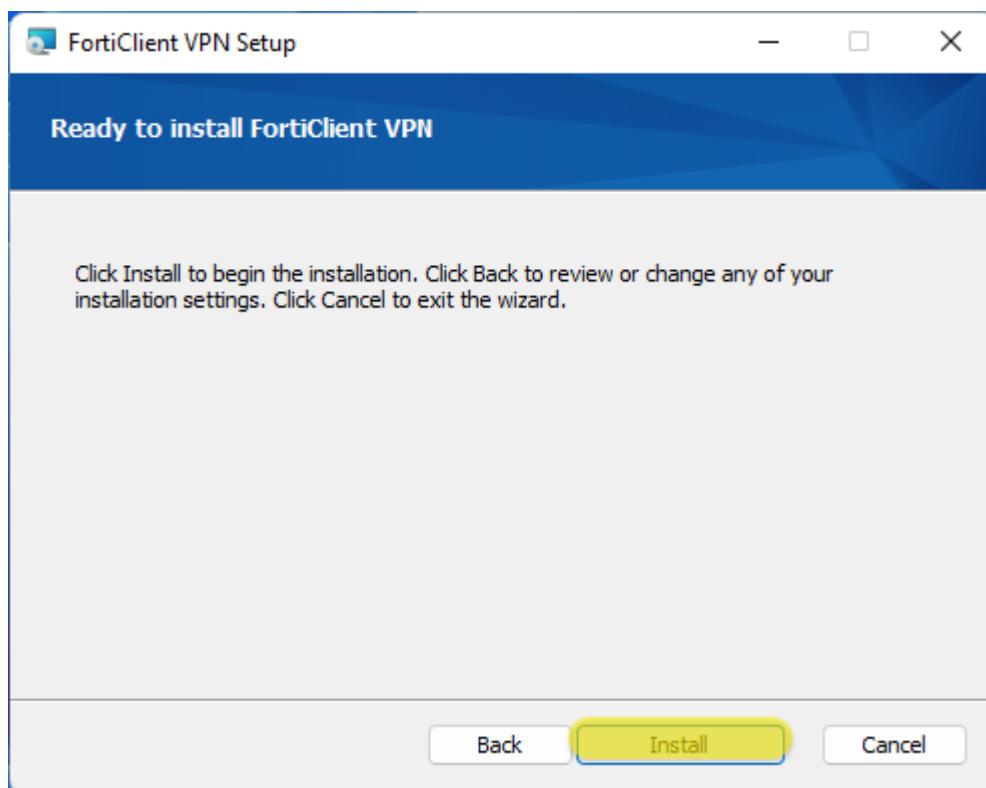
3 Choisissez votre système d'exploitation parmi la liste (iOS, Android, **Windows**, Mac) dans le menu  Download Forticlient.

4 Cliquez sur Enregistrer .**5 Une fois le téléchargement terminé, lancez l'exécutable **FortiClientVPNSetup.exe**.****6 Acceptez les conditions d'utilisations et cliquez sur **Next** .**

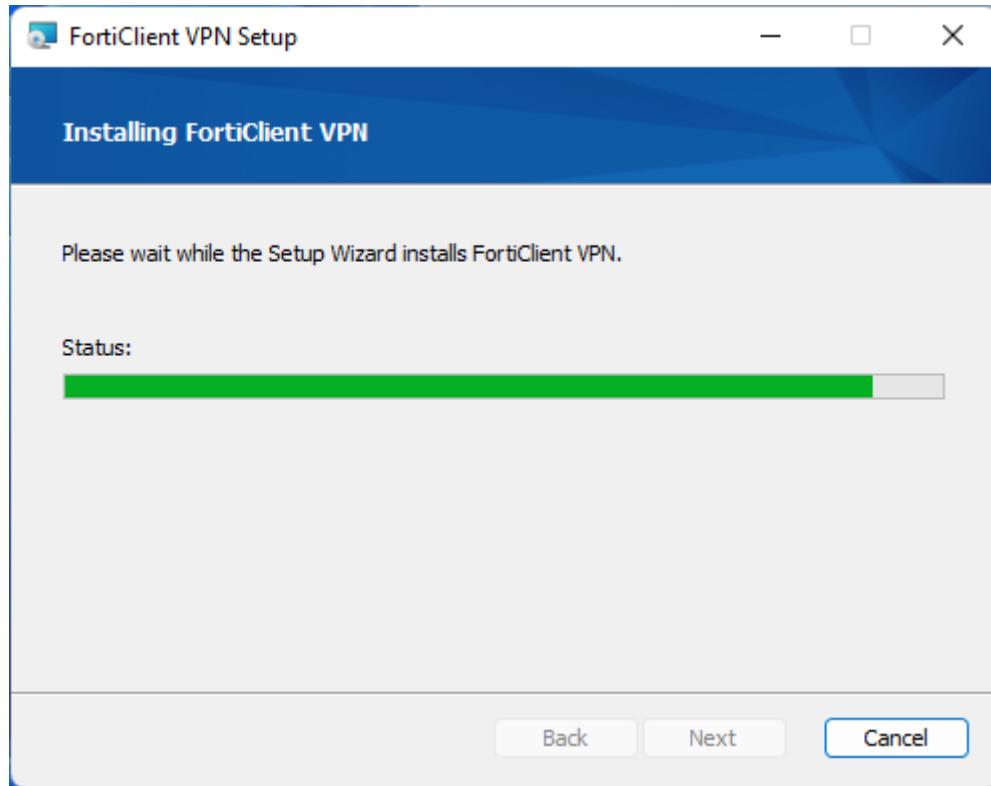
7 Cliquez sur **Next**.



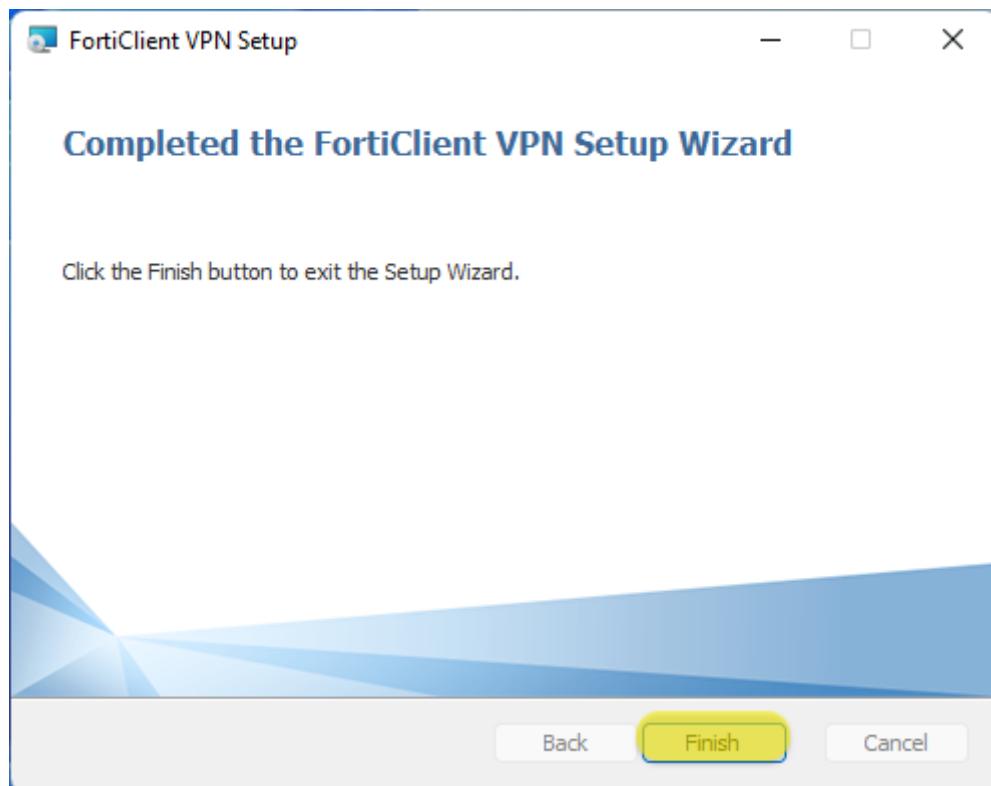
8 Cliquez sur **Install**.



9 Patienter durant l'installation.



10 Cliquez sur **Finish**.



Votre client Fortinet est maintenant installé.



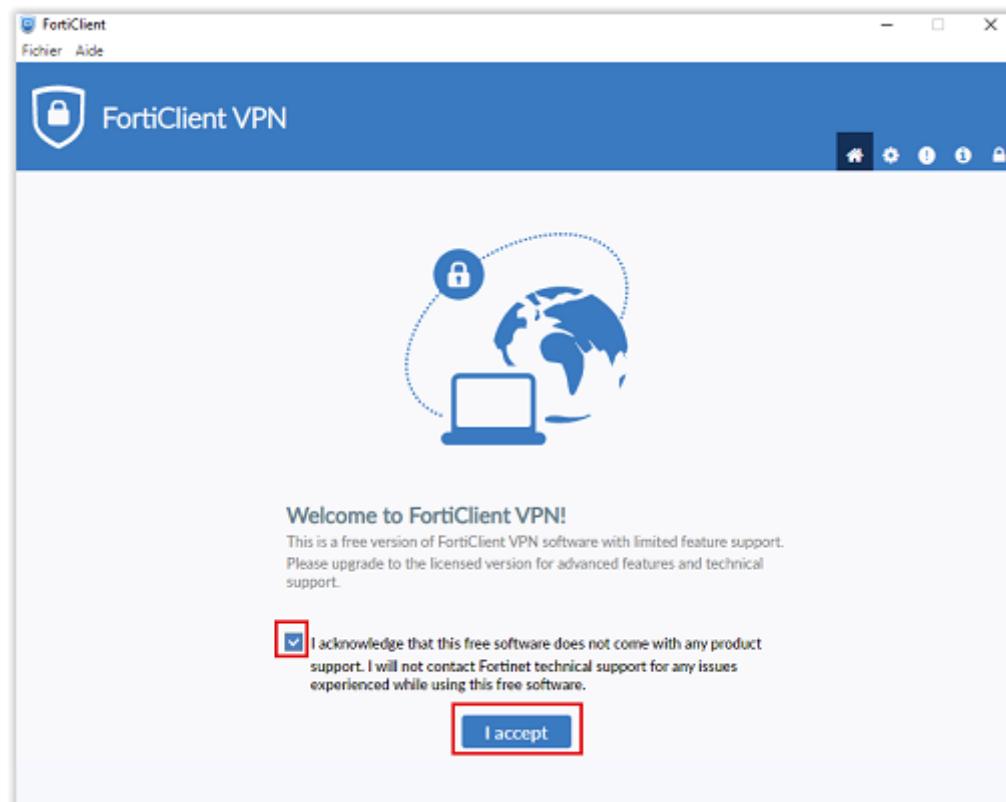
Pour fonctionner, le client doit être configuré.

2. Configurer votre client Fortinet Unistra

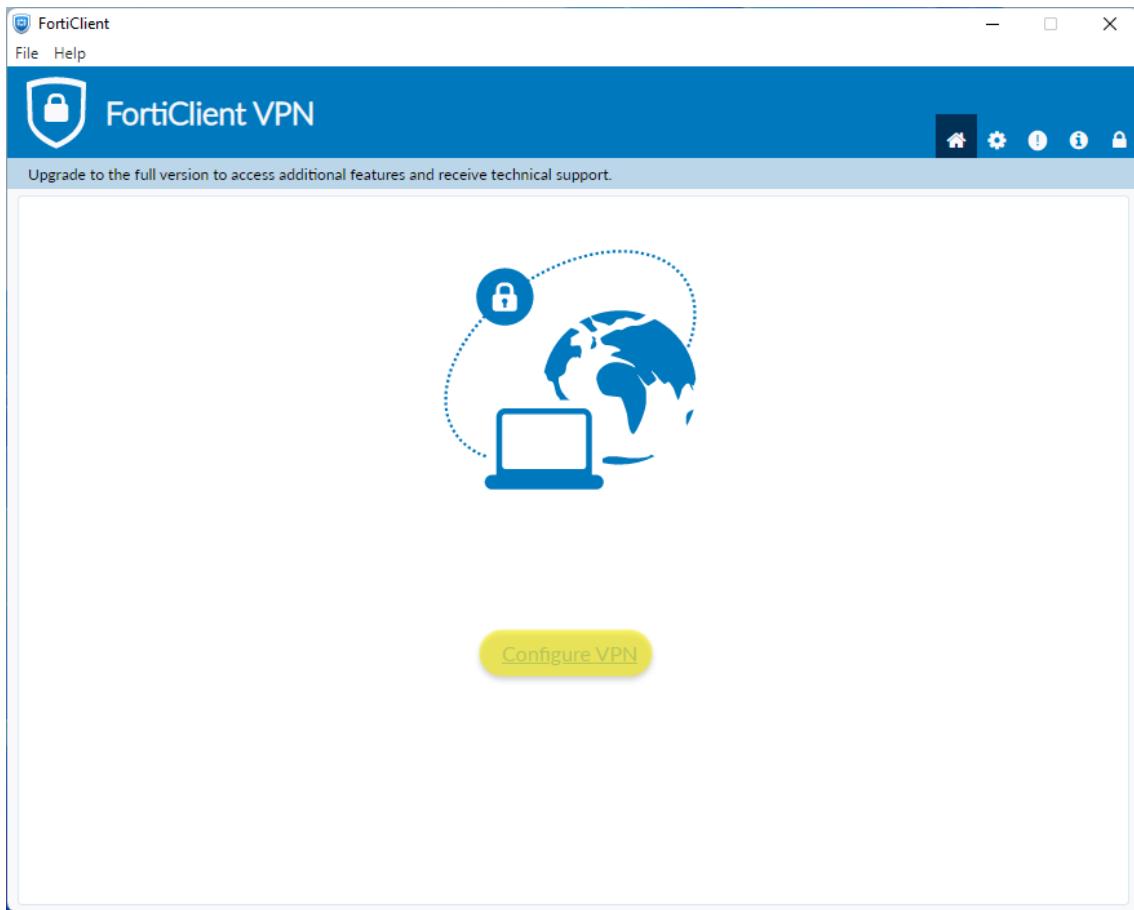
- 1 Lancez le client Fortinet qui vient d'être installé (dans le menu des applications).



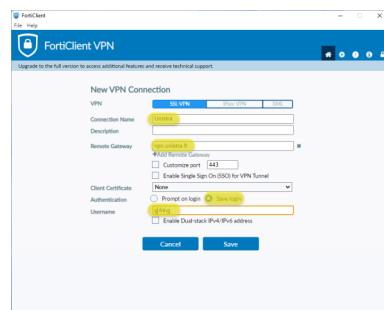
- 2 Acceptez les **conditions d'utilisation**.



3 Cliquez sur **Configurer le vpn**.



4 Renseignez les informations de connexion.



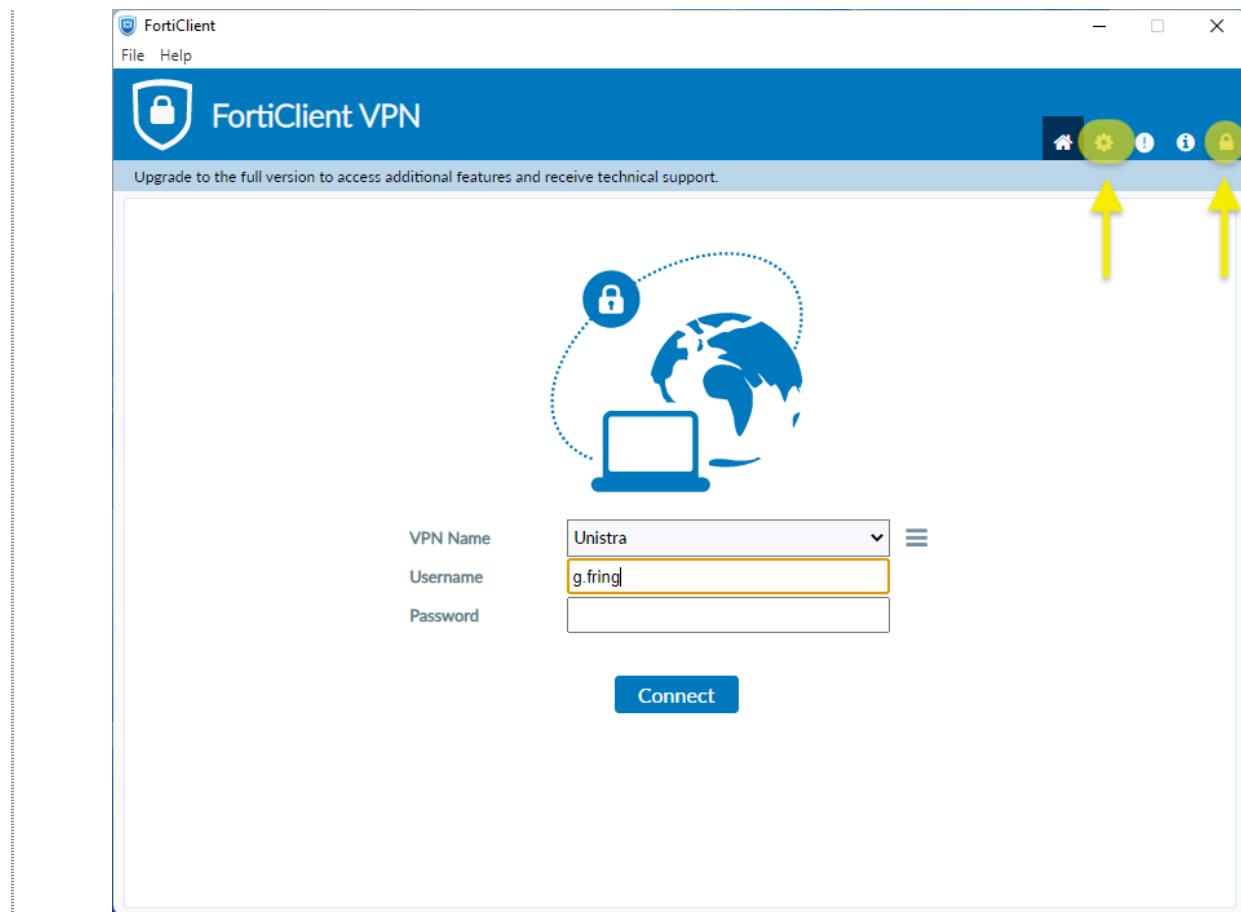
- **VPN :** VPN SSL
- **Nom de la connexion :** Unistra
- **Passerelle distante :** vpn.unistra.fr
- **Port personnalisé :** cocher la case et saisir **443**
- **Certificat Client :** Aucun
- **Authentification :** Save login (enregistrer les informations de connexion).

5 Cliquez sur **Save** (sauvegarder).

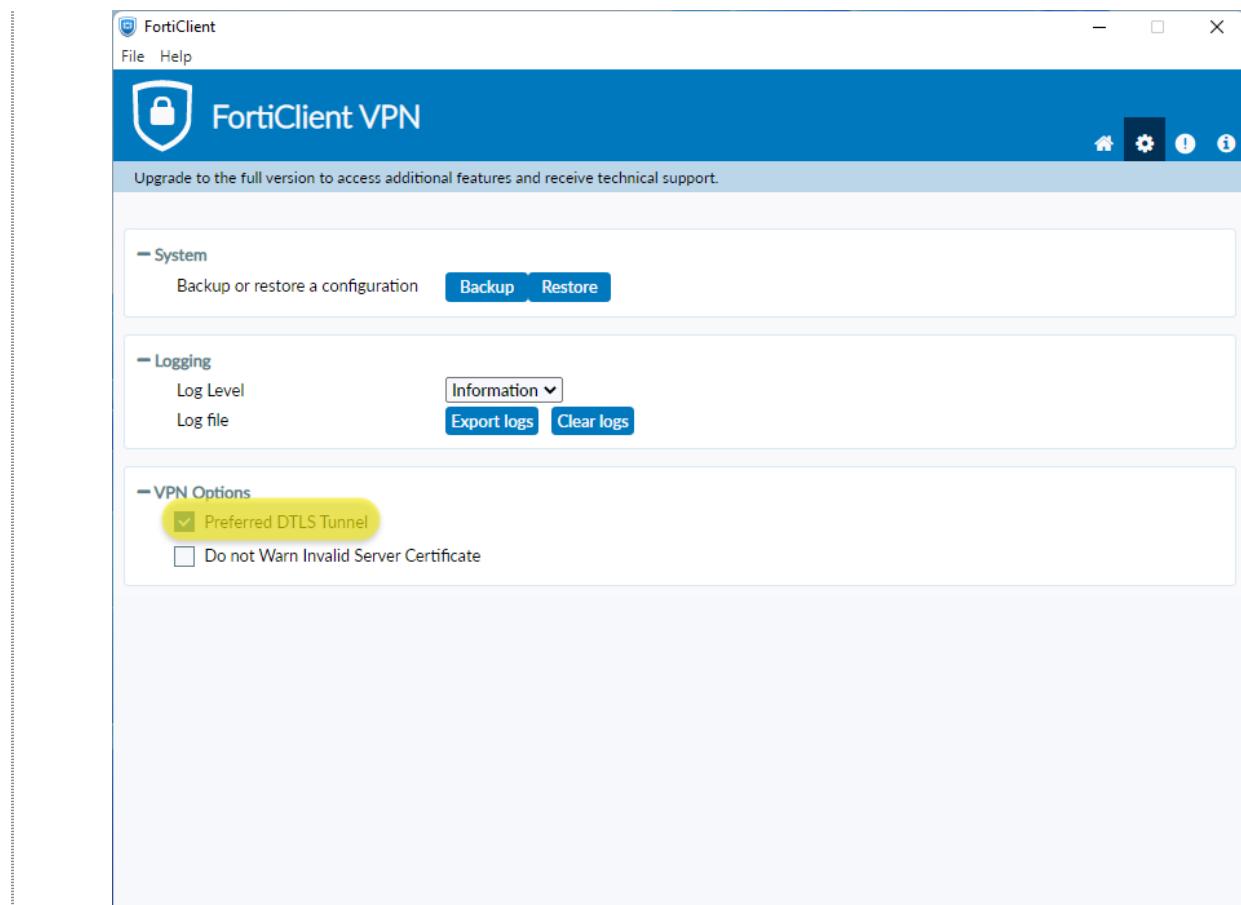
6 Cliquez sur la petite icône en forme de **cadenas** en haut à droite.

La configuration nécessite une "élévation de privilège".

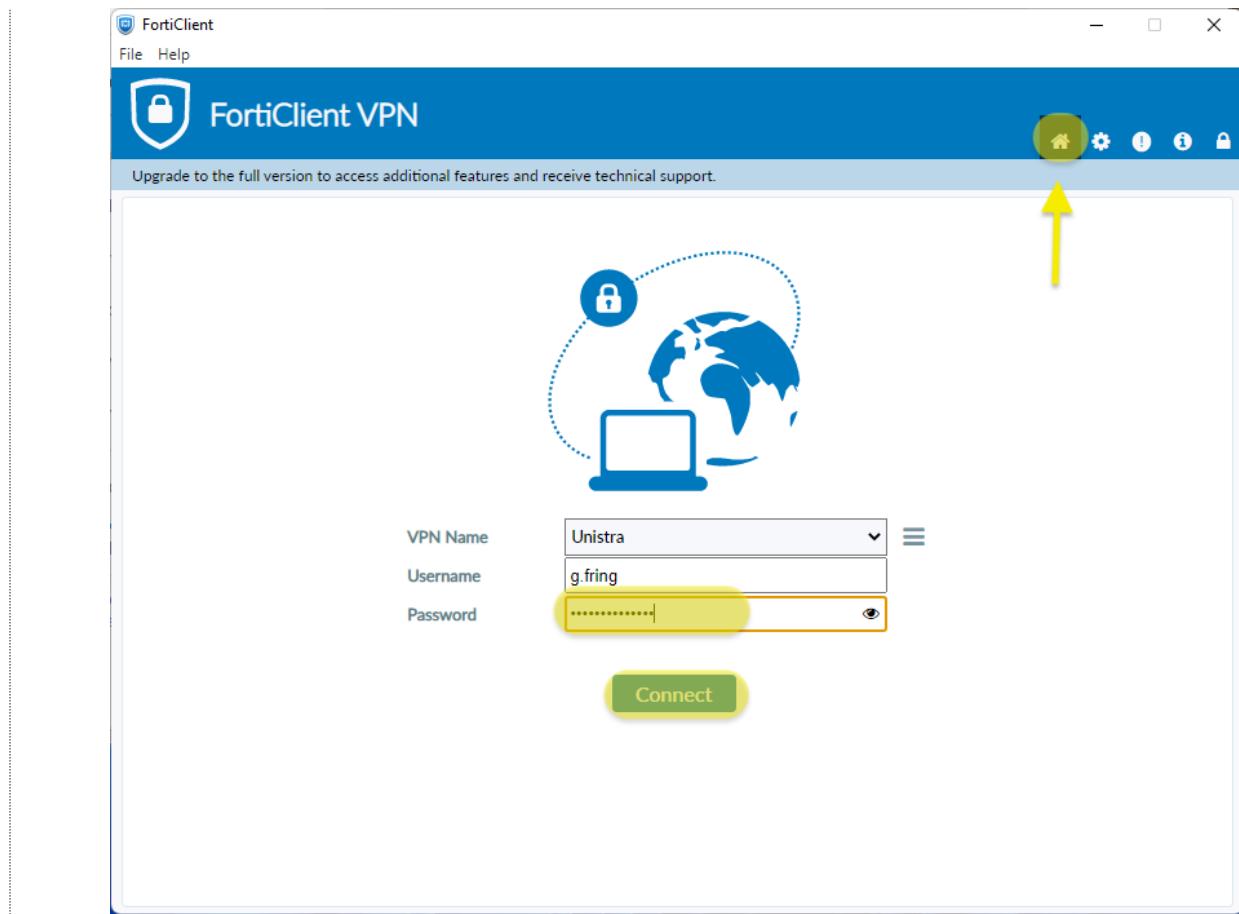
Puis cliquez sur l'icône en forme de **rouage**.



