Client VPN Android 6.4

Guide de l'utilisateur

Dernière mise à jour : 26 juillet 2023
Référence du document : 20230726_UG_VPA_6.4_FR_1.0

www.thegreenbow.com

TheGreenBow est un nom commercial déposé.

Microsoft et Windows 10 sont soit des marques déposées, soit des marques commerciales de Microsoft Corp. aux États-Unis et/ou dans d'autres pays.

Apple, le logo Apple, iPhone, iOS, Mac et macOS sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays et régions.

Android, Google Chrome, Google Play et le logo Google Play sont des marques commerciales de Google, LLC.

D'autres marques de commerce appartenant à des tiers et mentionnées dans ce document demeurent la propriété intellectuelle de ces tiers.

Toutes les informations fournies sont sujettes à modification à tout moment et sans préavis.

Malgré tous les soins apportés à la réalisation de ce document et à sa mise à jour régulière, des erreurs peuvent s'être glissées dans les informations présentées. Si vous en constatez n'hésitez pas à nous le faire savoir en nous contactant, nous procéderons aux rectifications correspondantes.

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2023-07-26	Toutes	Version initiale	FB, BB

1 Présentation

1.1 Introduction

Merci d'avoir téléchargé le logiciel Client VPN Android 6.4. Une fois installée sur votre terminal mobile, l'application s'appelle TheGreenBow VPN.

Le Client VPN Android sécurise les échanges de données depuis et vers les smartphones et les tablettes. Particulièrement adapté à la gestion des systèmes industriels (maintenance, diagnostics, logistique...), il répond également aux exigences de protection des communications critiques pour les services de sécurité publics et privés.

Il ne nécessite pas de remise en cause de l'infrastructure de gestion de clés (IGC/PKI) existante, et il est conçu pour s'intégrer de façon transparente avec les passerelles IKEv2 mises en place.

Le Client VPN Android est commercialisé sous forme d'abonnement annuel. Cet abonnement inclut un support dédié et la maintenance du logiciel.

Ce guide est destiné aux utilisateurs du Client VPN Android.

Il comporte toutes les informations permettant de mettre en œuvre et de configurer le logiciel pour permettre l'ouverture de tunnels VPN sécurisés.

1.2 Sécurité

Le Client VPN Android a été développé en suivant les recommandations du NIST et de l'ANSSI. Dans sa version actuelle, il est capable de répondre au profil IPsec DR (Diffusion restreinte) d'un point de vue protocolaire, conformément aux recommandations de l'ANSSI. Il est donc compatible avec les passerelles du marché qui respectent ce référentiel (notamment Stormshield SNS, Thales Mistral, Atos Trustway).

L'ensemble des protocoles et algorithmes mis en œuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN IPsec et OpenVPN du marché, qu'elles soient logicielles ou matérielles.

1.3 Ergonomie

L'installation sur n'importe quel terminal Android 10 ou supérieur s'effectue de manière transparente pour l'utilisateur. Le logiciel prend en charge une variété de protocoles, de paramètres et d'options permettant une interopérabilité avec votre passerelle / pare-feu et votre PKI.

1.4 Simplicité

Le Client VPN Android simplifie l'usage du VPN en proposant une interface utilisateur ergonomique pour établir des connexions sécurisées vers votre système d'information. Les utilisateurs ont une vision directe de l'état des connexions VPN pour vérifier que leurs communications sont bien protégées.