7 Activez l'option Preferred DTLS Tunnel (Tunnel DTLS préféré).



8 Revenez sur la fenêtre principale, saisissez vos **identifiants Unistra**.



9 Cliquez sur **Connect** (connecter).

La configuration est terminée.

Vous pouvez maintenant utiliser votre VPN Unistra.

3. CONFIGURATION POUR UN APPAREIL APPLE

3.1. Configuration pour MacOS Apple



1. Télécharger et installer le client

Prérequis

Si votre poste est géré par la Direction du numérique, cette étape n'est pas nécessaire, le programme est déjà installé. Vous pouvez passer à l'étape 2 « Configurer votre client Fortinet Unistra »



Système d'exploitation compatible: macOS 10.15 (Catalina), 11.x (Big Sur), 12.x (Monterey)

1 Sur votre navigateur internet, rendez-vous sur <https://vpn.unistra.fr>.



Attention : Le navigateur Chrome n'est pas compatible avec cette procédure. Vous pouvez utiliser Firefox, Edge, Safari ou autres.

2 Authentifiez-vous avec votre compte Unistra.



Vous pouvez retrouver votre compte unistra sur <https://quisuisje.unistra.fr>



Vous arrivez sur le portail Fortinet Unistra, il vous permettra de télécharger le fichier d'installation du client.

3 Choisissez votre système d'exploitation parmi la liste (iOS, Android, Windows, **Mac**) dans le menu  **Download Forticlient**.

4 Depuis votre répertoire **Téléchargement**, ouvrez **FortiClientVPNSetup.dmg**

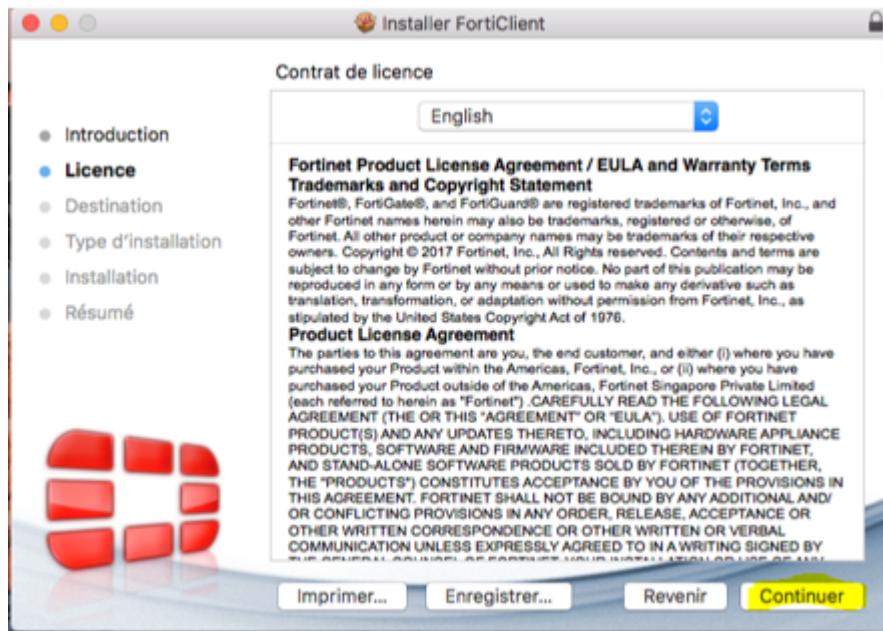
5 Cliquez sur **Install.**



6 Cliquez sur **Continuer.**



7 Cliquez sur Continuer.



8 Cliquez sur Agree (Accepter).

To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

[Read License](#)

[Disagree](#)

[Agree](#)

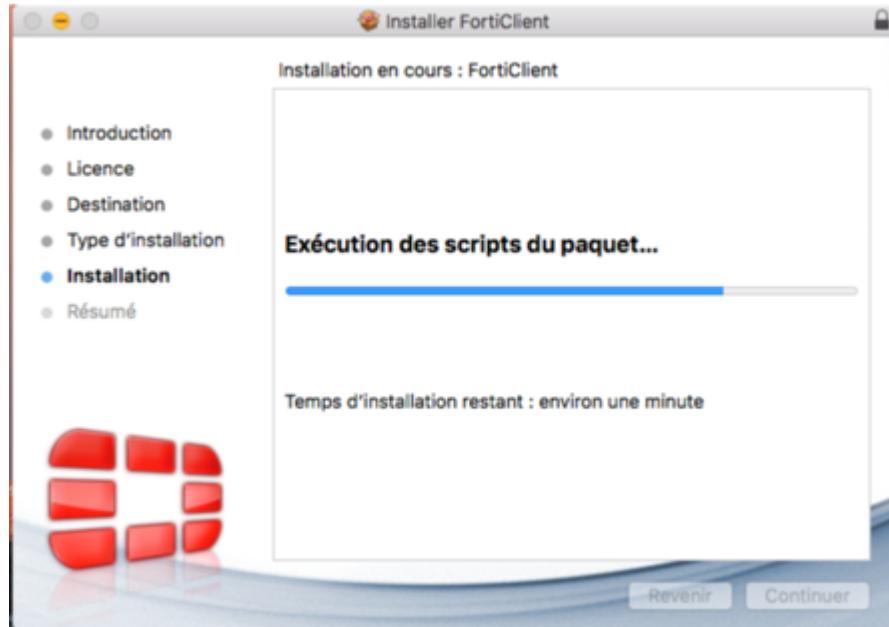
9 Cliquez sur **Installer**.



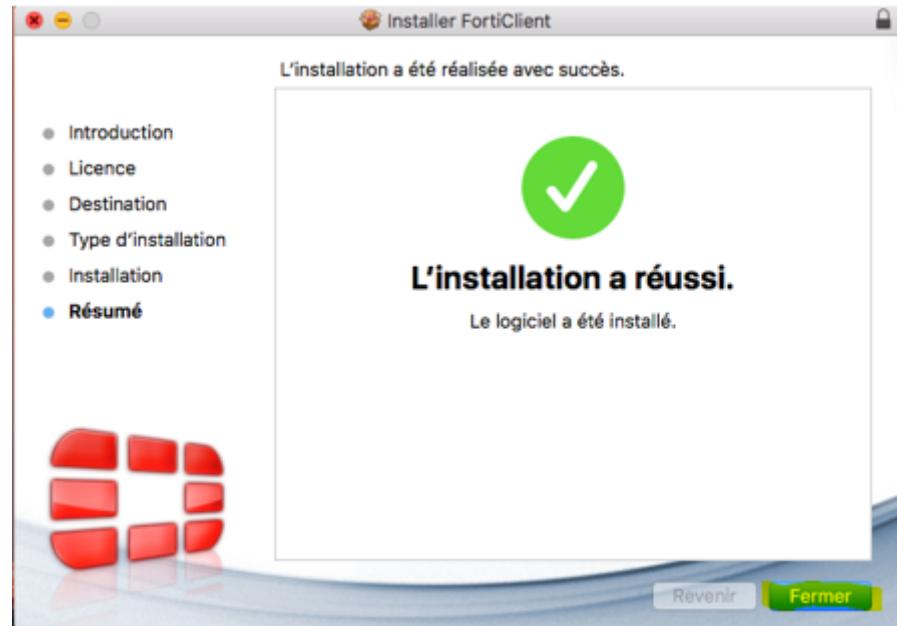
10 Cette opération nécessite une "élévation de privilège" :

- Saisissez votre mot de passe, puis
- Cliquez sur **Installer le logiciel**.



11 Patienter durant l'installation.**12** Cliquez sur Autoriser .

Le client VPN Fortinet est installé.



2. Configurer votre client Fortinet Unistra

- 1 Cliquer en haut à droite sur l'icône VPN FortiClient.

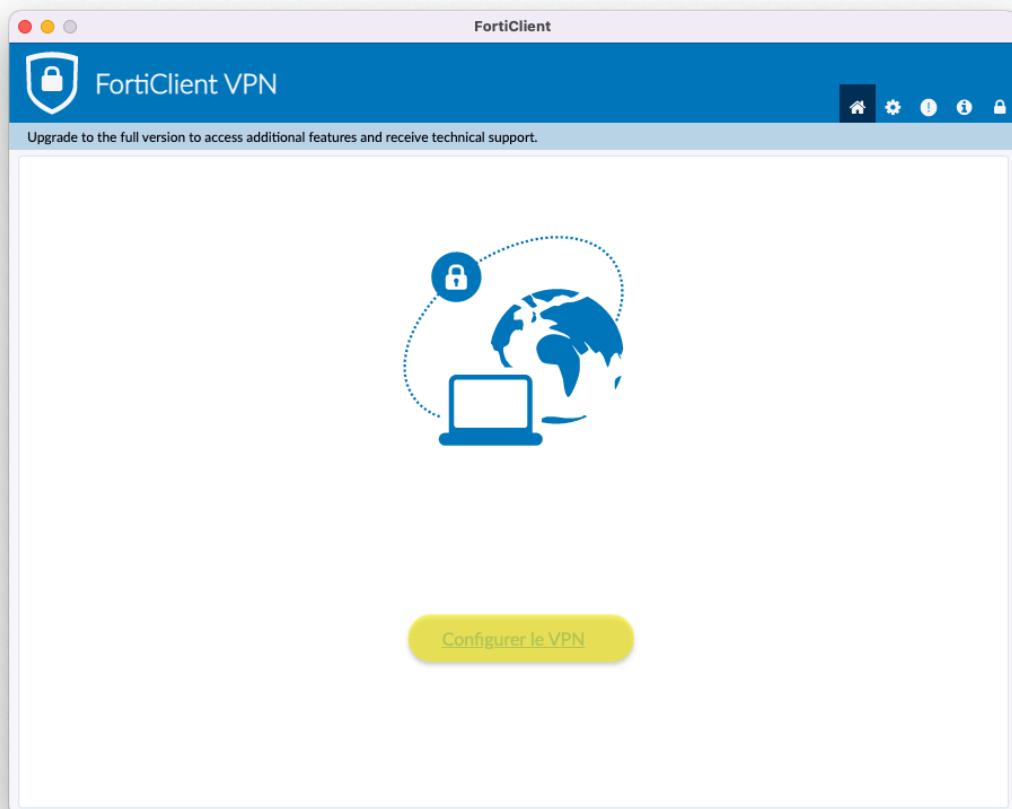
Cliquer sur **Open FortiClient Console**



2 Cochez la case de licence puis **I Accept** (J'accepte).



3 Cliquer sur **Configurer le VPN**.



4 Renseignez les informations de connexion.

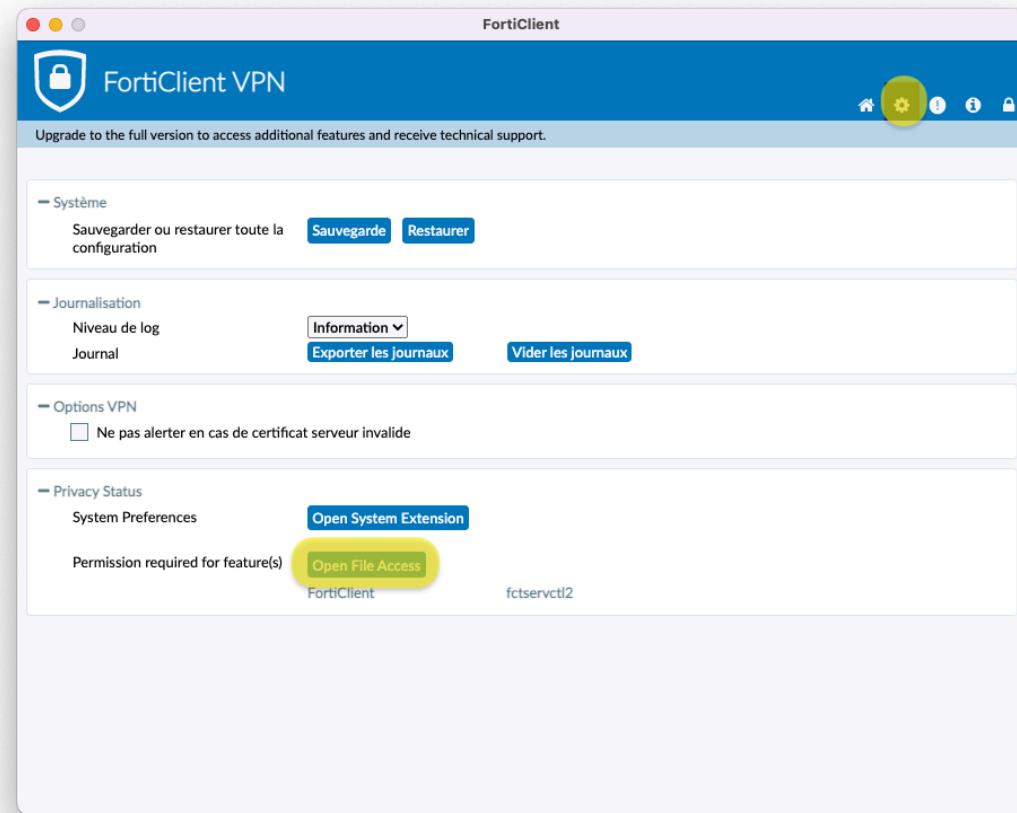


- **VPN :** VPN SSL
- **Nom de la connexion :** Unistra
- **Passerelle distante :** vpn.unistra.fr
- **Port personnalisé :** cocher la case et saisir **443**
- **Certificat Client :** Aucun
- **Authentification :** Sauvegarder les informations d'authentification
- **Nom d'utilisateur :** Identifiant de votre compte unistra

5 Cliquez sur **Sauvegarder**.

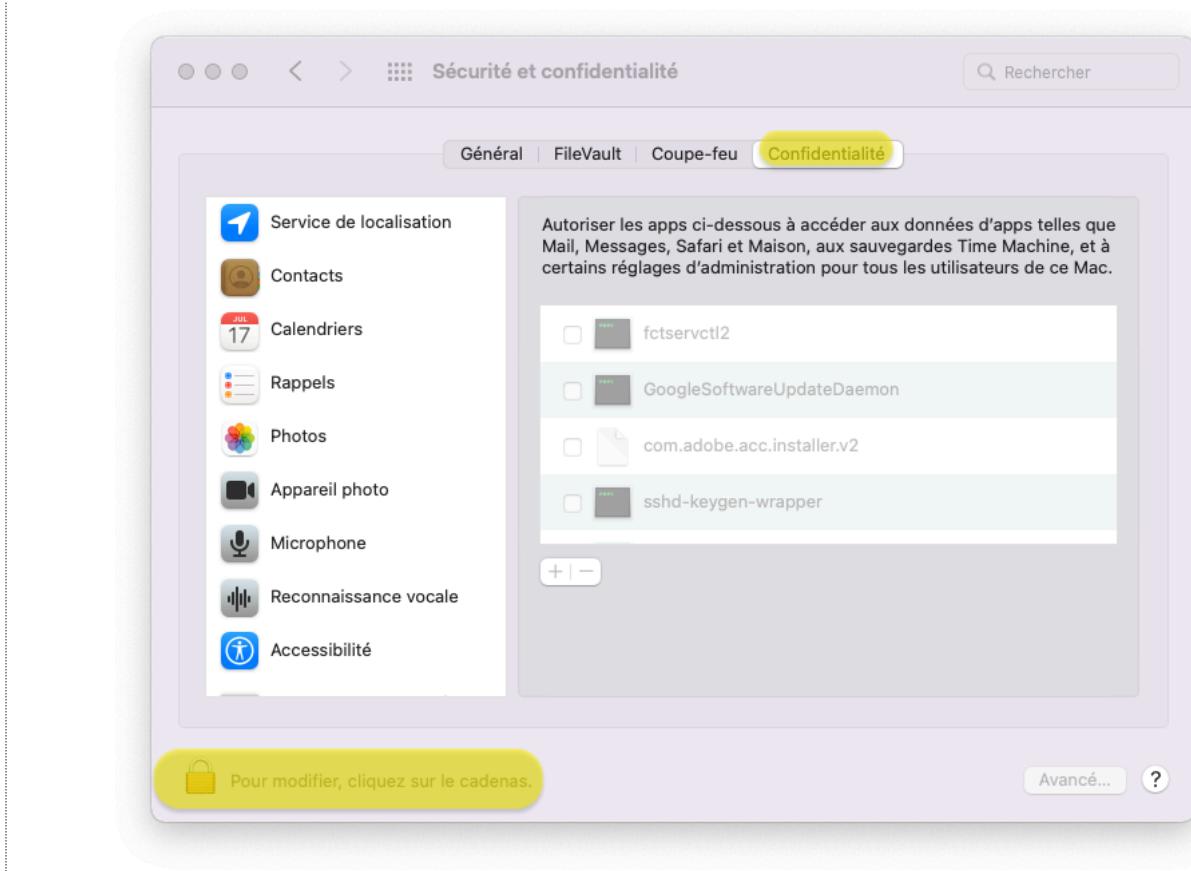
6 Cliquer sur l'icône représentant un **rouge** en haut à droite.

Puis cliquez sur **Open File Access**.



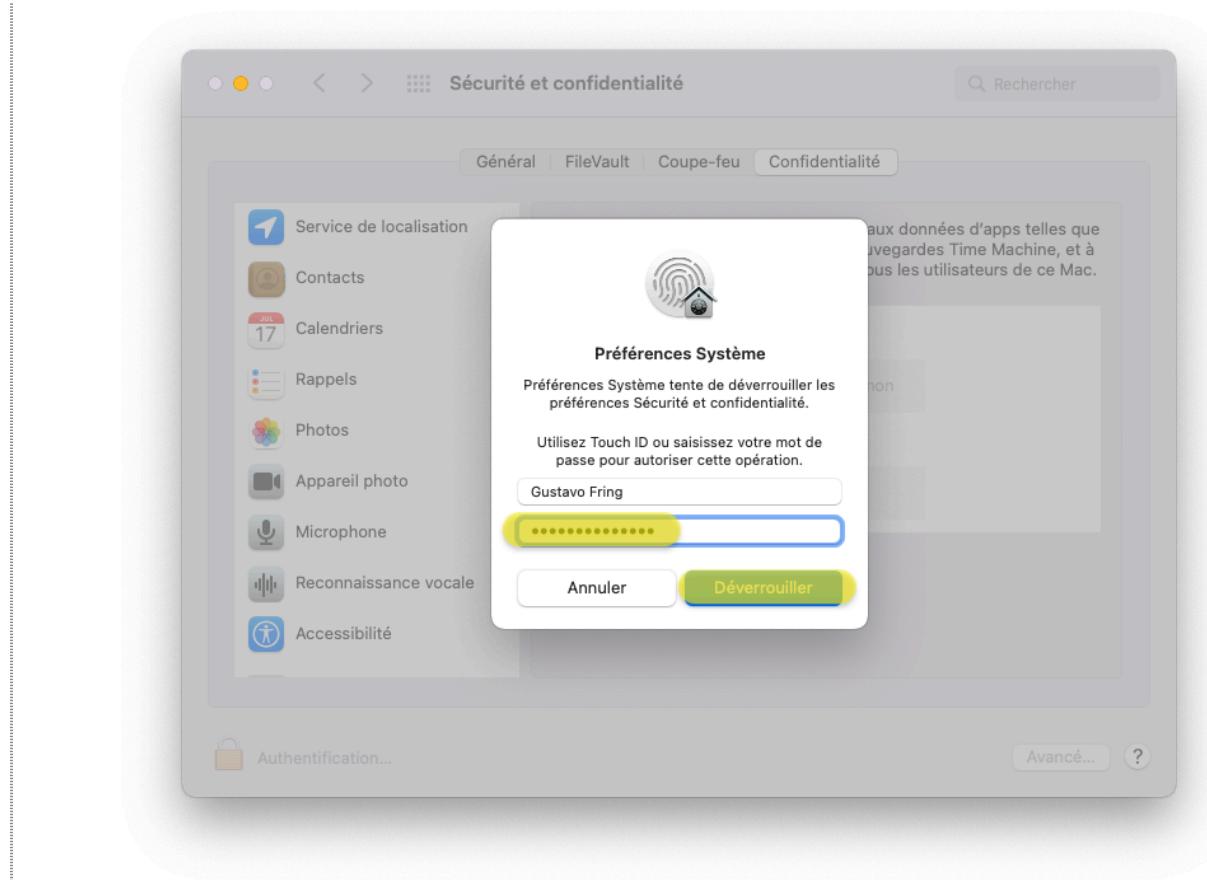
7 Cliquez sur Confidentialité .

Puis cliquez sur l'icône représentant un **cadenas** en bas en gauche.



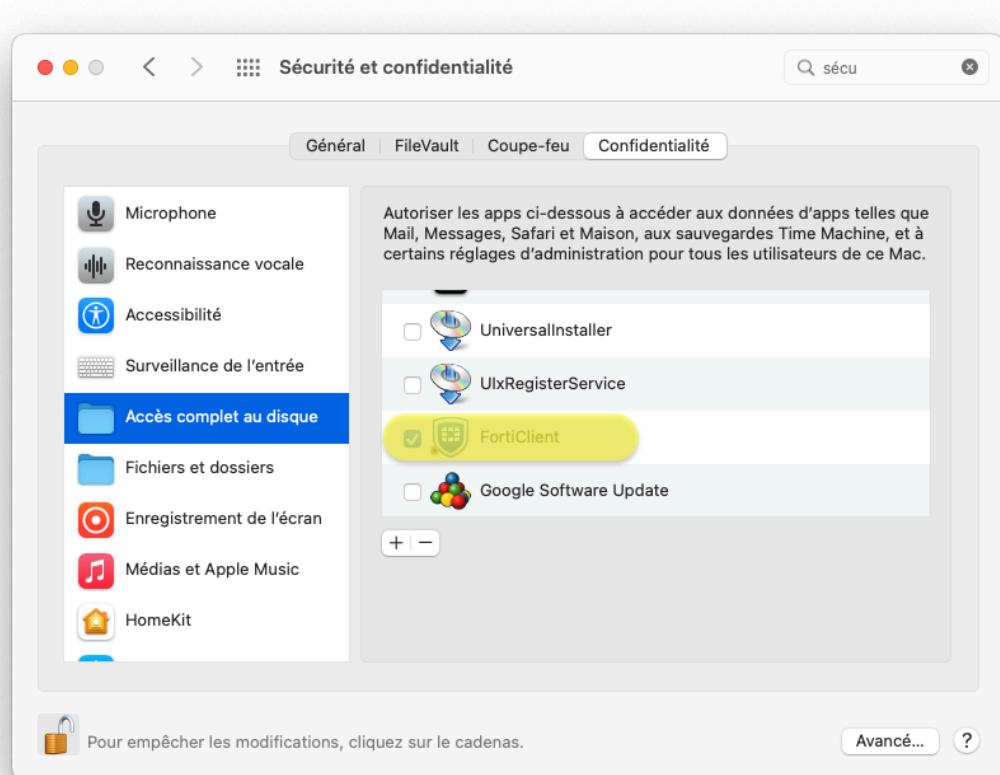
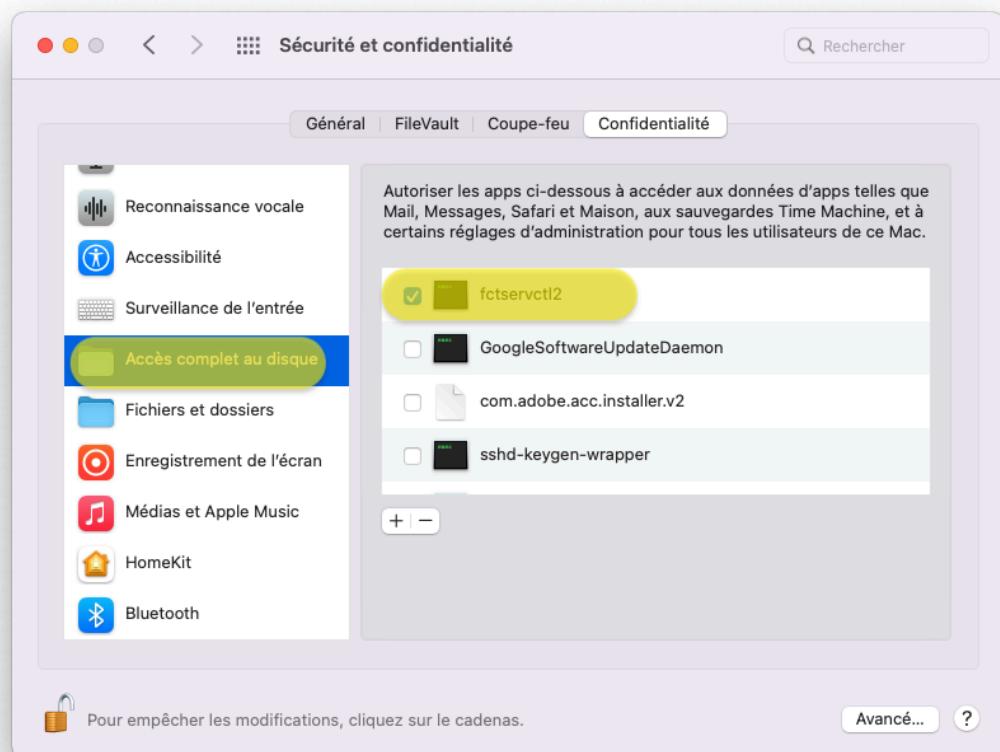
8 Cette opération nécessite une "élévation de privilège" :

- Saisissez votre mot de passe, puis
- Cliquez sur **Déverrouiller**.



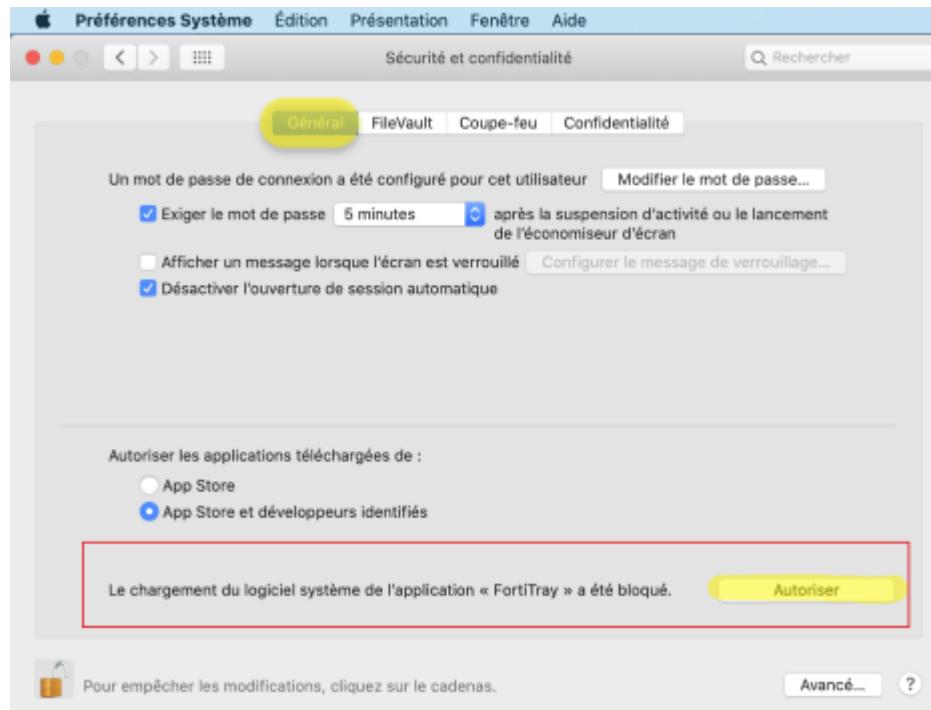
9 Sélectionner dans le menu de gauche **Accès complet au disque**.

Puis cocher l'application **fctservctl2 & Forticlient**.



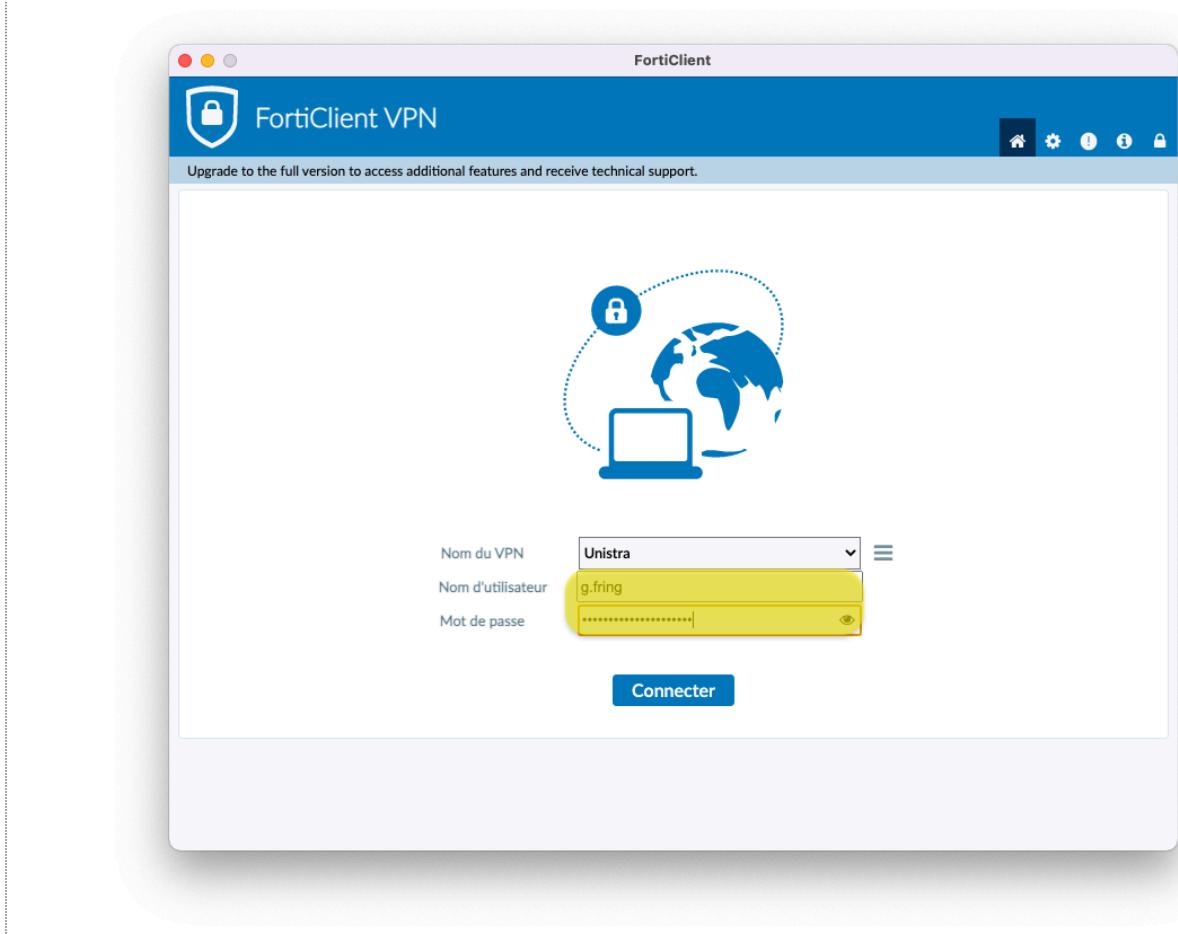
10 Vérifier dans l'onglet **Général** qu'un message n'apparaît pas indiquant que **Fortitray** est bloqué.

Si c'est le cas, vous **devez l'autoriser** en cliquant sur le bouton prévu à cet effet.



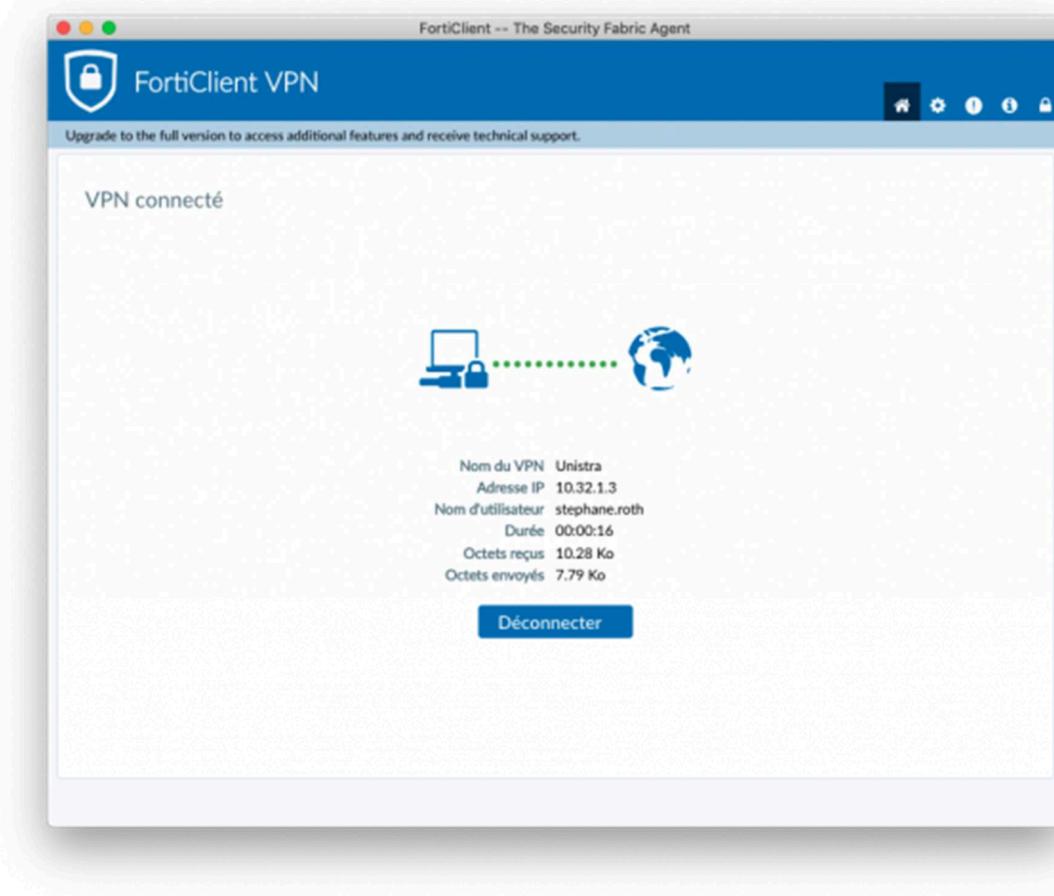
11 Revenez sur l'application Fortinet.

- Saisir vos identifiants Unistra
- Puis cliquer sur le bouton **Connacter**.



La configuration est terminée.

Vous pouvez maintenant utiliser votre VPN Unistra.



3.2. Configuration pour iPhone, iPad

Télécharger, installer et configurer le VPN Fortinet sur iPhone ou iPad Apple

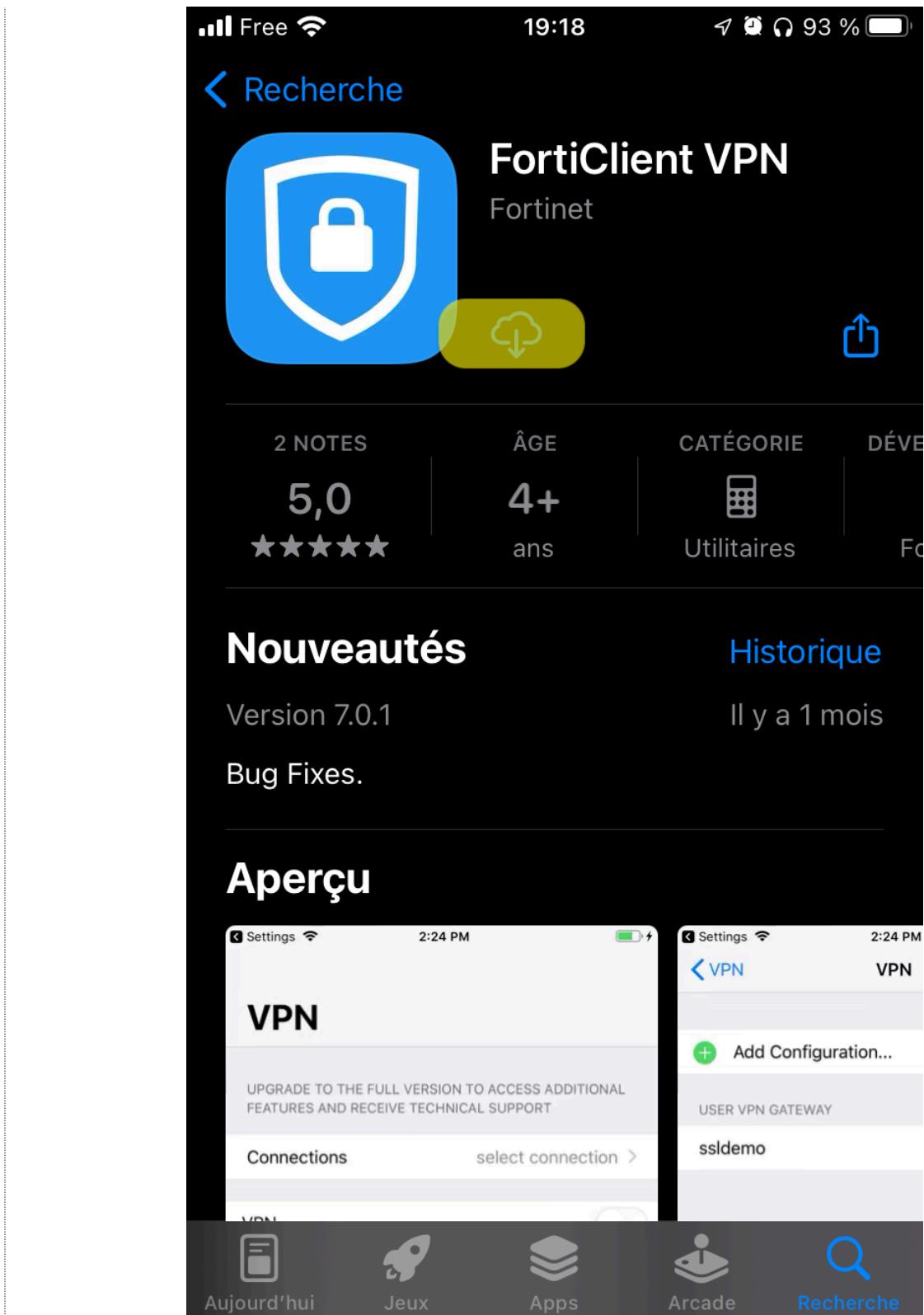
Prérequis



Système d'exploitation compatible:

- **iPhone** : iOS 9.0 ou version ultérieure
- **iPad** : iPadOS 9.0 ou version ultérieure

1 Télécharger sur l'Apple Store l'application "FortiClient VPN".



2 Ouvrir l'application et Accepter les conditions d'utilisation

◀ App Store

19:19

93 %

Points saillants de la politique de con...

FortiClient NE collecte AUCUNE information personnelle spécifique à l'utilisateur comme le nom d'utilisateur, les photos ou l'adresse e-mail pour les...



Analytique

FortiClient peut collecter des informations d'utilisation anonymes et les partager avec Fortinet dans le but d'améliorer la convivialité et la fonctionnalité.



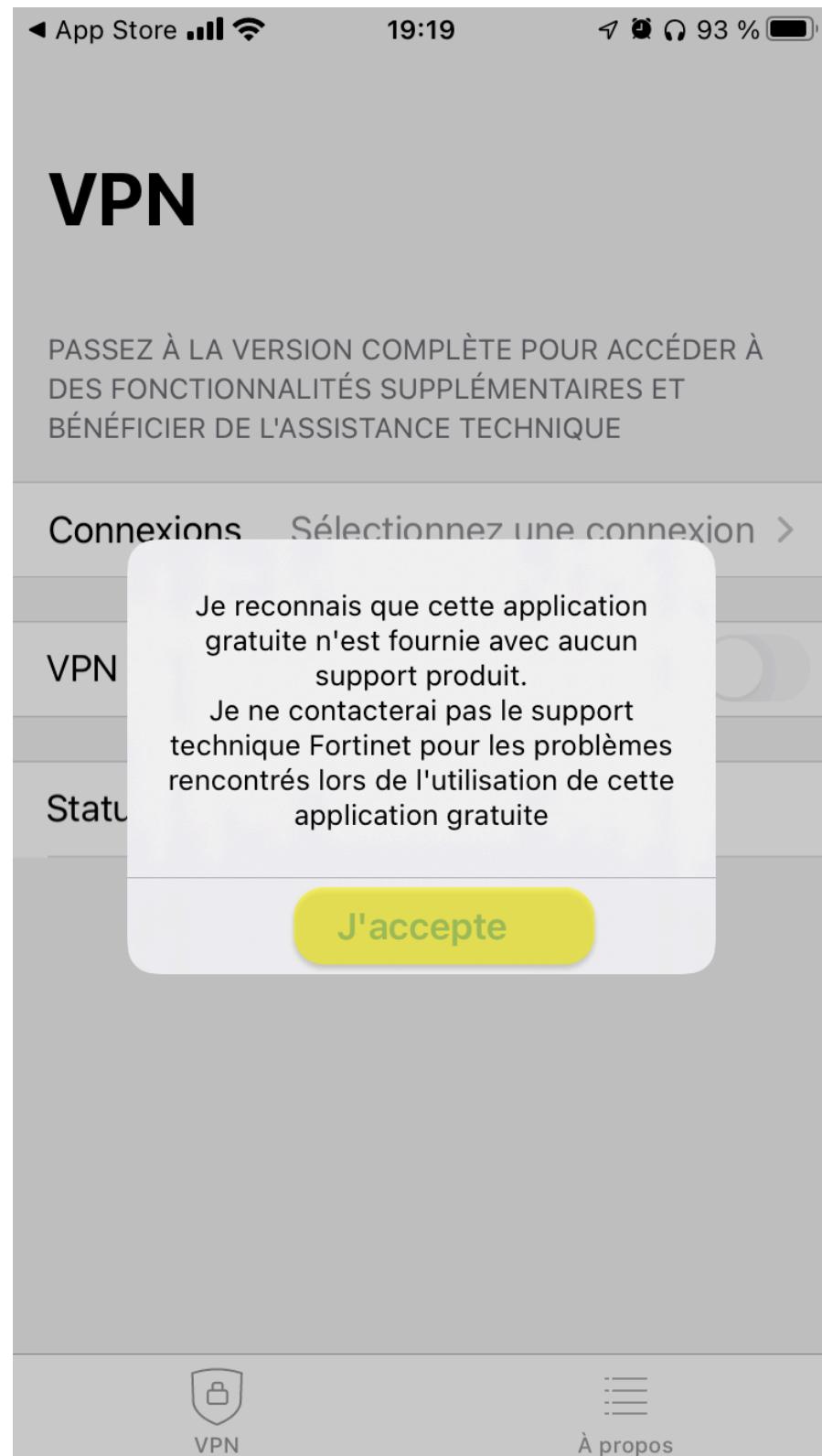
VPN

FortiClient ne surveille pas le trafic VPN de l'utilisateur.

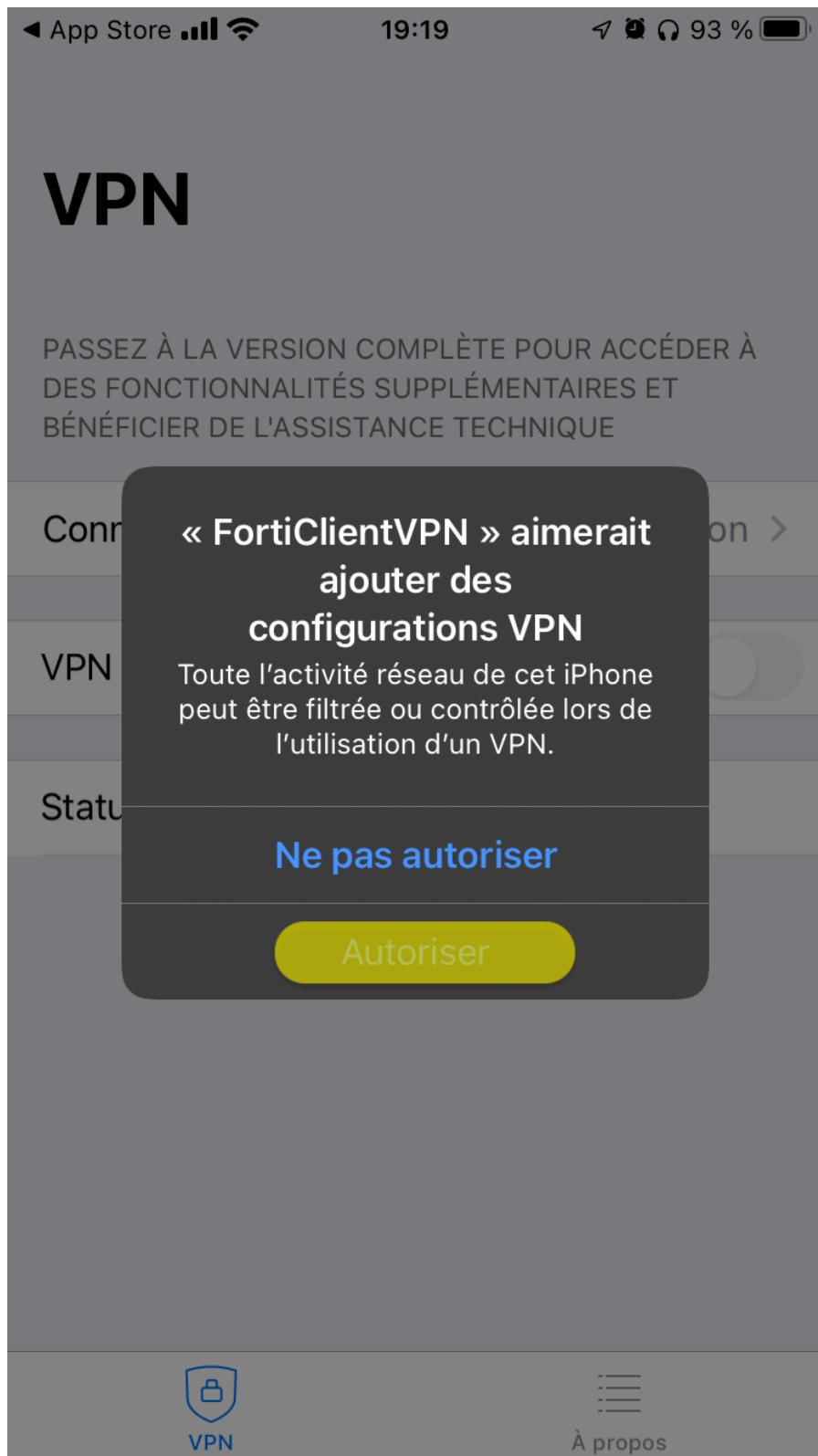
Il s'agit d'une version gratuite du logiciel FortiClient VPN avec fonctionnalités limitée.
Veuillez passer à la version pleine, sous licence, pour les fonctionnalités avancées et l'assistance technique.

En sélectionnant «J'accepte» ci-dessous, vous acceptez les <[Conditions d'utilisation](#)> et la <[Politique de confidentialité](#)> de FortiClient.