1.5 Fonctionnalités

- Interopérable avec tous les pare-feux/passerelles VPN compatibles IKEv2 et OpenVPN
- Cryptographie : AES CBC/CTR/GCM (128/192/256 bits)
- Hachage : SHA-2 (256/384/512 bits)
- Groupes de clés : DH 14-21, 28
- Gestion des certificats X.509 : PFX, PKCS #12[1]
- Authentification : clé partagée, certificats, EAP, double authentification (certificat + EAP)

1.6 Nouveautés de la version 6

- Utilisation de certificats stockés dans le magasin de certificats du terminal mobile, y compris ceux à courbe elliptique
- Activation permanente du VPN, y compris lorsque l'application n'est pas lancée
- Authentification biométrique
- Activation des licences par TAS (manuelle et dans un tunnel)
- Vérification des CA de la passerelle
- Fin de prise en charge du protocole IKEv1
- Évolution des journaux
- Envoi de notifications relatives aux évènements de l'application
- Améliorations graphiques

1.7 Cryptographie et authentification

1.7.1 Cryptographie

- Prise en charge du groupe de clé Diffie-Hellman DH 28 (BrainpoolP256r1) [RFC 5639]

[1] Configuration à réaliser avec le Client VPN Windows Enterprise.

1.7.2 Obsolescence de IKEv1 et des algorithmes vulnérables

Renforcement de la sécurité du logiciel par la fin de la prise en charge :

- du protocole IPsec/IKEv1 étant donné qu'il est vulnérable et qu'il a été déclaré obsolète par l'IETF depuis septembre 2019 ;
- des algorithmes vulnérables DES, 3DES, SHA-1, DH 1, DH 2, DH 5 en IPsec/IKEv2 (même en mode « auto »).

1.7.3 SSL / OpenVPN

- Mise à jour d'OpenSSL à la version 1.1.1s pour une sécurité renforcée
- Fin de la prise en charge des algorithmes vulnérables en SSL/OpenVPN : MD5, SHA-1, BF-CBC, TLS 1.1, suite de sécurité « LOW » pour TLS V1.2
- La compression n'est plus activée par défaut

1.7.4 Authentification et révocation des certificats

En raison des exigences de sécurité renforcées, de la dépréciation de certains algorithmes et d'une utilisation plus rigoureuse des certificats, la version 6 du Client VPN Android comprend des restrictions sur les certificats.

- Prise en charge des méthodes d'authentification des certificats suivantes :
  - Méthode 1 : RSA Digital Signature avec SHA-2 [RFC 7296]
  - Méthode 9 : ECDSA sur courbe secp256r1 avec SHA-2 (256 bits) [RFC 4754]
  - Méthode 10 : ECDSA sur courbe secp384r1 avec SHA-2 (384 bits) [RFC 4754]
  - Méthode 11 : ECDSA sur courbe secp521r1 avec SHA-2 (512 bits) [RFC 4754]
  - Méthode 14 : Digital Signature Authentication RSASSA-PSS avec SHA-2 (256/384/512 bits) [RFC 7427]
  - Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) (uniquement disponible avec des passerelles prenant en charge cette méthode)
- La méthode d'authentification des certificats 14 basée sur l'algorithme de signature RSASSA-PSS est utilisée par défaut pour tous les certificats RSA
- Le mode d'encapsulation UDP est forcé pour le protocole IKEv2
- Fin de prise en charge de la Méthode 1 : RSA Digital Signature avec SHA-1 [RFC 7296]
- Refus des certificats RSA de taille inférieure à 2048 bits
- Refus des certificats ECDSA de taille inférieure à 256 bits
- Vérification des Key Usage et Extended Key Usage des certificats

1.8 Limitations actuelles

- Le logiciel ne prend actuellement pas en charge les certificats avec des date de validité trop lointaines (uniquement pour téléphones en ARMv7).
- La licence du Client VPN Android ne peut pas être renouvelé lorsque l'application est en mode VPN permanent. Pour mettre à jour la licence, il convient de revenir en mode VPN interactif, renouveler l'abonnement, puis revenir en mode VPN permanent.