[J'accepte](#)

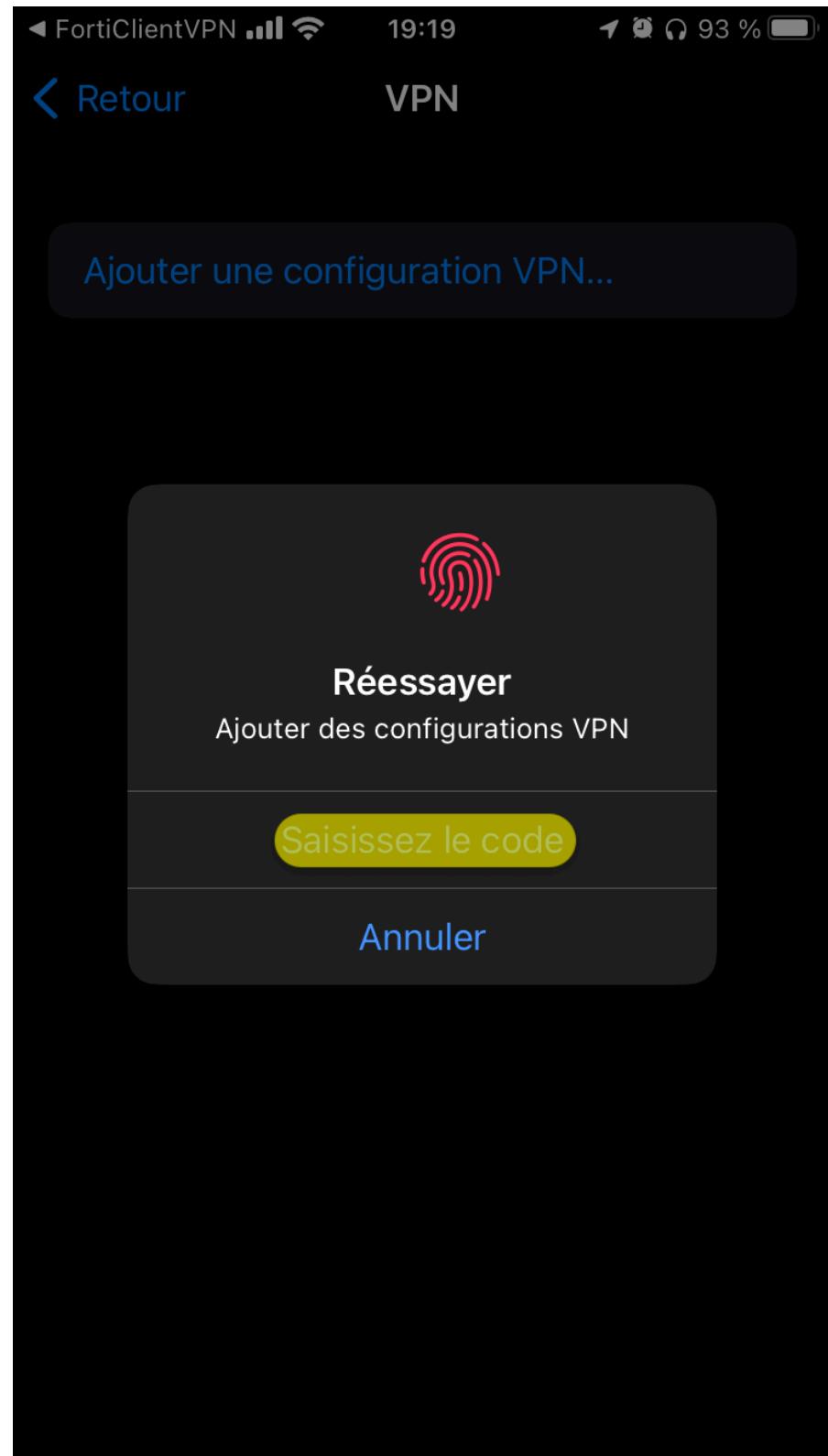
3 Cliquez sur J'accepte

4 Cliquez sur Autoriser

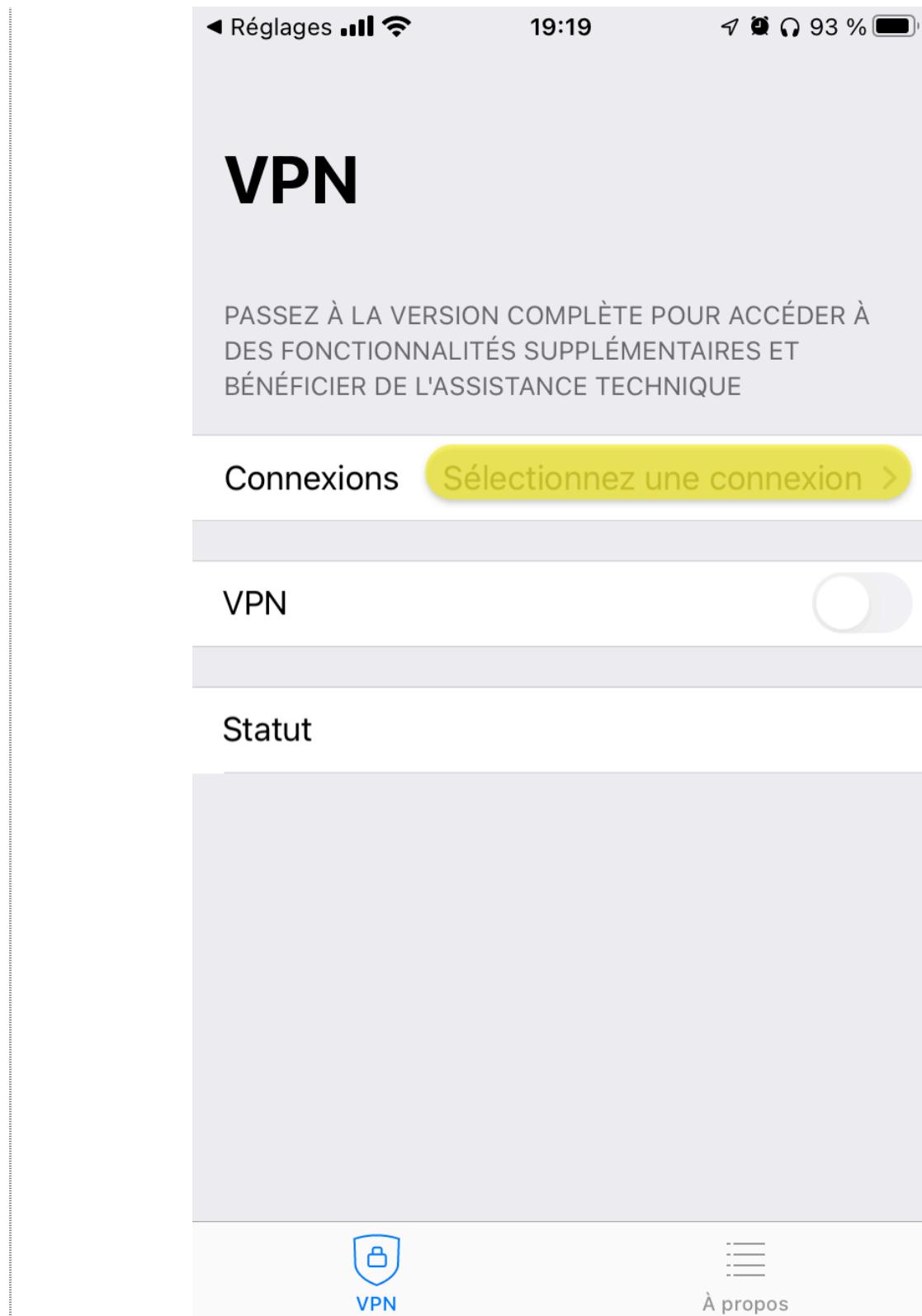


5 Cette opération nécessite une "élévation de privilège" :

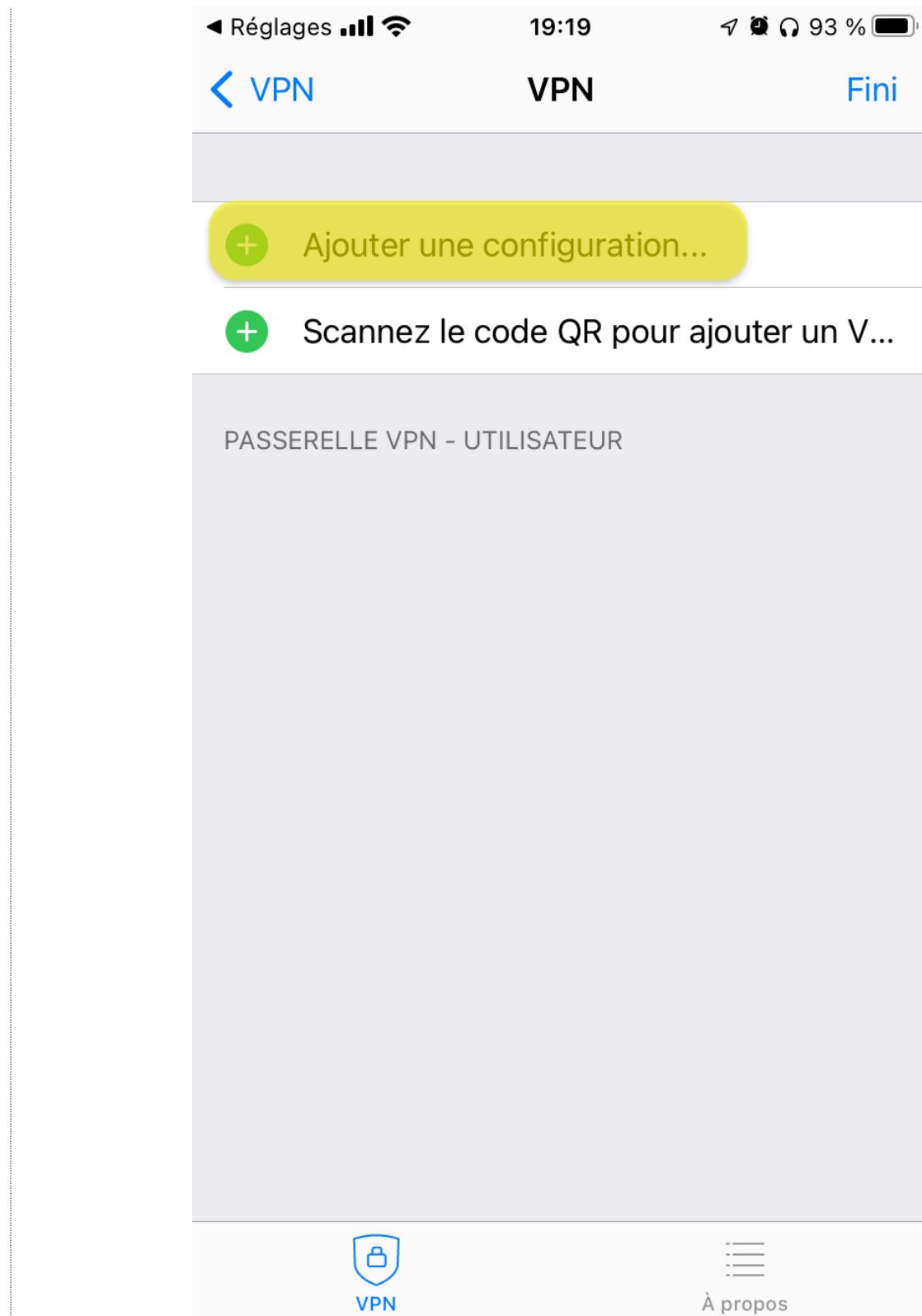
Saisissez votre **code personnel**.



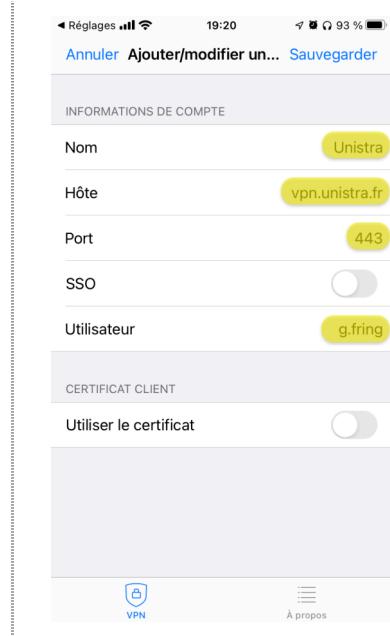
6 Cliquez sur Sélectionnez une connexion



7 Cliquez sur Ajouter une configuration

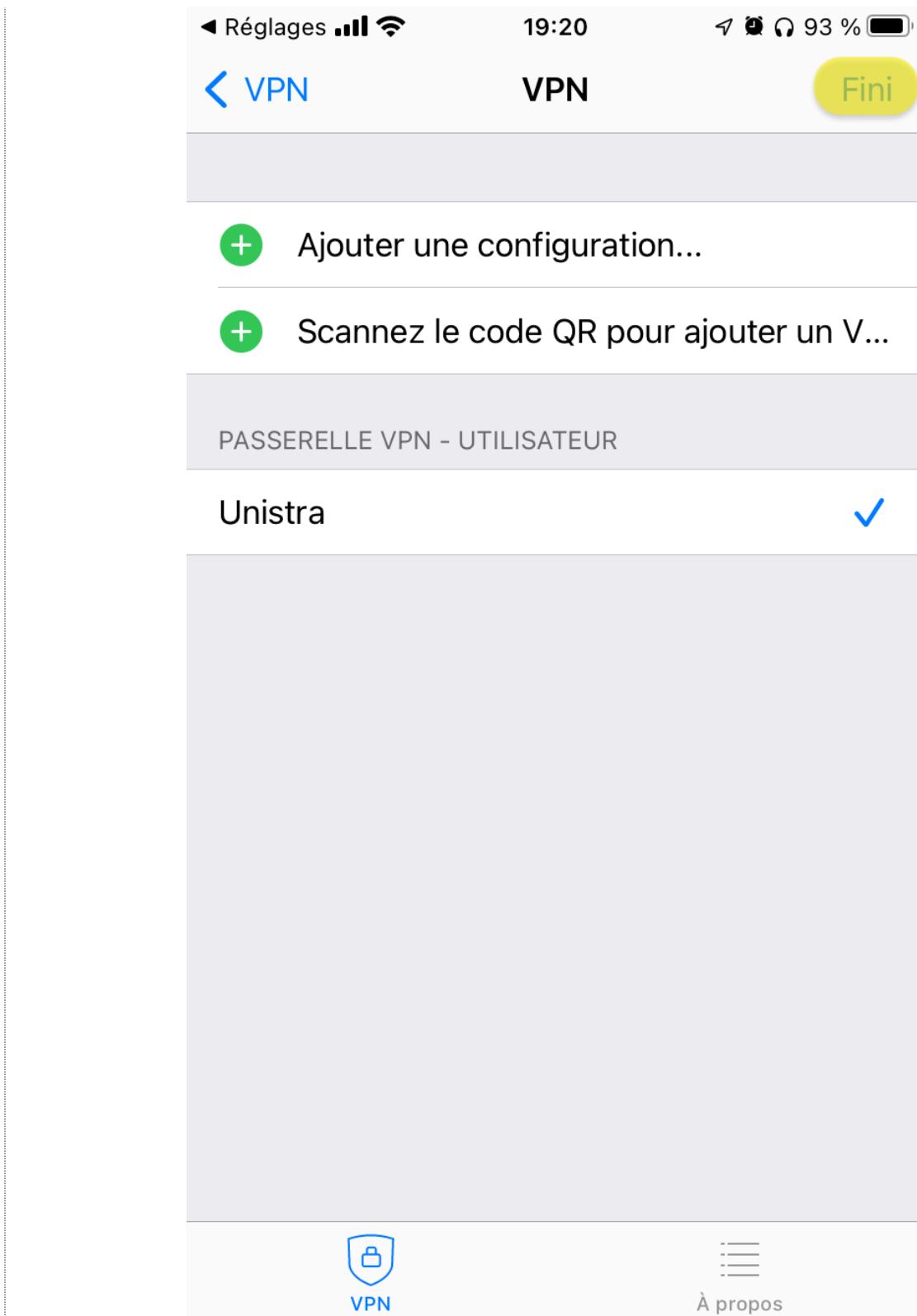


8 Renseigner ensuite les champs (cf. ci-dessous) et cliquer sur **Sauvegarder**.

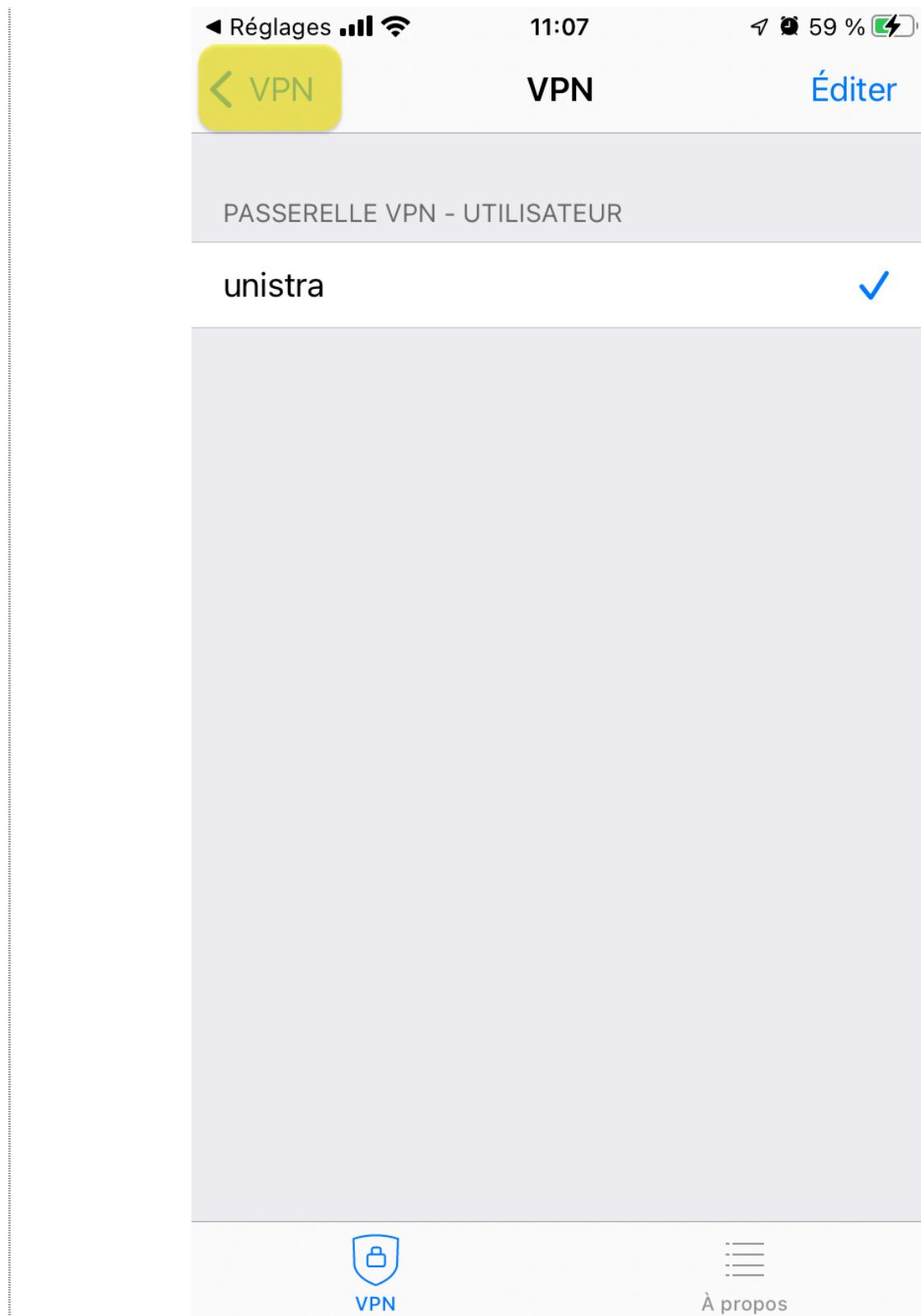


- **Nom:** Unistra
- **Hôte:** <https://vpn.unistra.fr>
- **Port :** 443
- **Utilisateur:** votre identifiant Unistra

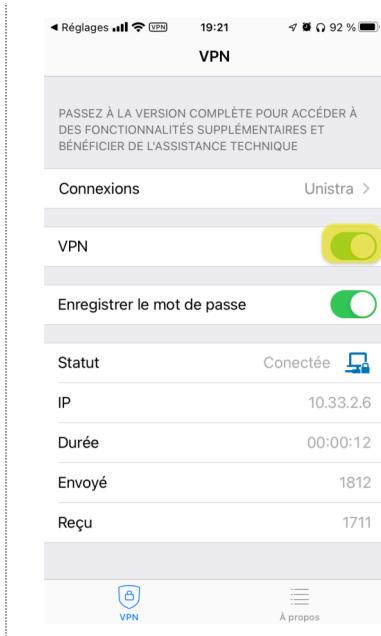
9 Cliquez sur Fini



10 Retournez sur l'écran d'accueil de l'application.



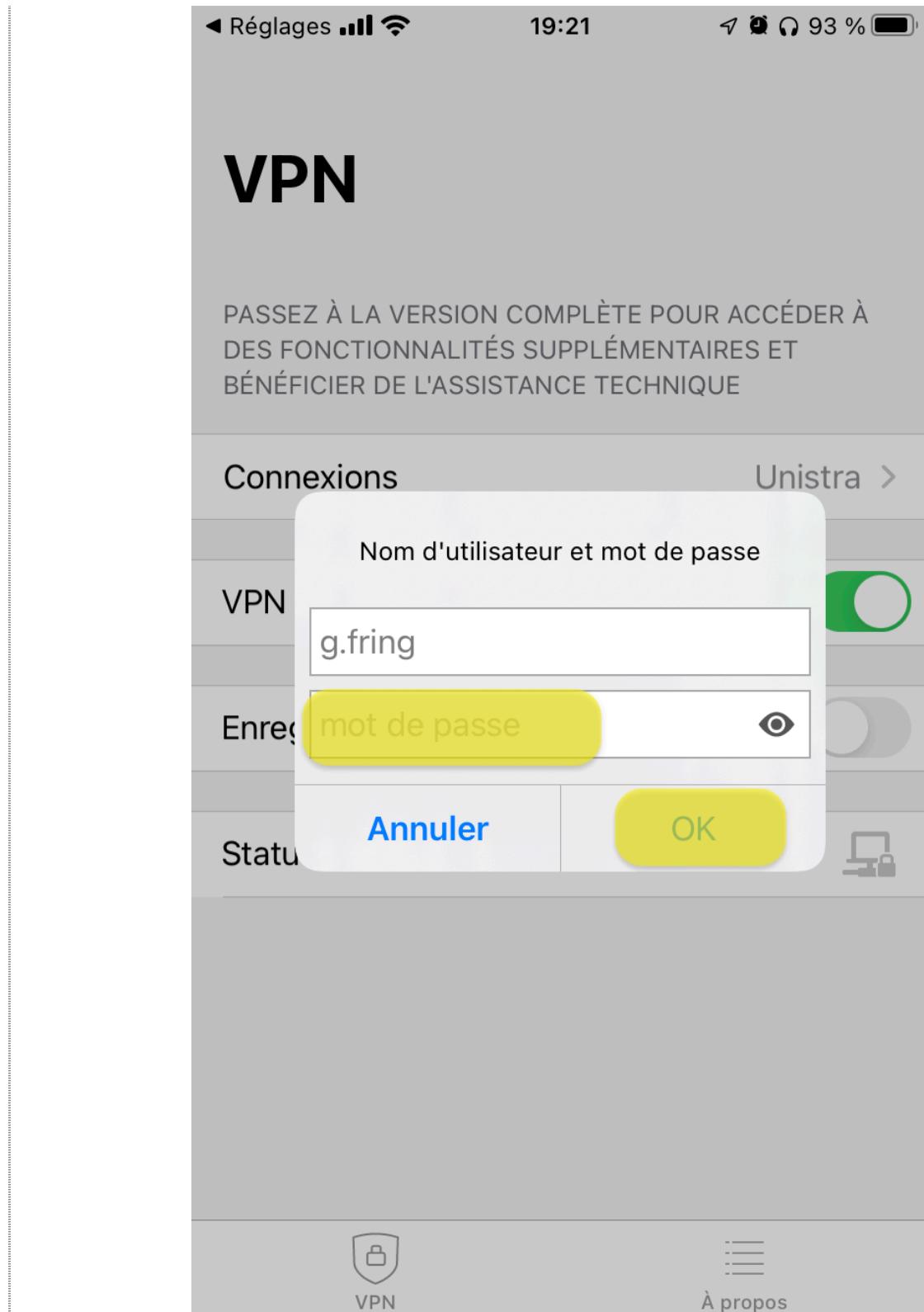
11 Activez la connection VPN.



- **Connections** : Unistra
- **VPN** : (activez-le)

12 Cette opération nécessite une "élévation de privilège" :

Renseignez vos **identifiants Unistra**.



L'application doit vous indiquer que votre connexion VPN est active.

Vous avez la possibilité de sauvegarder votre mot de passe pour faciliter les futures connexions.

◀ Réglages 19:21 ⌂ 92 %

VPN

PASSEZ À LA VERSION COMPLÈTE POUR ACCÉDER À DES FONCTIONNALITÉS SUPPLÉMENTAIRES ET BÉNÉFICIER DE L'ASSISTANCE TECHNIQUE

Connexions [Unistra >](#)

VPN

Enregistrer le mot de passe

Statut

IP 10.33.2.6

Durée 00:00:12

Envoyé 1812

Reçu 1711

[À propos](#)

4. CONFIGURATION POUR UN APPAREIL ANDROID

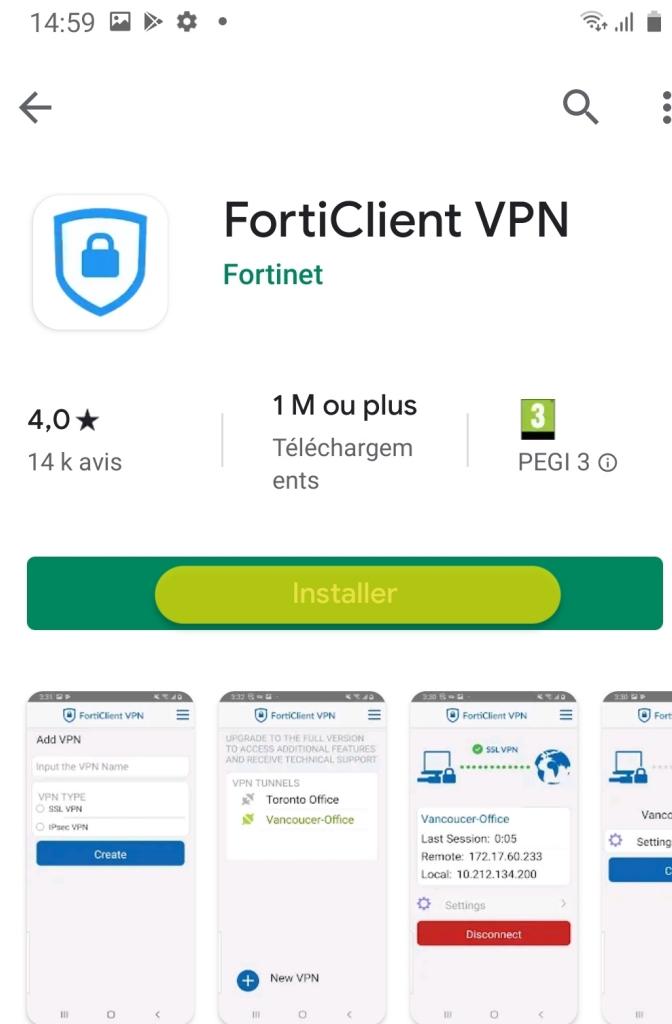


Télécharger, installer et configurer le VPN Fortinet sur Android

Prérequis



Système d'exploitation compatible: **Android** 5.0 ou version ultérieure.

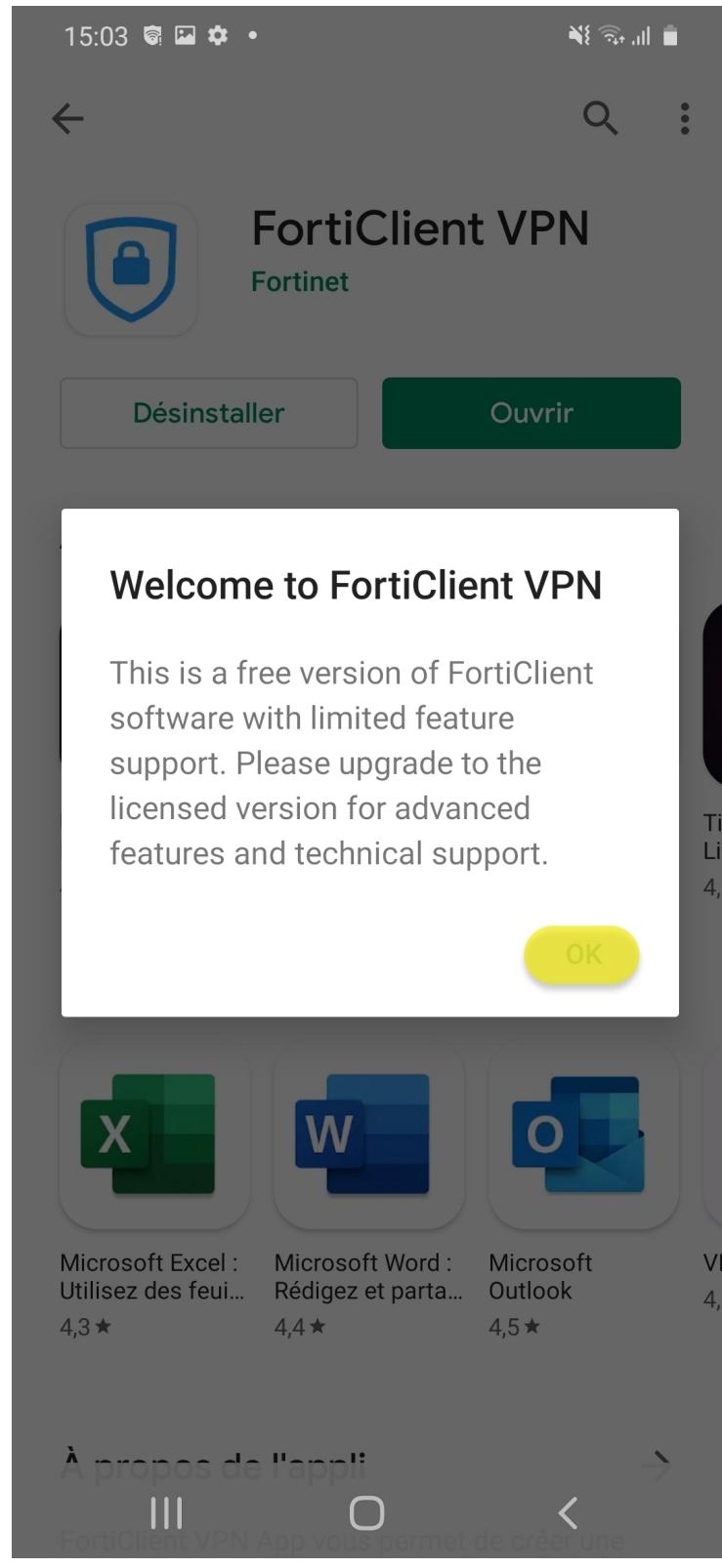
1 Télécharger sur le Play Store l'application "FortiClient VPN".**À propos de l'appli**

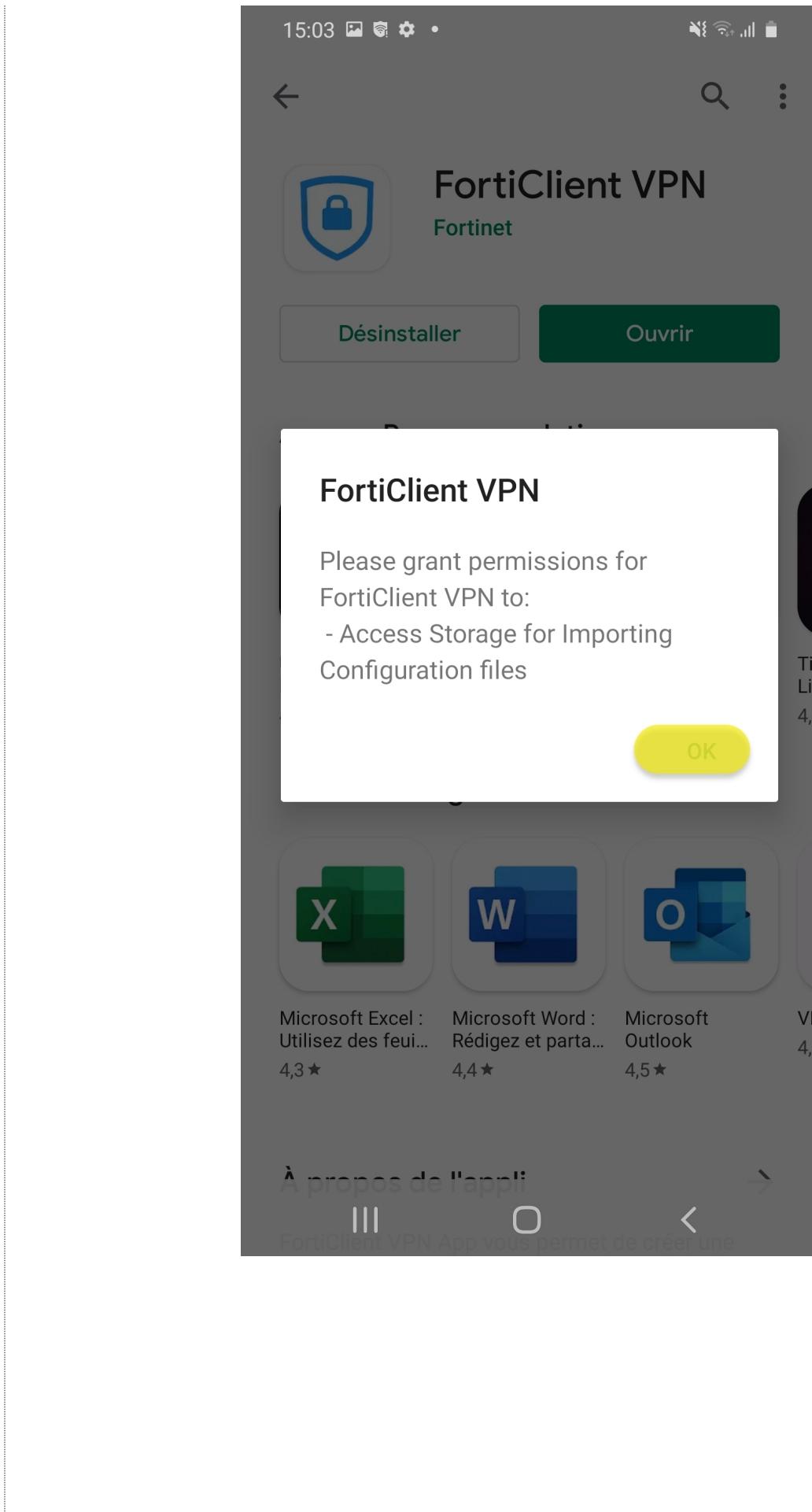
FortiClient VPN App vous permet de créer une connexion VPN sécurisée avec le pare-feu

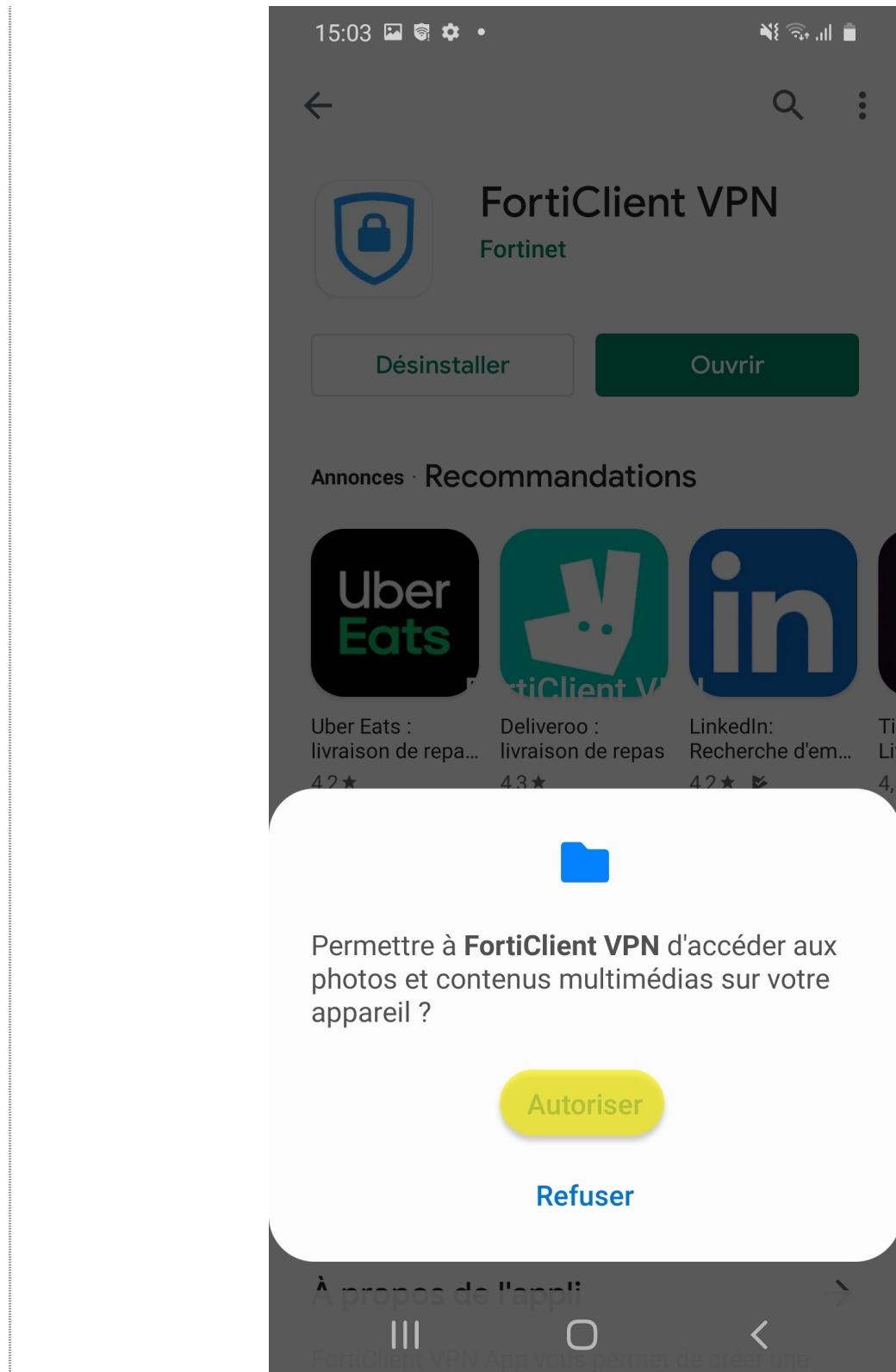
Professional

Notes et avis ⓘ

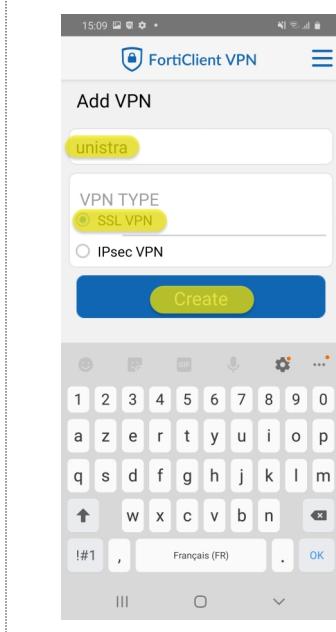
2 Ouvrir l'application et valider les conditions d'utilisations.





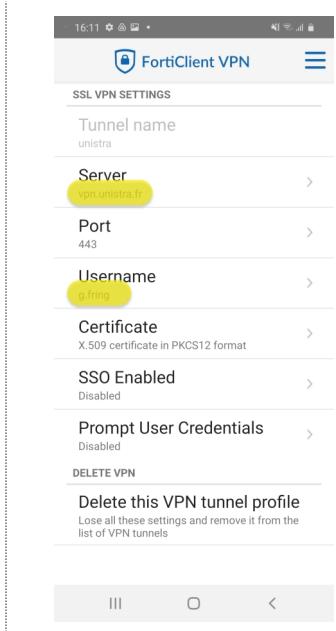


3 Renseigner ensuite les champs (cf. ci-dessous) et cliquer sur **Create**.



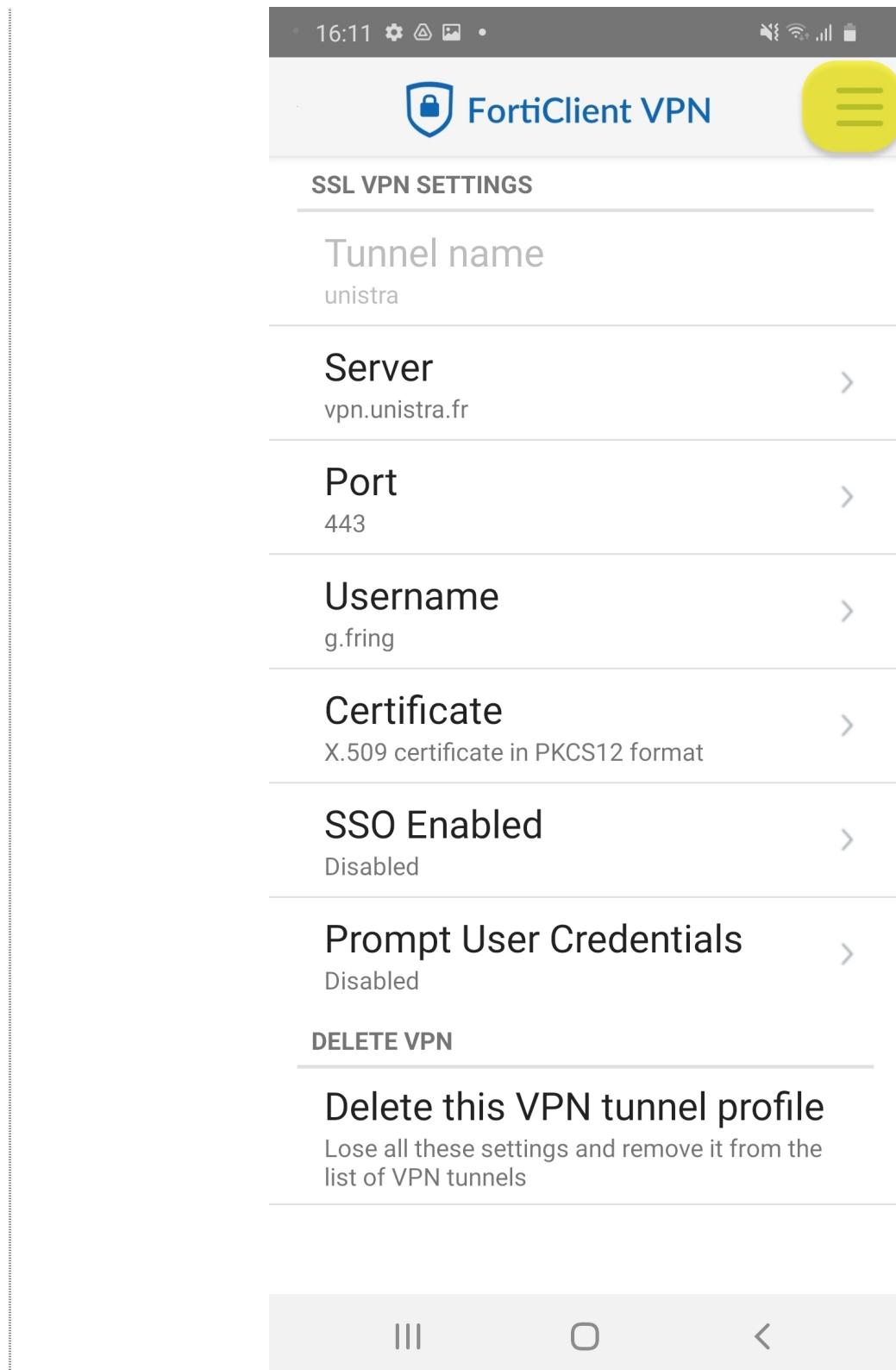
- **Unistra**
- **VPN Type** : SSL VPN

4 Puis, renseigner les champs (cf. ci-dessous).

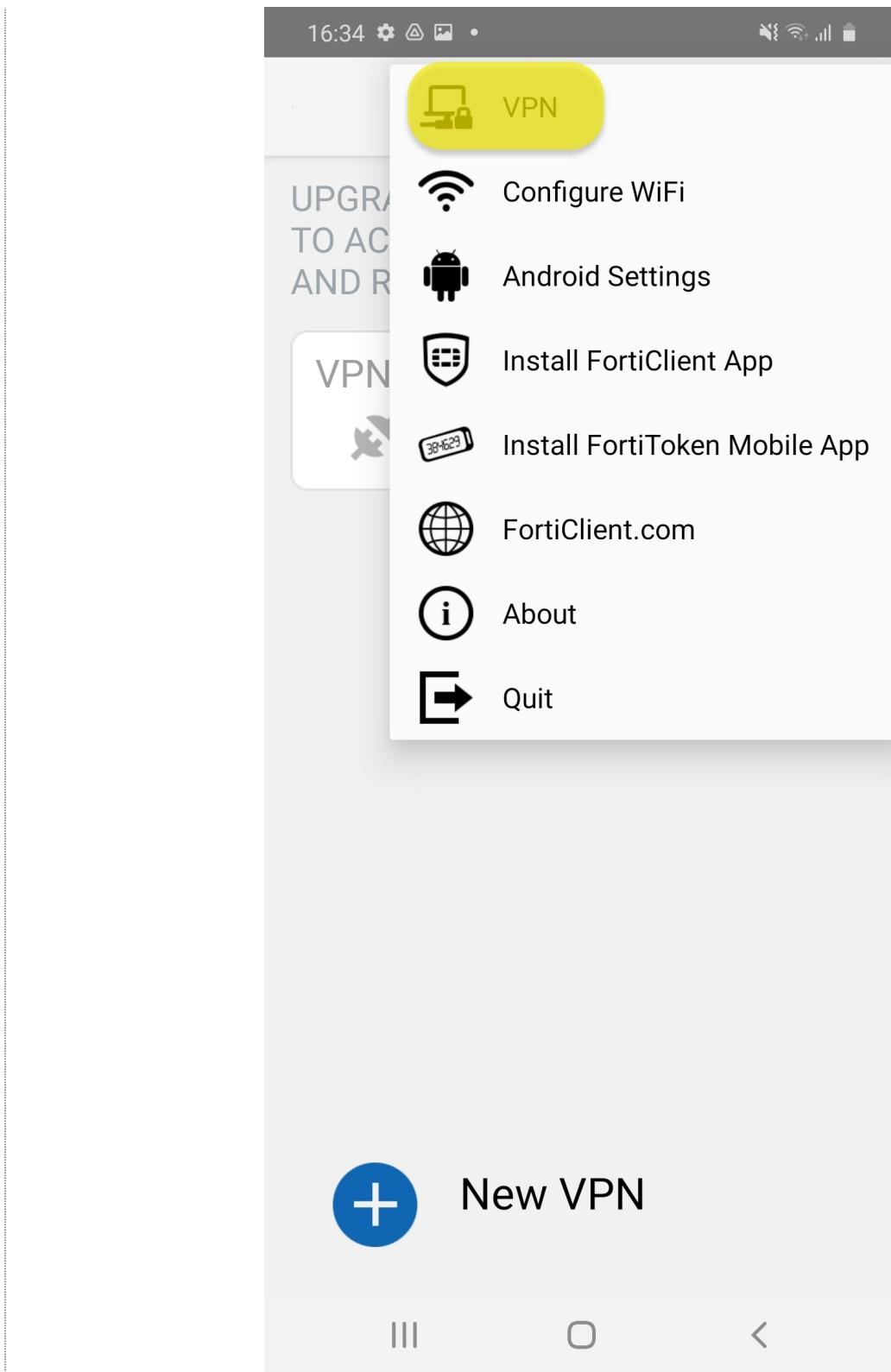


- **Server** : <https://vpn.unistra.fr>
- **Username** : login Unistra

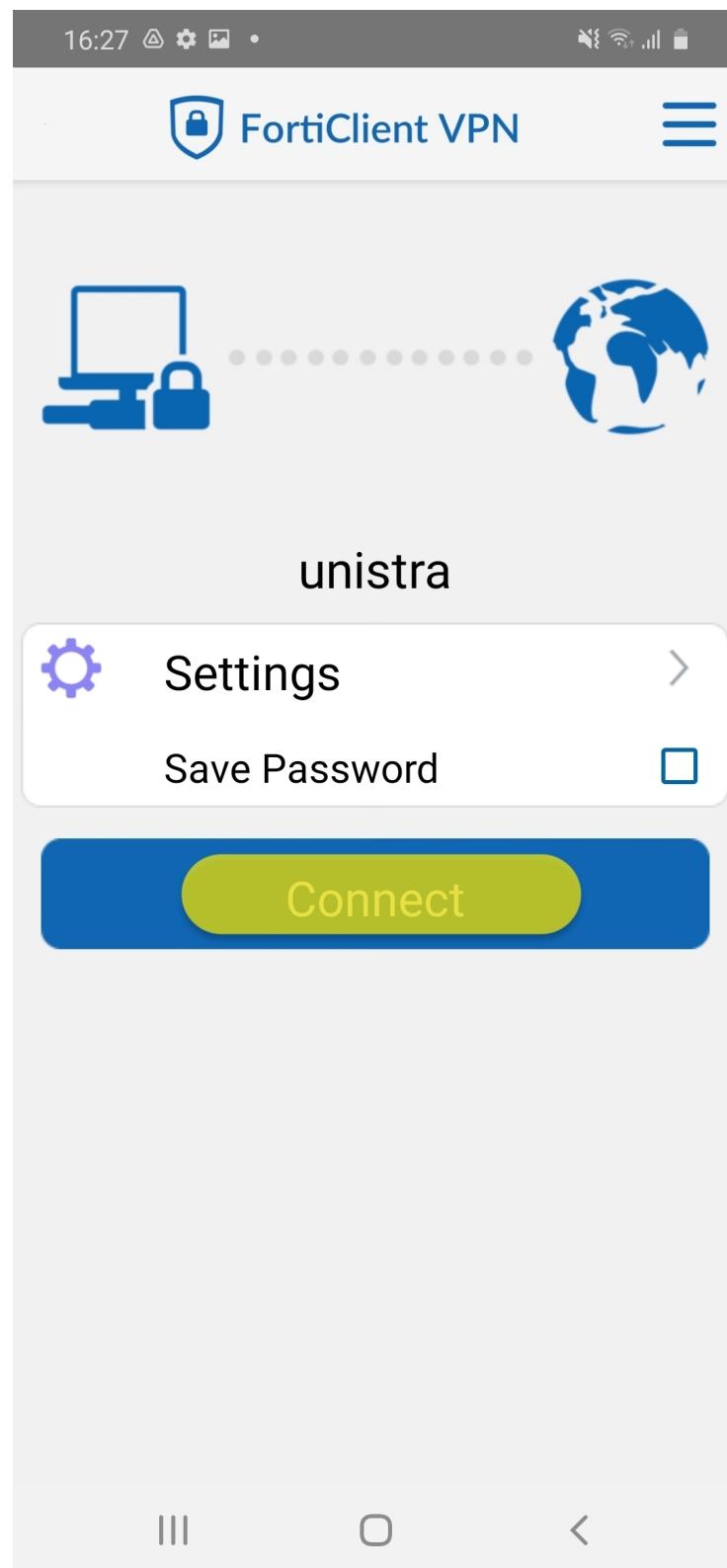
5 Cliquez sur le menu à 3 barres en haut à droite.