2 Installation

2.1 Procédure d'installation

Pour installer le Client VPN Android, procédez comme suit :

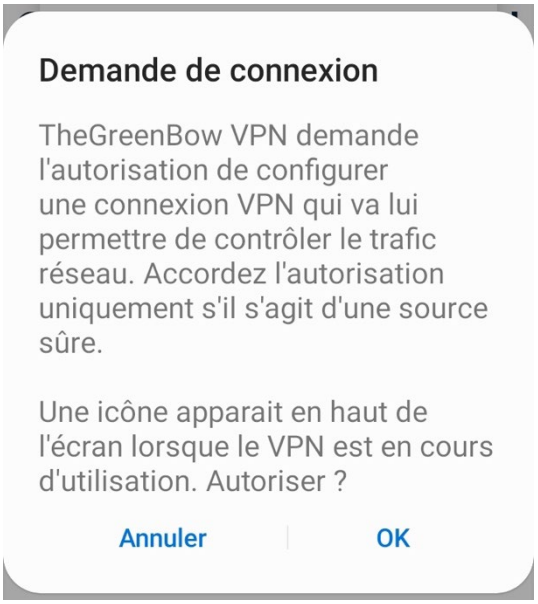
1. Téléchargez le fichier `TheGreenBow_VPN_Android.apk` à partir de la boutique en ligne sur notre site web store.thegreenbow.com.
2. Si vous avez téléchargé le paquet Android depuis un poste de travail, transférez-le sur l'appareil cible.
3. Lancez l'APK depuis l'explorateur de fichiers de l'appareil et suivez les instructions à l'écran.

Si vous n'avez pas encore installé d'APK depuis vos fichiers sur votre terminal mobile, un message s'affiche vous demandant d'autoriser l'installation de fichiers inconnus depuis cette source. Appuyez sur **Paramètres**, puis activez l'option **Autorisation depuis cette source** pour autoriser l'installation d'applications depuis votre explorateur de fichiers.

4. Lorsque vous lancez l'application pour la première fois, un certain nombre de boîtes de dialogue vont s'afficher pour vous demander l'autorisation d'utiliser une fonctionnalité de l'application ou du système d'exploitation du terminal mobile.

L'ordre d'affichage de ces demandes d'autorisation peut varier en fonction de votre interaction avec le terminal.

5. Un premier message s'affiche pour vous demander de déverrouiller l'application. Entrez le même code PIN que vous utilisez pour déverrouiller le terminal mobile ou utilisez la reconnaissance faciale ou votre empreinte digitale, si cette fonctionnalité est disponible et activée sur votre terminal.
6. Appuyez sur **Continuer**.
7. Si c'est la première fois que vous installez une application VPN, une boîte de dialogue s'affiche pour vous demander l'autorisation de configurer une connexion VPN.



8. Appuyez sur **OK**.
9. Lorsque le système vous demande d'accéder aux photos et contenus multimédias sur votre appareil, il est recommandé de l'autoriser afin de pouvoir importer et exporter les fichiers de configuration, les fichiers journaux et les fichiers d'activation manuelle.

L'application TheGreenBow VPN est installée et vous pouvez commencer à l'utiliser.

Pour ajouter une connexion VPN de test, reportez-vous au chapitre 5 Test du Client VPN.

Pour apprendre comment utiliser l'application, reportez-vous au chapitre 6 Prise en main de l'application.

Pour plus d'informations sur l'activation de l'application, reportez-vous au chapitre 3 Activation de l'application.

2.2 Conditions d'installation

Version minimale d'Android : 10

Espace de stockage interne disponible : 40 Mo

2.3 Période d'évaluation

Une fois installée, l'application peut être utilisée gratuitement pendant une période d'évaluation de 30 jours. Pendant cette période d'évaluation, le Client VPN Android est complètement opérationnel : toutes les fonctions sont disponibles.

Pour afficher l'écran d'activation, appuyez sur le menu en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Activation**, puis **Entrer votre numéro de licence**.

Cet écran indique le nombre de jours d'évaluation restants.

Pour plus d'informations sur l'activation de l'application, reportez-vous au chapitre 3 Activation de l'application.