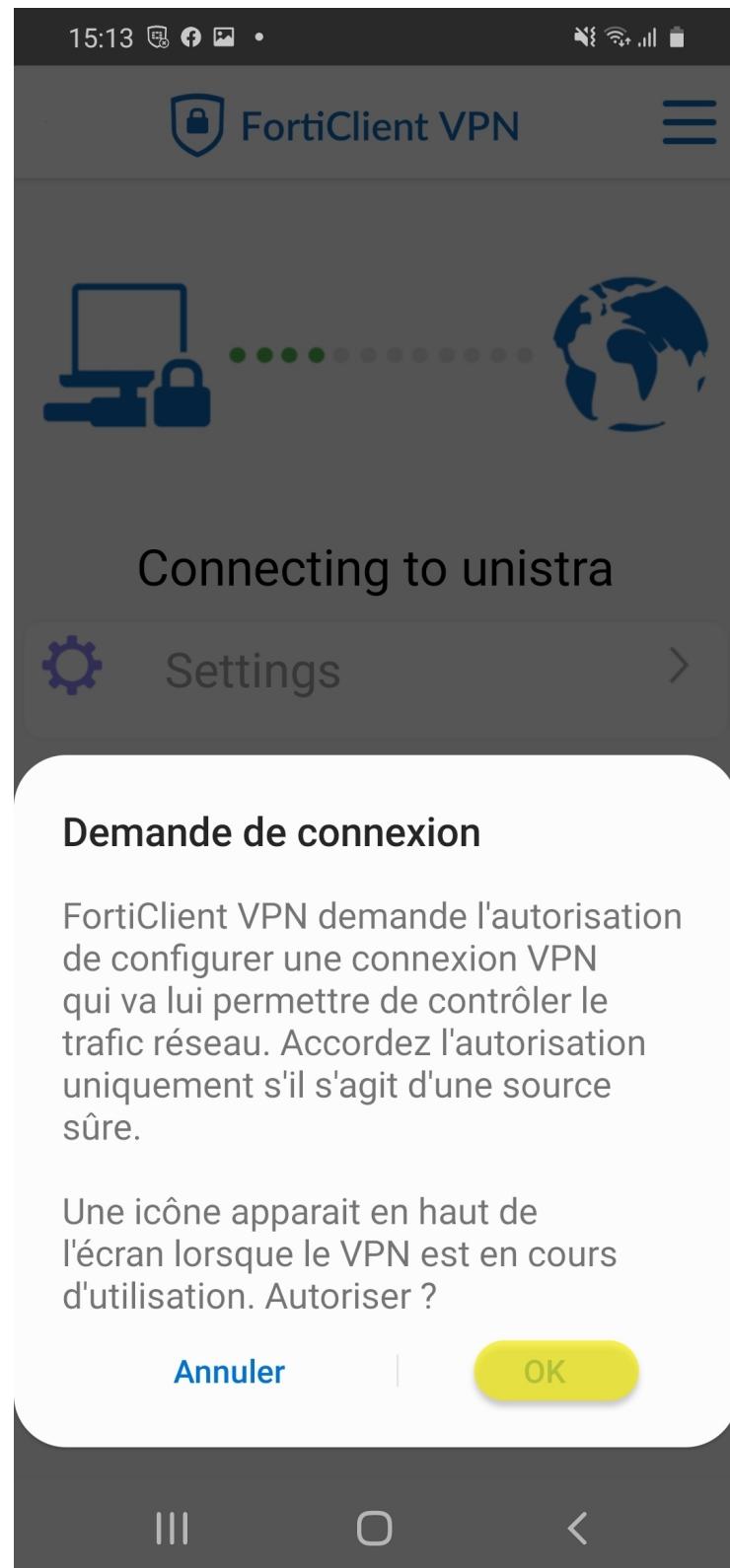
6 Validez en appuyant sur  VPN .



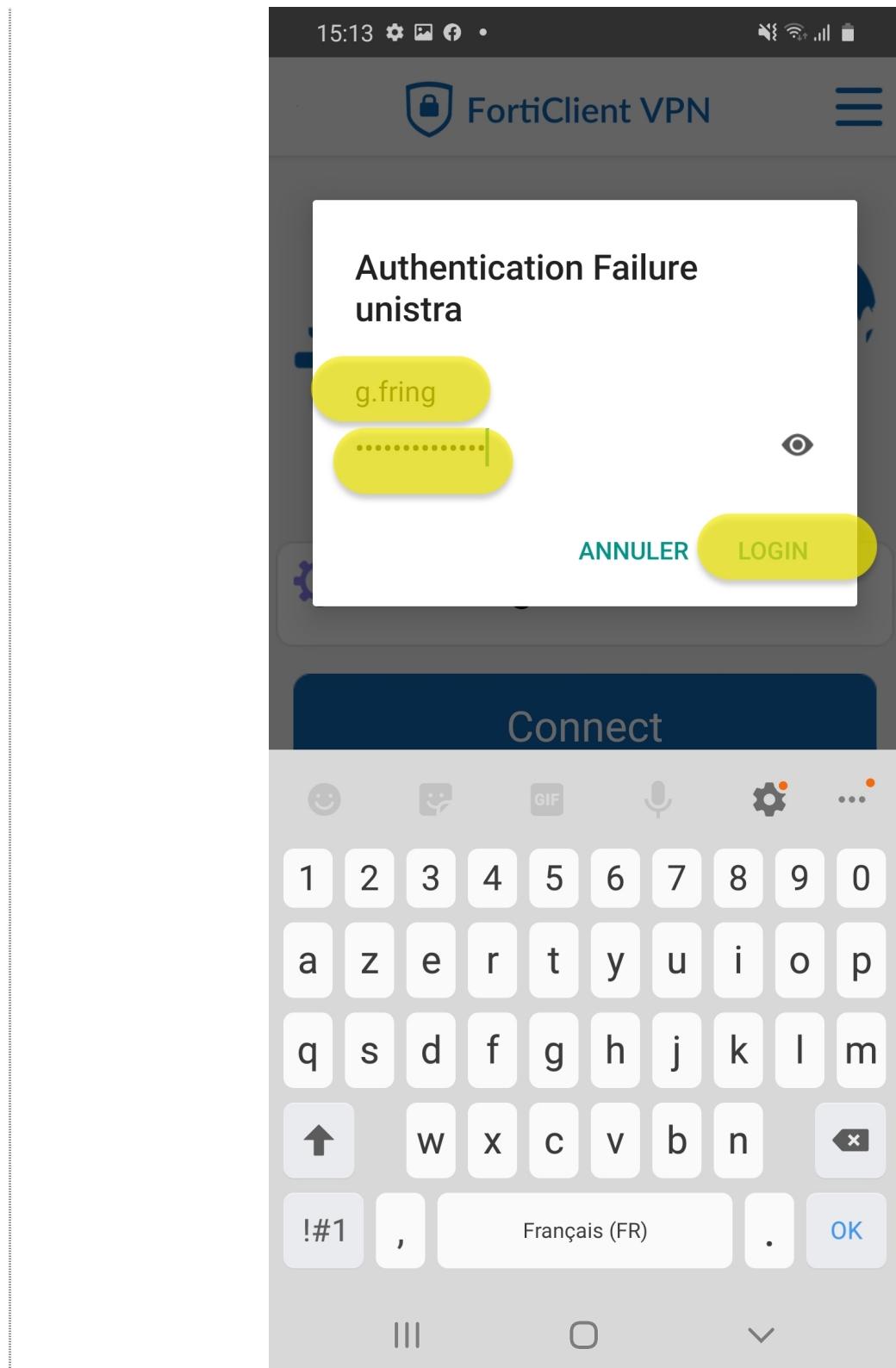
7 Se connecter en appuyant sur **Connect**.



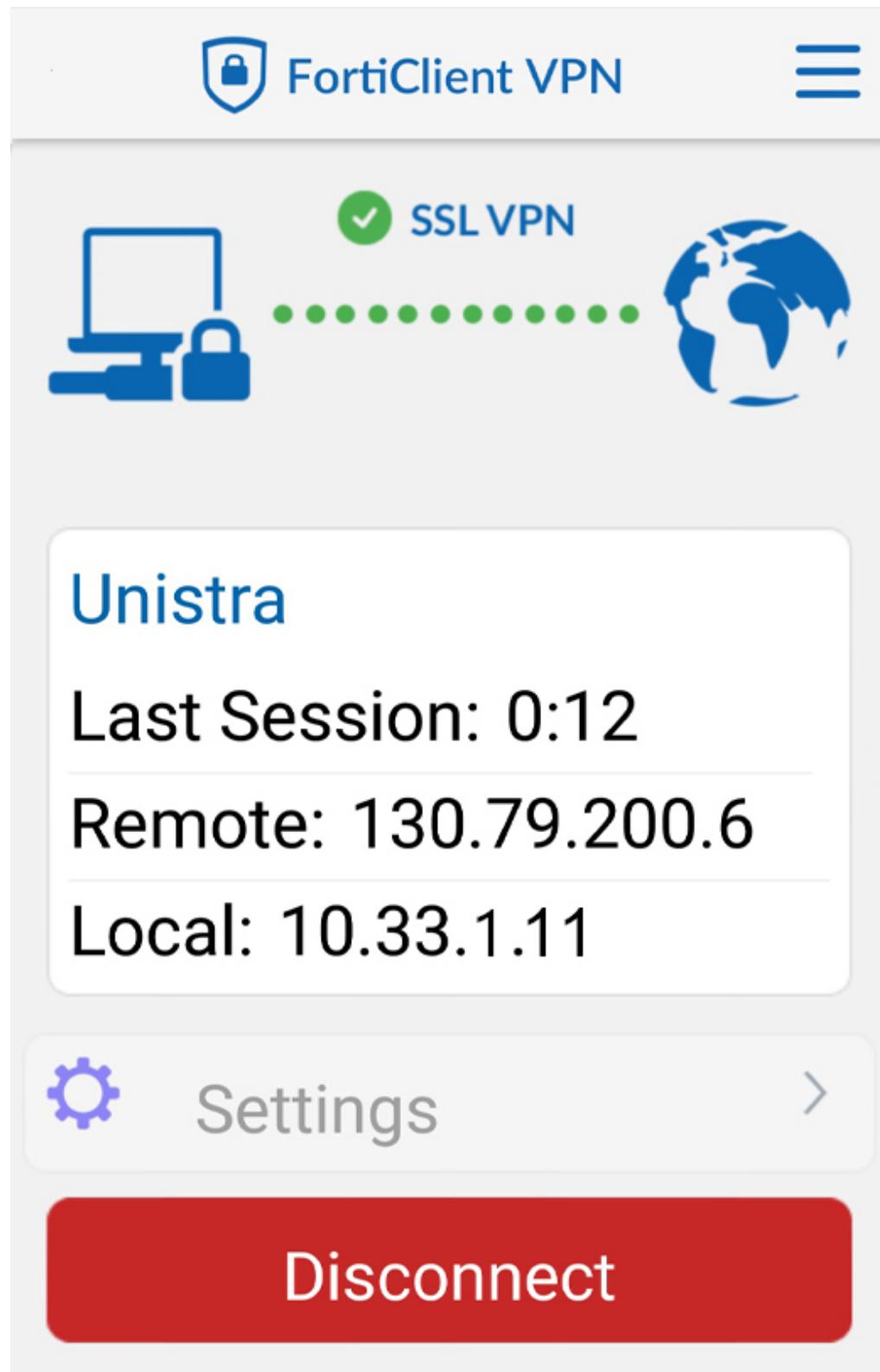
8 Cliquez sur **OK**



9 Saisir ses **identifiants** Unistra et cliquez sur **Login**.



Vous êtes à présent connecté au VPN.



5. CONFIGURATION POUR UN APPAREIL LINUX

5.1. Via le terminal de commande



Ces procédures ont été réalisées pour une distribution de type Debian/Ubuntu.



Autres distributions

Le client est également disponible sur d'autres distributions : n'hésitez pas à le chercher dans votre gestionnaire de paquets habituel.



Les commandes suivantes sont à saisir dans un terminal.



Installation du client OpenFortiVPN via le gestionnaire de paquet.

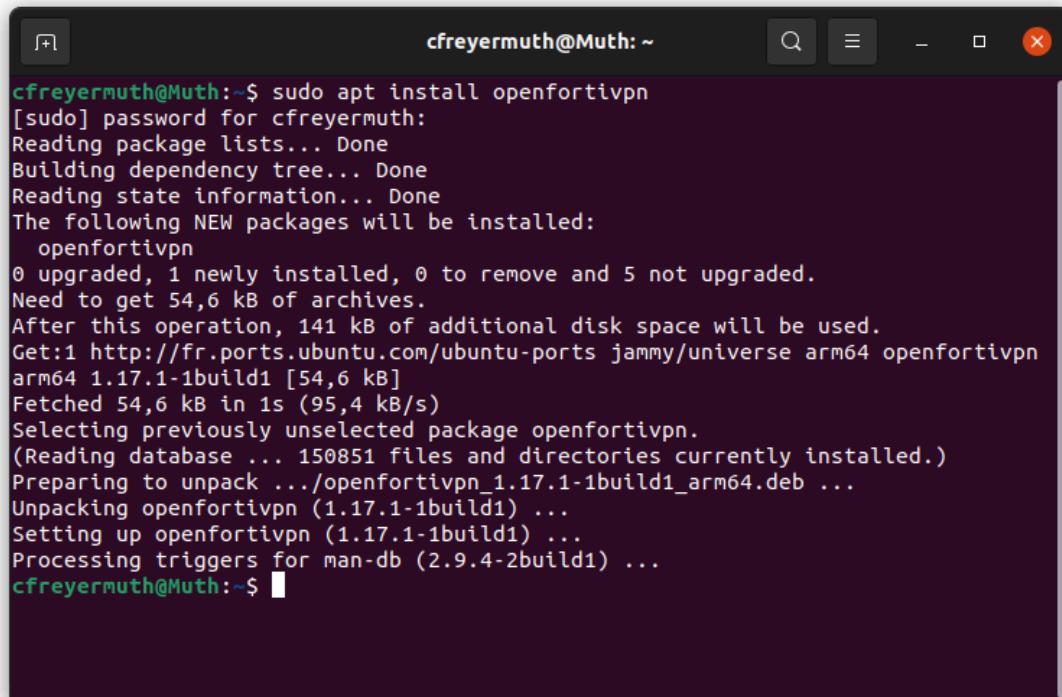
- 1 Lancez l'installation du client

```
sudo apt install openfortivpn
```

A screenshot of a terminal window titled 'cfreyermuth@Muth: ~'. The window shows the command 'sudo apt install openfortivpn' being typed, followed by '[sudo] password for cfreyermuth:'. The terminal has a dark background and light-colored text. The window title bar includes icons for minimize, maximize, and close.

- 2 Cette opération nécessite une élévation de privilèges, saisissez le **mot de passe** de votre poste

Le client est correctement installé.

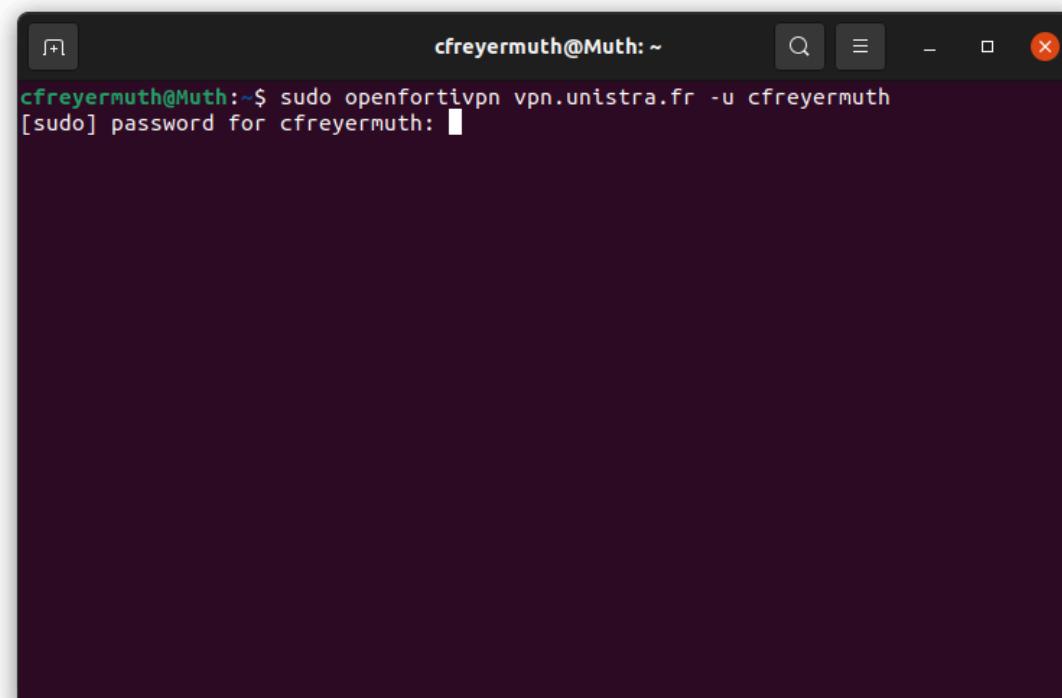


```
cfreyermuth@Muth:~$ sudo apt install openfortivpn
[sudo] password for cfreyermuth:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  openfortivpn
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 54,6 kB of archives.
After this operation, 141 kB of additional disk space will be used.
Get:1 http://fr.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 openfortivpn
arm64 1.17.1-1build1 [54,6 kB]
Fetched 54,6 kB in 1s (95,4 kB/s)
Selecting previously unselected package openfortivpn.
(Reading database ... 150851 files and directories currently installed.)
Preparing to unpack .../openfortivpn_1.17.1-1build1_arm64.deb ...
Unpacking openfortivpn (1.17.1-1build1) ...
Setting up openfortivpn (1.17.1-1build1) ...
Processing triggers for man-db (2.9.4-2build1) ...
cfreyermuth@Muth:~$
```

Se connecter au VPN

1 Lancez le client OpenFortiVPN

```
sudo openfortivpn vpn.unistra.fr:443 -u USER
```



```
cfreyermuth@Muth:~$ sudo openfortivpn vpn.unistra.fr -u cfreyermuth
[sudo] password for cfreyermuth: ■
```



Le champ "**USER**" est à remplacer par son nom d'utilisateur unistra.



Vous pouvez retrouver votre compte unistra sur <https://quisuisje.unistra.fr>

2 Cette opération nécessite une élévation de priviléges, saisissez le **mot de passe** de votre poste

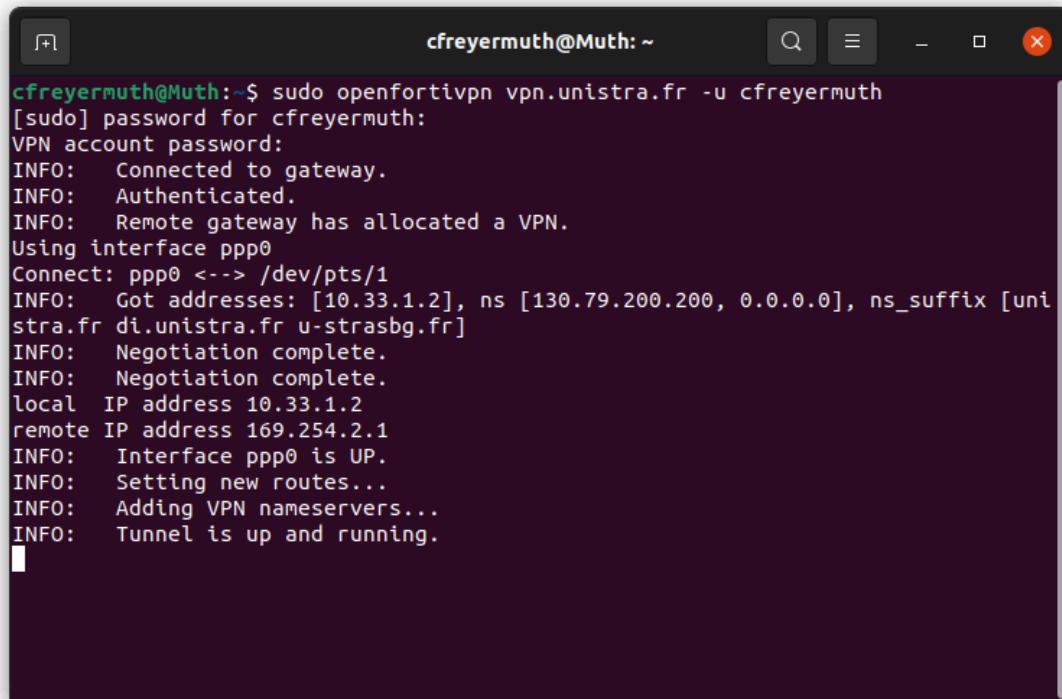
3 Saisissez le **mot de passe** de votre compte Unistra

A screenshot of a terminal window titled "cfreyermuth@Muth: ~". The window contains the following text:

```
cfreyermuth@Muth:~$ sudo openfortivpn vpn.unistra.fr -u cfreyermuth
[sudo] password for cfreyermuth:
VPN account password: [REDACTED]
```

The terminal window has a dark background and light-colored text. The password fields are redacted with black squares.

Vous êtes connecté au VPN



```
cfreyermuth@Muth:~$ sudo openfortivpn vpn.unistra.fr -u cfreyermuth
[sudo] password for cfreyermuth:
VPN account password:
INFO: Connected to gateway.
INFO: Authenticated.
INFO: Remote gateway has allocated a VPN.
Using interface ppp0
Connect: ppp0 <--> /dev/pts/1
INFO: Got addresses: [10.33.1.2], ns [130.79.200.200, 0.0.0.0], ns_suffix [uni
stra.fr di.unistra.fr u-strasbg.fr]
INFO: Negotiation complete.
INFO: Negotiation complete.
local IP address 10.33.1.2
remote IP address 169.254.2.1
INFO: Interface ppp0 is UP.
INFO: Setting new routes...
INFO: Adding VPN nameservers...
INFO: Tunnel is up and running.
```



(Optionnel) Connexion au VPN via un fichier de configuration.

- 1 Créez un fichier de configuration pour le client

```
vim /etc/openfortivpn/config
```

- 2 Insérez les paramètres suivant dans le fichier

```
host = vpn.unistra.fr
port = 443
username = USER
```

- 3 Lancez le client

```
sudo openfortivpn -c /etc/openfortivpn/config
```



Vous aurez à renseigner le mot de passe de votre poste puis celui de votre compte Unistra.

Vous êtes connecté

5.2. Via l'interface graphique



Ces procédures ont été réalisées pour une distribution de type Debian/Ubuntu.



Autres distributions

Le client est également disponible sur d'autres distributions : n'hésitez pas à le chercher dans votre gestionnaire de paquets habituel.



Les commandes suivantes sont à saisir dans un terminal.



Installation du client OpenFortiVPN via le gestionnaire de paquet.

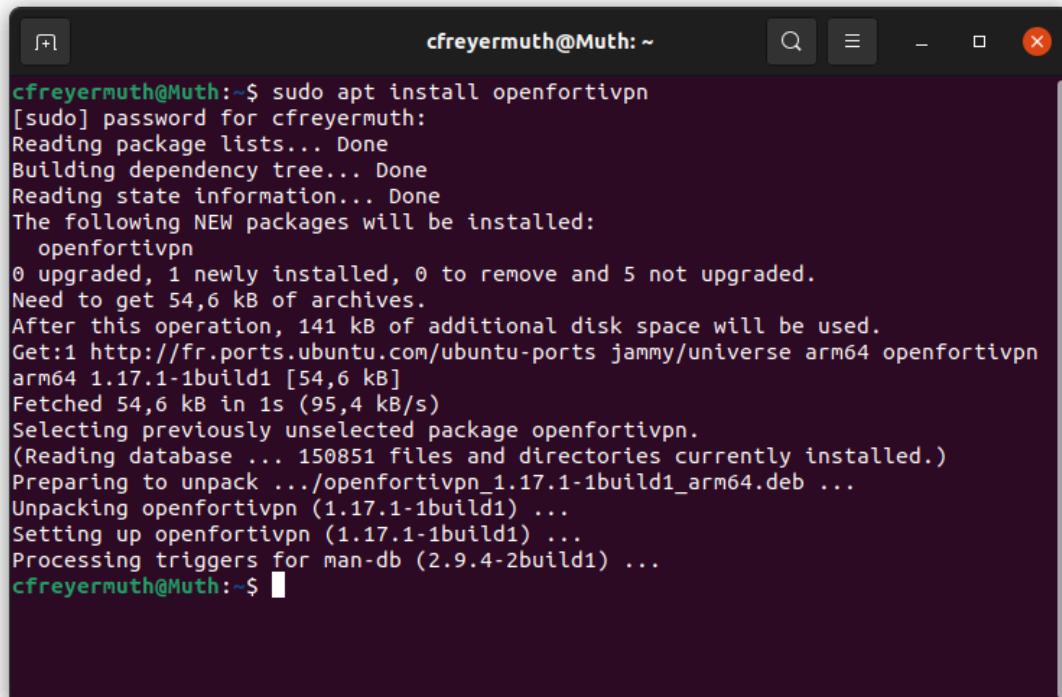
1 Lancez l'installation du client

```
sudo apt install openfortivpn
```

The screenshot shows a terminal window with a dark background. At the top, the title bar displays the user's name 'cfreyermuth@Muth: ~'. Below the title bar, there is a standard Linux terminal interface with icons for closing, minimizing, and maximizing. The main area of the terminal shows the command 'sudo apt install openfortivpn' being typed in. The text is white on a dark background. A password prompt '[sudo] password for cfreyermuth:' is visible, with the password field containing several dots to indicate it has been entered.

2 Cette opération nécessite une élévation de privilèges, saisissez le **mot de passe** de votre poste

Le client est correctement installé.

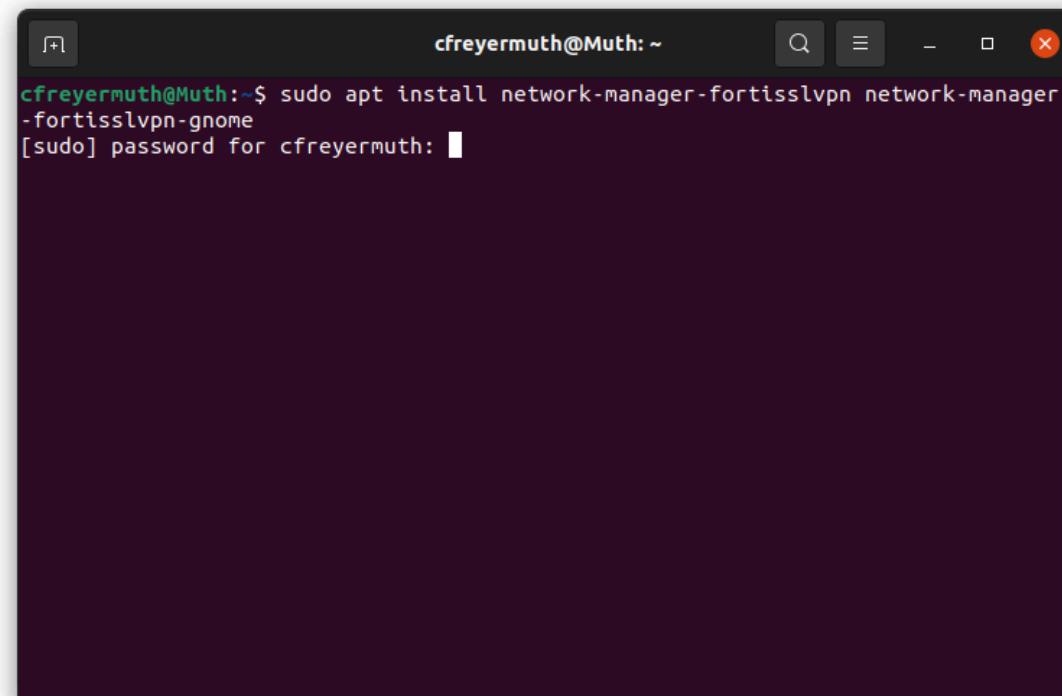


```
cfreyermuth@Muth:~$ sudo apt install openfortivpn
[sudo] password for cfreyermuth:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  openfortivpn
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 54,6 kB of archives.
After this operation, 141 kB of additional disk space will be used.
Get:1 http://fr.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 openfortivpn
arm64 1.17.1-1build1 [54,6 kB]
Fetched 54,6 kB in 1s (95,4 kB/s)
Selecting previously unselected package openfortivpn.
(Reading database ... 150851 files and directories currently installed.)
Preparing to unpack .../openfortivpn_1.17.1-1build1_arm64.deb ...
Unpacking openfortivpn (1.17.1-1build1) ...
Setting up openfortivpn (1.17.1-1build1) ...
Processing triggers for man-db (2.9.4-2build1) ...
cfreyermuth@Muth:~$
```

Installation des paquets complémentaires

1 Lancez l'installation des paquets

```
sudo apt install network-manager-fortisslvpn network-
manager-fortisslvpn-gnome
```



```
cfreyermuth@Muth:~$ sudo apt install network-manager-fortisslvpn network-manager-
-fortisslvpn-gnome
[sudo] password for cfreyermuth: ■
```

- 2** Cette opération nécessite une élévation de privilèges, saisissez le **mot de passe** de votre poste

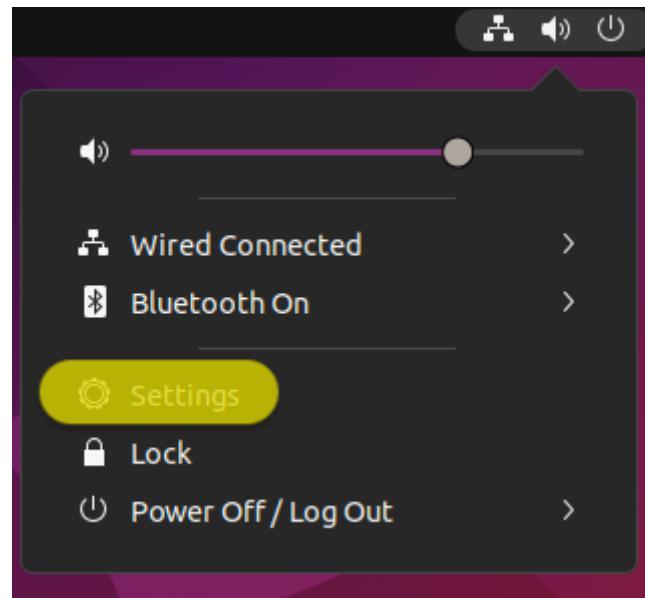
Les paquets sont correctement installés.

```
cfreyermuth@Muth:~$ sudo apt install network-manager-fortisslvpn network-manager-fortisslvpn-gnome
[sudo] password for cfreyermuth:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  network-manager-fortisslvpn network-manager-fortisslvpn-gnome
0 upgraded, 2 newly installed, 0 to remove and 5 not upgraded.
Need to get 77,6 kB of archives.
After this operation, 473 kB of additional disk space will be used.
Get:1 http://fr.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 network-manager-fortisslvpn arm64 1.2.10-0ubuntu2 [59,7 kB]
Get:2 http://fr.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 network-manager-fortisslvpn-gnome arm64 1.2.10-0ubuntu2 [17,9 kB]
Fetched 77,6 kB in 1s (114 kB/s)
Selecting previously unselected package network-manager-fortisslvpn.
(Reading database ... 150862 files and directories currently installed.)
Preparing to unpack .../network-manager-fortisslvpn_1.2.10-0ubuntu2_arm64.deb ...
Unpacking network-manager-fortisslvpn (1.2.10-0ubuntu2) ...
Selecting previously unselected package network-manager-fortisslvpn-gnome.
Preparing to unpack .../network-manager-fortisslvpn-gnome_1.2.10-0ubuntu2_arm64.deb ...
Unpacking network-manager-fortisslvpn-gnome (1.2.10-0ubuntu2) ...
Setting up network-manager-fortisslvpn (1.2.10-0ubuntu2) ...
Setting up network-manager-fortisslvpn-gnome (1.2.10-0ubuntu2) ...
Processing triggers for dbus (1.12.20-2ubuntu2) ...
cfreyermuth@Muth:~$
```

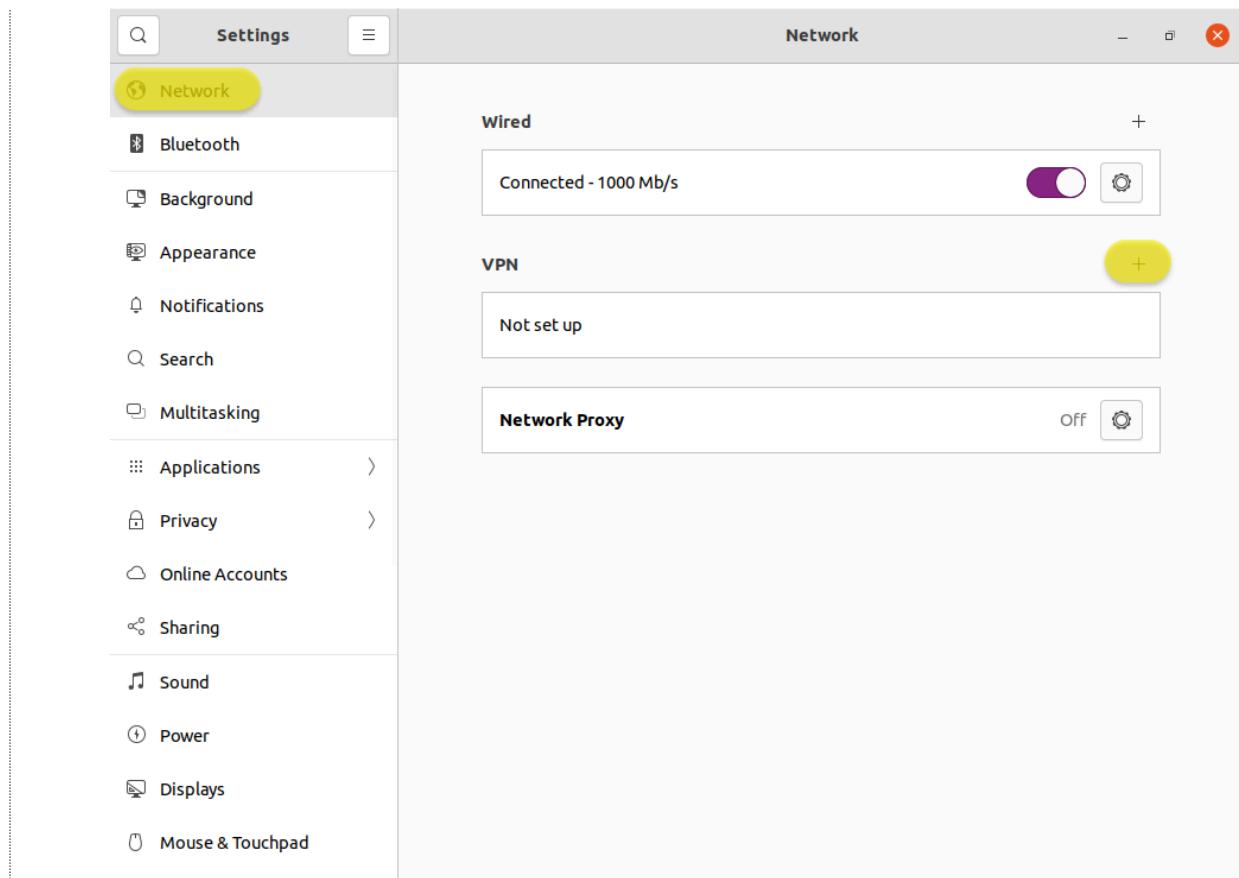
Paramétrage graphique

- 1** Cliquez sur la barre des menues en haut à droite de votre écran

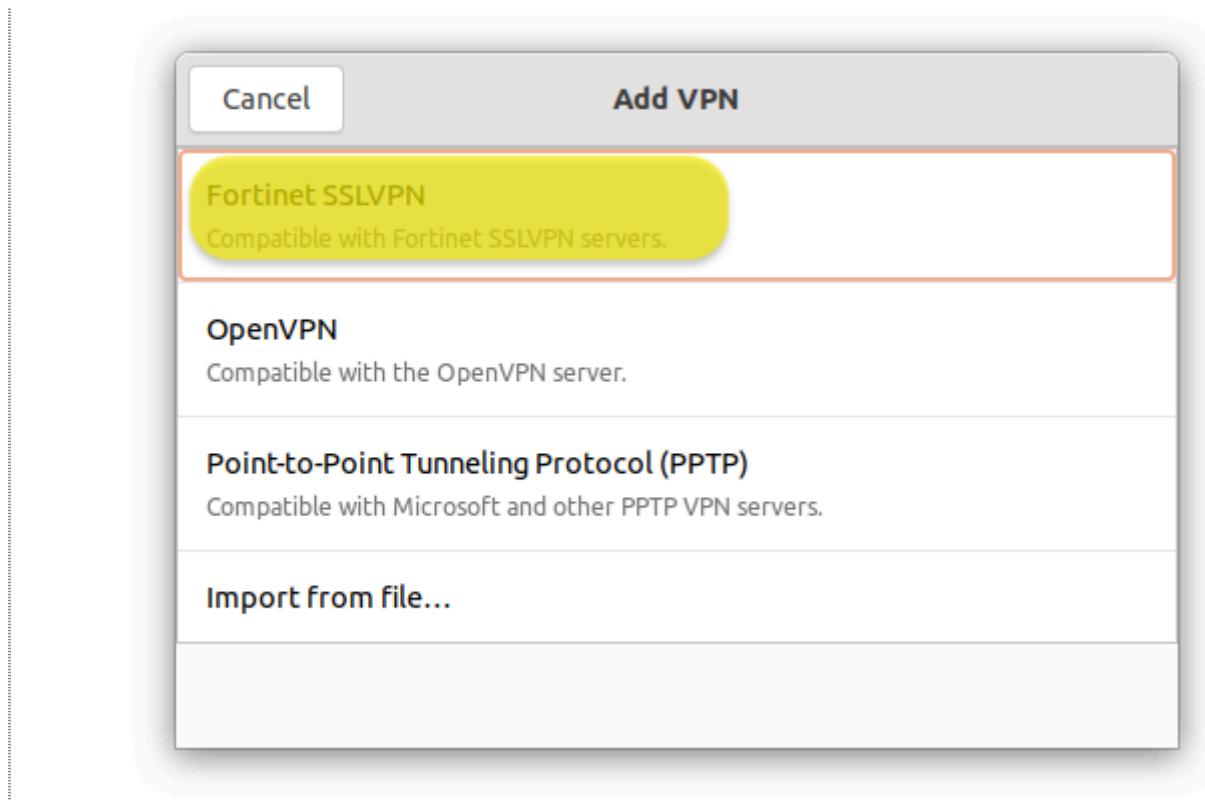
Puis cliquez sur **Settings**



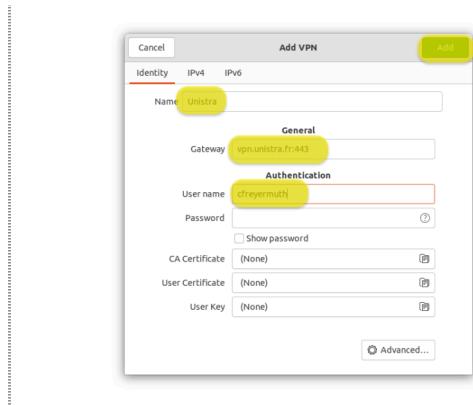
2 Dans l'onglet **Network** ajoutez une nouvelle configuration VPN via le bouton +



3 Cliquez sur **Fortinet SSLVPN**



4 Renseignez les champs suivant puis cliquez sur **Add**



- **Name:** Unistra
- **Gateway :** vpn.unistra.fr:443
- **Username :** Identifiant de votre compte unistra

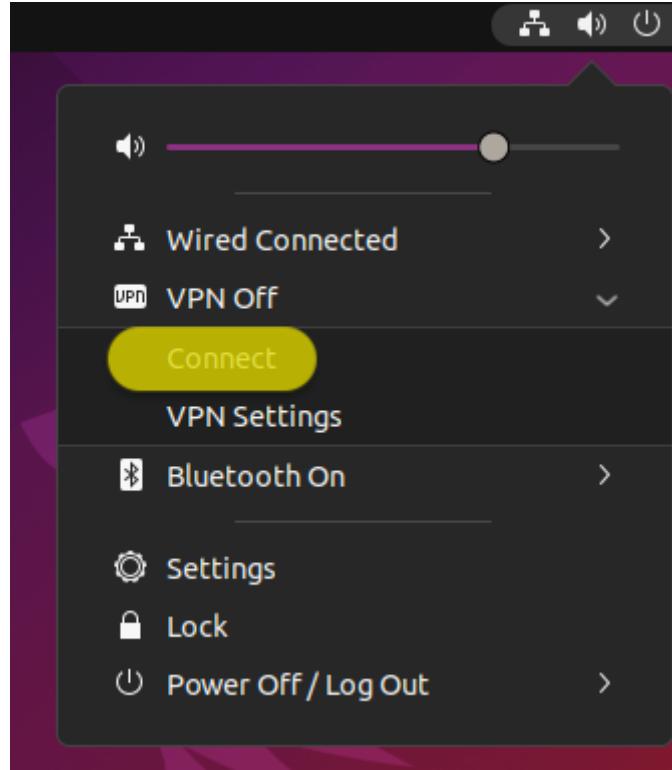
Votre connexion VPN à été paramétrée



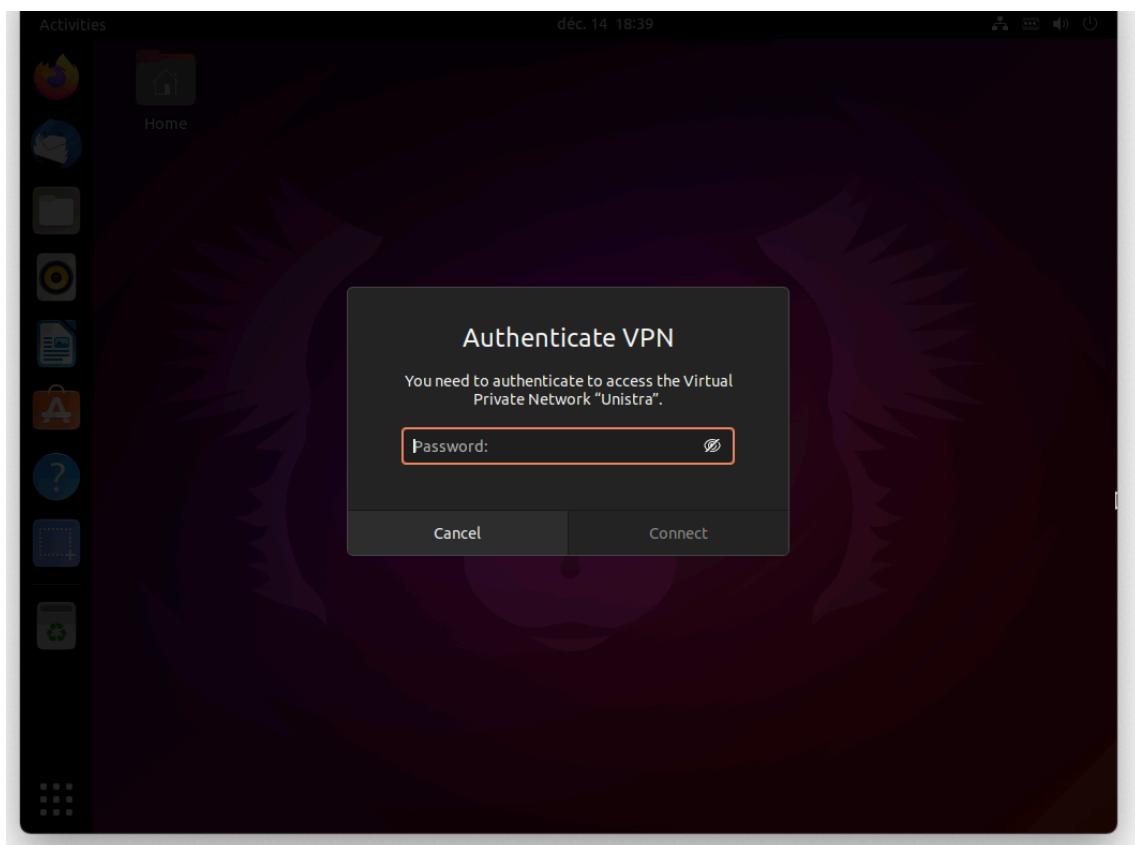
Connexion au VPN

1 Cliquez sur la barre des menus en haut à droite de votre écran

Puis cliquez sur **VPN** et sur **Connect**



2 Saisissez le **mot de passe** de votre compte Unistra



Vous êtes connecté au VPN

6. ASSISTANCE

FAQ générale - Réponses aux questions fréquentes sur le service VPN.



Cliquer sur les phrases pour afficher une solution à votre problème.



1

Comment utiliser le service d'accès à distance sur Osiris ?

Pour utiliser ce service, vous devez installer un **logiciel spécifique**, téléchargeable sur le site de la Direction Informatique après vous être authentifié(e) avec vos identifiants ENT.

2

Est-ce que le logiciel d'accès à distance est payant ?

Non. Le logiciel d'accès est gratuit pour les utilisateurs d'Osiris.

3

Est-ce que j'ai encore besoin de mon fournisseur d'accès à Internet ?

Oui. Le service d'accès à distance sur Osiris n'est pas un service d'accès à Internet. C'est un service vous permettant une fois connecté(e) sur Internet, d'accéder aux ressources telles que les publications scientifiques ou à l'intranet de votre laboratoire et ce en vous donnant une adresse dans le réseau Osiris.

4

Quels sont les systèmes d'exploitation qui supportent le client « VPN » d'accès à distance sur Osiris ?

FortiClientVPN

Le client VPN Fortinet est disponible pour les systèmes suivants :

- Microsoft Windows : 11 (64-bit), 10 (32-bit and 64-bit), 8.1 (32-bit and 64-bit), 7 (32-bit and 64-bit)
- Apple MacOS : 10.15 (Catalina), 11.x (Big Sur), 12.x (Monterey)
- Linux : Ubuntu 18.04 et plus
- iPhone, iPad, et iPodTouch : iOS 9.0 et plus
- Android version 5.0 et plus

5

Est-ce que je peux utiliser d'autres clients VPN pour me connecter au service d'accès à distance sur Osiris ?

La Direction du Numérique préconise de suivre scrupuleusement les procédures d'installations et n'a pas validé le fonctionnement d'autre clients, et ne peut garantir leur bon fonctionnement.

6

Quel trafic passe dans la connexion VPN qui me relie à Osiris ?

Tout le trafic réseau, à l'exception du trafic vers le réseau local, passe par la connexion VPN.

7

Dans quel réseau IP d'Osiris mon ordinateur est-il ?

Cela dépend de votre profil de connexion.

- Si votre service/composante/laboratoire a activé l'option de vpn-lab, votre ordinateur obtient une adresse IP dans votre réseau habituel de service /composante/laboratoire.
- Sinon, une fois connecté(e) au service d'accès à distance sur Osiris, votre ordinateur obtient son adresse IP dans le réseau vpn-default 130.79.1.248/24.

Vous pouvez visualiser votre ip sur la page de « Test de connexion VPN [<http://vpnadr.unistra.fr/>] »

8

Comment puis je vérifier que ma connexion avec le service d'accès à distance sur Osiris est correcte ?

Vous pouvez tester votre connexion VPN sur la page de « Test de connexion VPN [<http://vpnadr.unistra.fr/>] »

9

Lorsque je démarre le client d'accès à distance sur Osiris, mes applications réseaux en cours ne fonctionnent plus, est ce normal ?