2.4 Procédure de mise à niveau

Pour mettre à niveau le Client VPN Android sur votre appareil mobile, il vous suffit d'installer la nouvelle version de l'application par-dessus la version actuelle, en suivant les étapes décrites à la section 2.1 Procédure d'installation.

⚠ Si vous effectuez une mise à jour à partir d'une version 5.11 ou antérieure, vous devez désinstaller le logiciel existant avant d'installer la nouvelle version.

Tous les fichiers de configuration et d'activation VPN existants seront conservés et automatiquement réutilisés.

Cela vous permet de continuer à utiliser le Client VPN Android comme précédemment, tout en bénéficiant des nouvelles fonctionnalités et correctifs.

⚠ En raison d'un changement de signature, qui empêche la conversion des anciens fichiers de configuration au nouveau format des fichiers `.tgb`, les fichiers de configuration des versions 5.11 et antérieures ne sont pas compatibles avec la version 6.0 ou supérieure.
Vous devez réexporter la configuration depuis un Client VPN Windows de version 6.87 ou supérieure.

3 Activation de l'application

3.1 Introduction

L'activation du Client VPN Android peut être effectuée de plusieurs manières différentes :

- en ligne, directement à partir de l'application (voir section 3.2 Activation en ligne) ;
- hors ligne, à partir d'un autre poste connecté à internet (voir section 3.3 Activation manuelle hors ligne) ;
- à l'aide du serveur d'activation TAS :
  - dans un tunnel connecté à un serveur TAS (voir section 3.4.2 Activation dans un tunnel connecté à un serveur TAS) ;
  - sur le réseau local où se trouve le serveur TAS (voir section 3.4.3 Activation sur le réseau local où se trouve le serveur TAS).

Les procédures correspondantes sont décrites dans les sous-sections ci-dessous.

Pour plus d'informations sur le serveur d'activation TAS, consultez la page suivante sur notre site : https://www.thegreenbow.com/fr/produits-vpn-thegreenbow/secure-connection-management/.

3.2 Activation en ligne

Si vous souhaitez acquérir une licence pour le Client VPN Android et l'activer directement depuis le terminal mobile, procédez comme suit :

1. À partir du menu **Activation**, sélectionnez **Entrer votre numéro de licence**.
2. Dans l'écran qui s'affiche, appuyez sur le bouton **Acheter**.

   La boutique en ligne TheGreenBow s'ouvre dans une fenêtre de navigateur.

3. Sélectionnez le **Client VPN Android**, puis la **Méthode de livraison**, la durée **d'Engagement** et le **Nombre de licences**.
4. Ajoutez le produit au panier, puis terminez votre achat.

   Vous recevrez la licence dans un e-mail d'activation.

5. Retournez à l'application TheGreenBow VPN et saisissez le numéro de licence dans le champ prévu à cet effet, puis appuyez sur **Activer**.

Vous pouvez également accéder à la boutique en ligne à partir d'un poste de travail et saisir ensuite le numéro de licence reçu dans l'e-mail d'activation.

Pour connaître la signification des codes d'erreur d'activation, reportez-vous à la section 3.6 Erreurs d'activation.

Pour savoir comment renouveler une licence activée en ligne, reportez-vous à la section 3.5 Renouvellement de la licence.