C'est possible. Lorsque vous vous connectez au service d'accès à distance sur Osiris, toutes vos connexions passent par le tunnel VPN qui vient d'être créé. Si vous aviez lancé des applications utilisant le réseau, elles sont coupées du réseau.

FAQ technique - Réponses aux questions fréquentes sur les problèmes du client VPN.



Cliquer sur les phrases pour afficher une solution à votre problème.

Problèmes d'installation

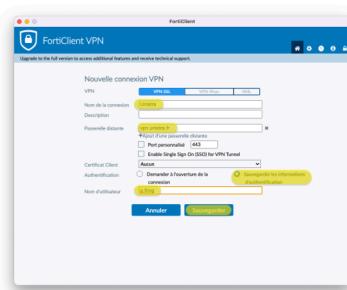
1

Je n'arrive pas à installer le logiciel ?

Vérifiez que vous avez les droits suffisants. Vous devez être administrateur de votre poste.

2

L'application FortiClient est elle configuré correctement ?

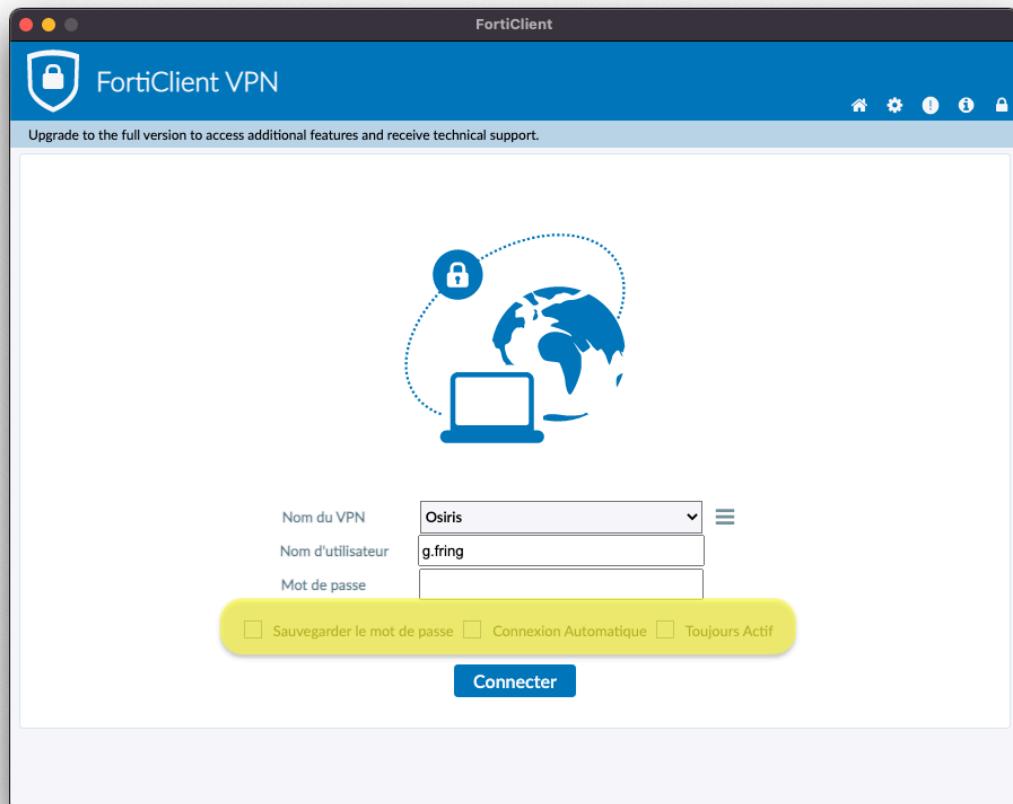


- **VPN :** VPN SSL
- **Nom de la connexion :** Unistra
- **Passerelle distante :** vpn.unistra.fr
- **Port personnalisé :** cocher la case et saisir **443**
- **Certificat Client :** Aucun
- **Authentification :** Sauvegarder les informations d'authentification
- **Nom d'utilisateur :** Identifiant de votre compte unistra

3

Est il possible d'activer les options Sauvegarder le mot de passe , Connexion Automatique , Toujours Actif

Malheureusement non, notre version de FortiClient ne le permet pas.



Problèmes de connexion

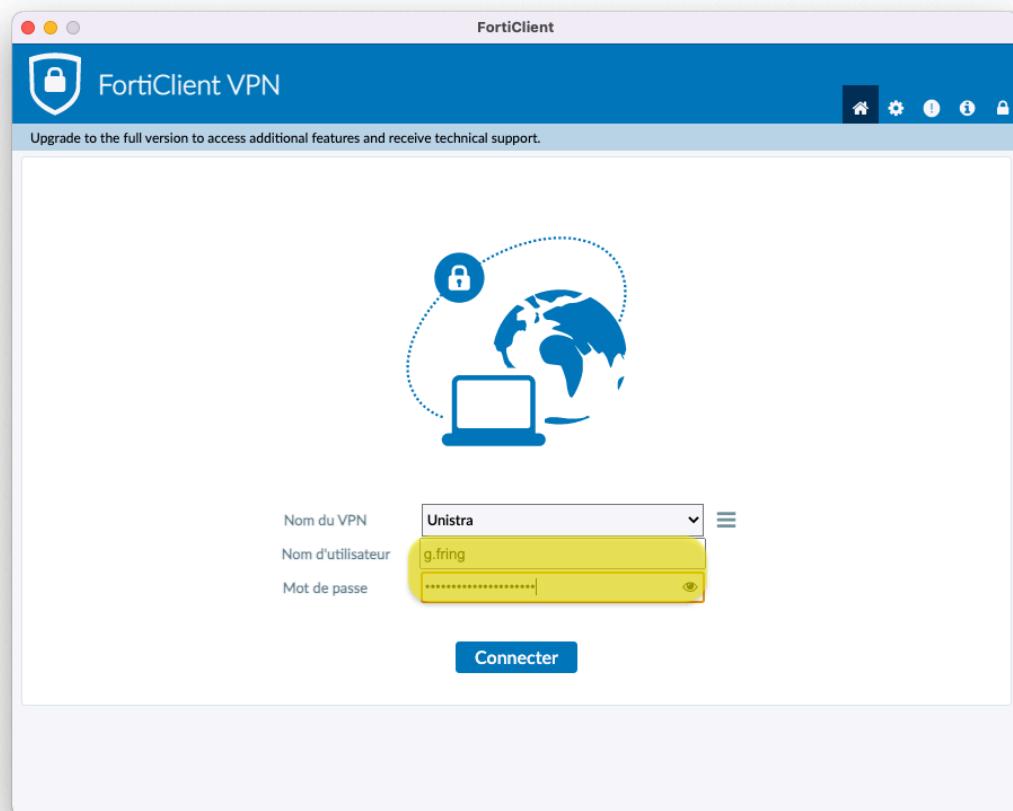
1

 Comment me connecter au service VPN lorsqu'il est installé ?

Via l'application **FortiClient**



1. Cliquez sur l'icône de l'application pour démarrer le client.



2. La page suivante apparaît, entrez vos identifiants de connexion puis cliquez sur **Connecter**.

2

Que signifie le message d'erreur : "Network Error. The request timed out." ?

L'application n'arrive pas à joindre le serveur de l'université.

Vérifiez que vous êtes connecté à internet et que vous arrivez naviguez correctement.

3

Que signifie le message d'erreur : "Network Error. Can not connect to VPN server" ?

L'application n'arrive pas à joindre le serveur de l'université. Il pourrait être mal renseigner dans les paramètres.

Vérifiez que votre application est correctement configuré :

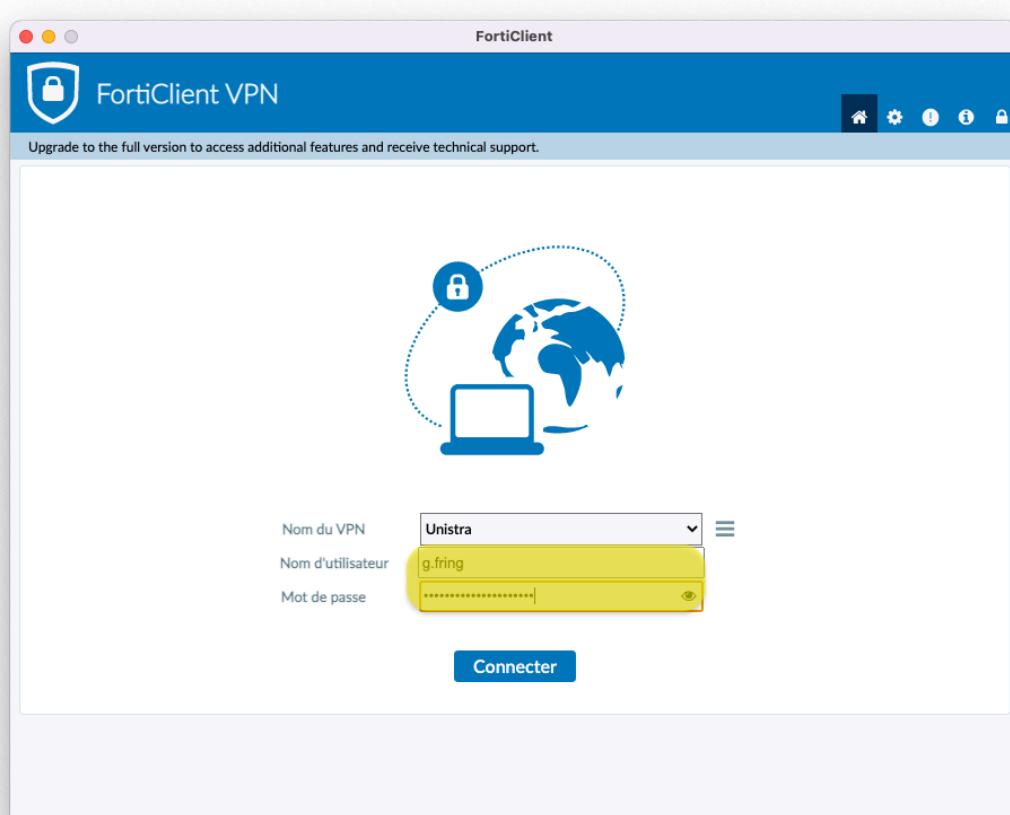


- **VPN : VPN SSL**
- **Nom de la connexion :** Unistra
- **Passerelle distante :** vpn.unistra.fr
- **Port personnalisé :** cocher la case et saisir **443**
- **Certificat Client :** Aucun
- **Authentification :** Sauvegarder les informations d'authentification
- **Nom d'utilisateur :** Identifiant de votre compte unistra

4

Que signifie le message d'erreur : "Login failed. Insufficient credential(s)" ?

Vos identifiants de connexion Unistra n'ont pas été reconnus par le serveur.
Vérifiez votre couple login/mot de passe



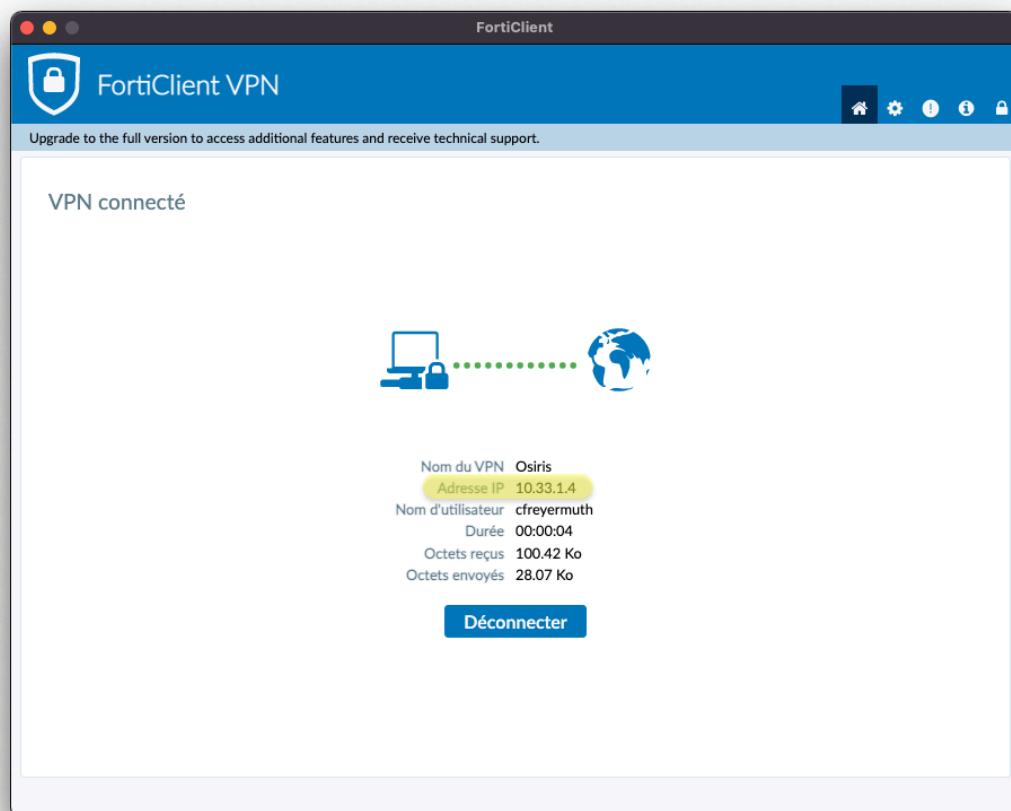
Vous pouvez retrouver votre nom d'utilisateur (login) sur <https://quisuisje.unistra.fr>.

Vous avez perdu votre mot de passe, accéder à la procédure de réinitialisation [<https://pan-dore.unistra.fr/recovery/all/>].

5

 L'adresse IP affiché par le client ne correspond pas à celle de mon réseau.

C'est normal, le client VPN fonctionne en NAT, l'adresse IP affiché par le client en 10.33.0.0/16 ne correspond pas à l'adresse publique réel de sortie.



Vous pouvez visualiser votre ip publique sur la page de « Test de connexion VPN [<http://vpn.adr.unistra.fr/>] »

6

 Pourquoi la connexion se bloque à 98% et ne finalise jamais ?

Il se peut que votre version de l'application soit pas à jour ou présente un défaut d'installation.

1. Désinstaller proprement l'application FortiClient
2. Redémarrer votre poste
- 3 Réinstallez l'application FortiClient en suivant scrupuleusement nos procédures.

7

 Pourquoi, sous MacOS, l'application se fige sur un écran blanc ?

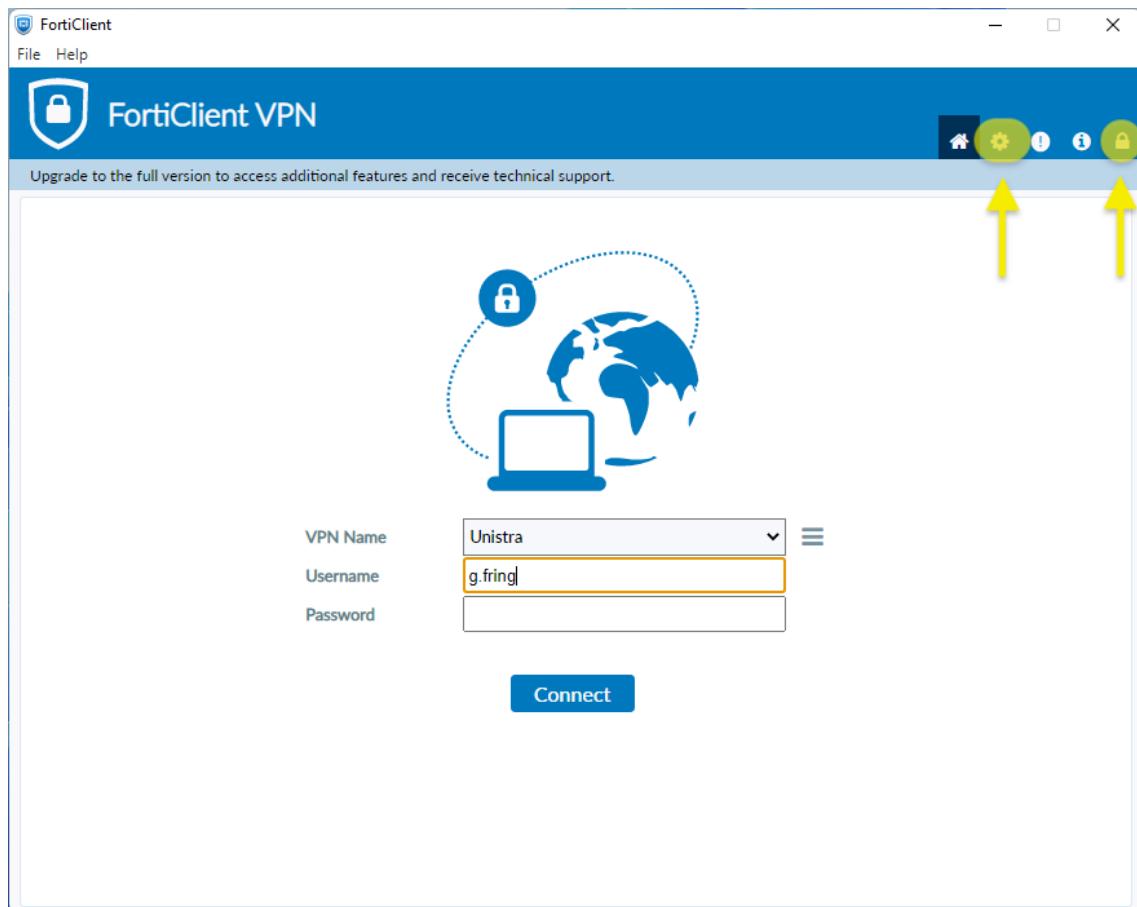
Vérifiez les paramètres de sécurité de macOS à partir de la section 2.6 de  cette procédure. ^[p.13]

Problèmes de lenteur

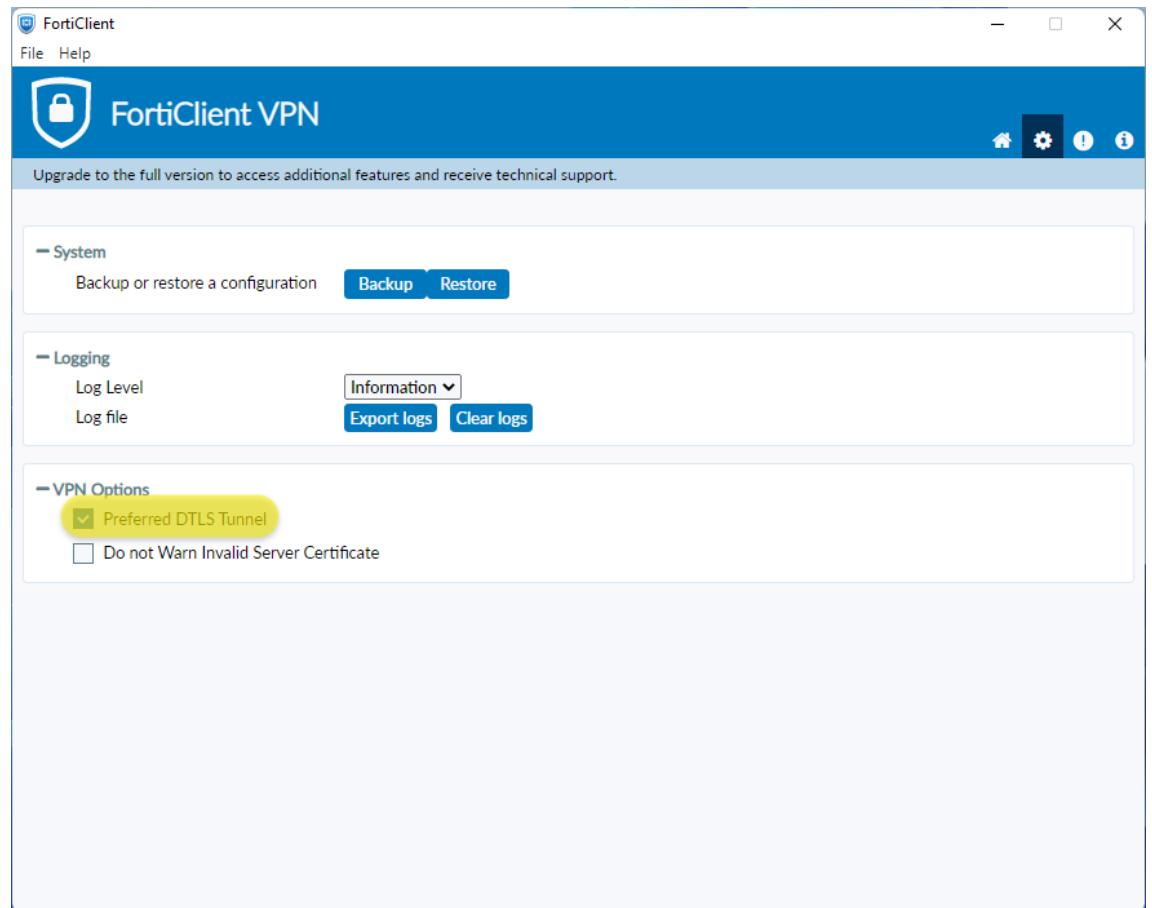
1

 Que faire si je suis sur Windows ?

Vous devez activer le support du **protocole DTLS** dans les paramètres de l'application.



1. Cliquez sur la petite icône en forme de **cadenas** en haut à droite.
(cette opération nécessite une "élévation de privilège".)
2. Cliquez sur l'icône en forme de **rouage**.



3. Activez l'option Preferred DTLS Tunnel (Tunnel DTLS préféré).

2

Que faire si je suis sur MacOS ?

Malheureusement à l'heure de la rédaction de cette procédure l'application FortiClient ne supporte pas le protocole DTLS sur MacOS.

Une solution alternative existe,  l'installation du client Openconnect.

Contacter le support

En cas de difficulté persistante, par ex. pour installer et configurer le client correspondant à votre appareil, rendez-vous sur notre site d'assistance <https://support.unistra.fr> [<https://support.unistra.fr/>]

Pour aller plus loin



Voir la fiche catalogue présentant le service. [https://services-numeriques.unistra.fr/catalogue/service.html?service=s-services_gestiondelinfrastructuredaccesreseaudistantvpn]



Description des principes techniques du service d'accès distant.

1

Principes techniques du service VPN

Brève description de VPN et de son implémentation sur OSIRIS

VPN, ou « virtual Private Network » (ou encore RPV pour « Réseau Privé Virtuel ») est le nom générique donné au service permettant à un ordinateur distant de se connecter, via un réseau public (en général Internet), sur un réseau privé et d'être vu comme une machine interne au réseau privé (dans notre cas Osiris).

Les services VPN utilisent le principe du « Tunneling ». Après authentification de l'utilisateur, l'ordinateur distant crée un tunnel dans lequel toutes les données sont chiffrées, ce qui assure la confidentialité des échanges.

Le service VPN sur Osiris utilise deux Fortigate 1100E redondants.

Lors d'une demande de connexion en provenance d'un client distant, le serveur authentifie le client et s'accorde avec lui sur les méthodes de chiffrement et les clés à utiliser. Une fois le tunnel créé, la source chiffre les données et les envoie dans ce tunnel. À l'arrivée, le serveur VPN déchiffre les données et les transmet sur le réseau local.

Du côté du client, deux éléments sont requis :

- un client VPN compatible avec le serveur VPN : Forticlient ;
- une connexion Internet via un FAI (Fournisseur d'Accès à Internet) de votre choix.



Logiciels

Le client VPN est un logiciel qui met en oeuvre les fonctions d'établissement du tunnel SSL et de chiffrement et déchiffrement des données, au dessus d'une connexion IP existante.

Le client VPN peut être activé manuellement à la demande. Quand une connexion est établie sur le serveur VPN, celui-ci affecte un adresse IP Osiris à votre ordinateur distant. À partir de cet instant **toutes vos communications réseau passent par le serveur VPN Osiris**.

Ceci permet de voir vos communications réseau comme étant émises à partir du réseau Osiris. Vous devez alors, bien sûr, respecter la **charte Osiris**.

Autorisation d'accès au service VPN

Ce service n'est ouvert qu'aux personnels et étudiants des établissements membres d'Osiris [<https://services-numeriques.unistra.fr/documentations/les-services-dinfrastructures/reseau-et-securite/osiris.html>]. Chaque utilisateur devra s'authentifier en utilisant son identifiant et son mot de passe référencés dans l'annuaire de son établissement.



Vous pouvez tester votre connexion VPN sur la page de « Test de connexion VPN [<http://vpnadr.unistra.fr/>] »

7. REMARQUES, SUGGESTIONS

Votre avis nous intéresse !

Afin de contribuer à l'amélioration de la qualité des documentations, vous pouvez transmettre vos remarques et suggestions à sn-documentations@unistra.fr (sans omettre d'indiquer le nom de la documentation et, si possible, l'URL de consultation).

Les données collectées seront uniquement utilisées par la Direction du numérique.