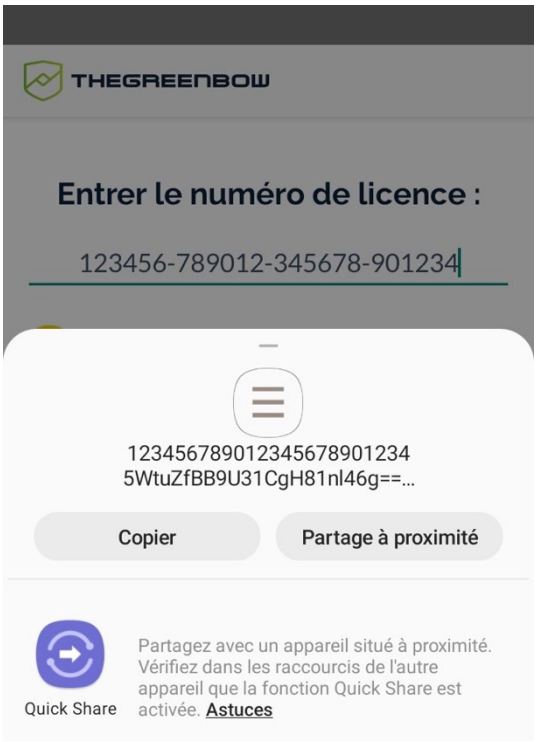
3.3 Activation manuelle hors ligne

Dans certains cas, l'accès à internet peut être restreint sur le terminal mobile pour des raisons de sécurité. Vous pouvez alors procéder à une activation hors ligne à partir d'un autre poste connecté à internet.

Pour procéder à une activation manuelle à partir d'un autre poste connecté à internet, suivez les étapes ci-dessous :

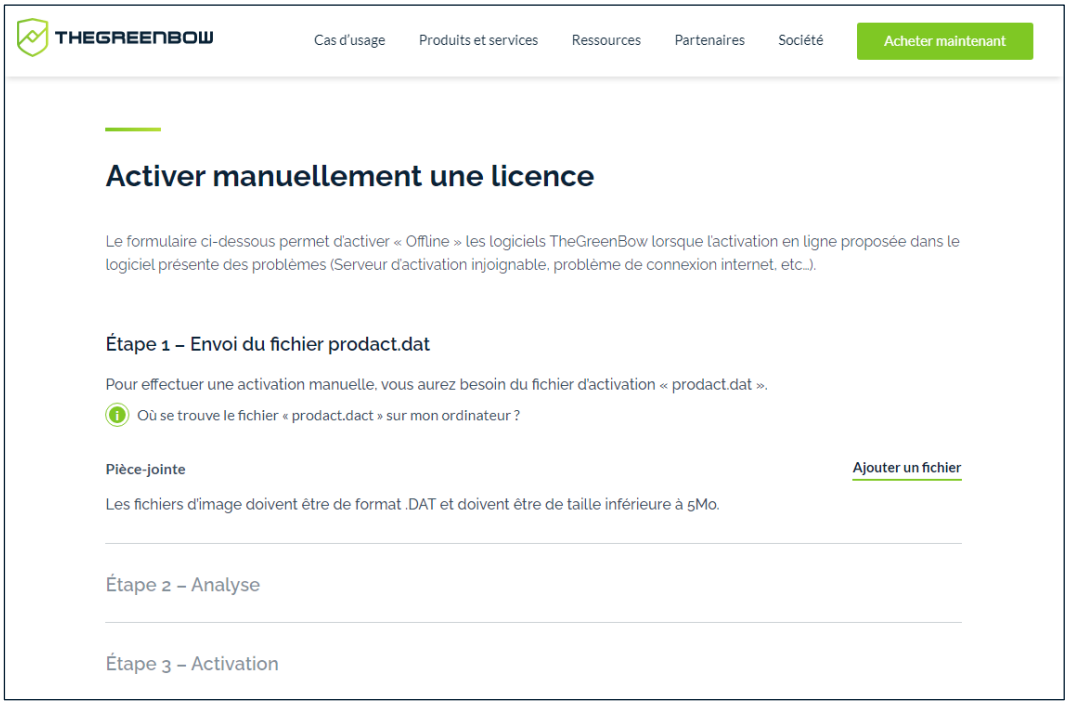
1. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Activation**, puis **Entrer votre numéro de licence**.
2. Renseignez le numéro de licence que vous avez reçu dans l'e-mail d'activation dans le champ prévu à cet effet.
3. Cochez la case **Activation manuelle**.
4. Appuyez sur le bouton **Activer**.

Un volet de partage de fichier s'affiche :

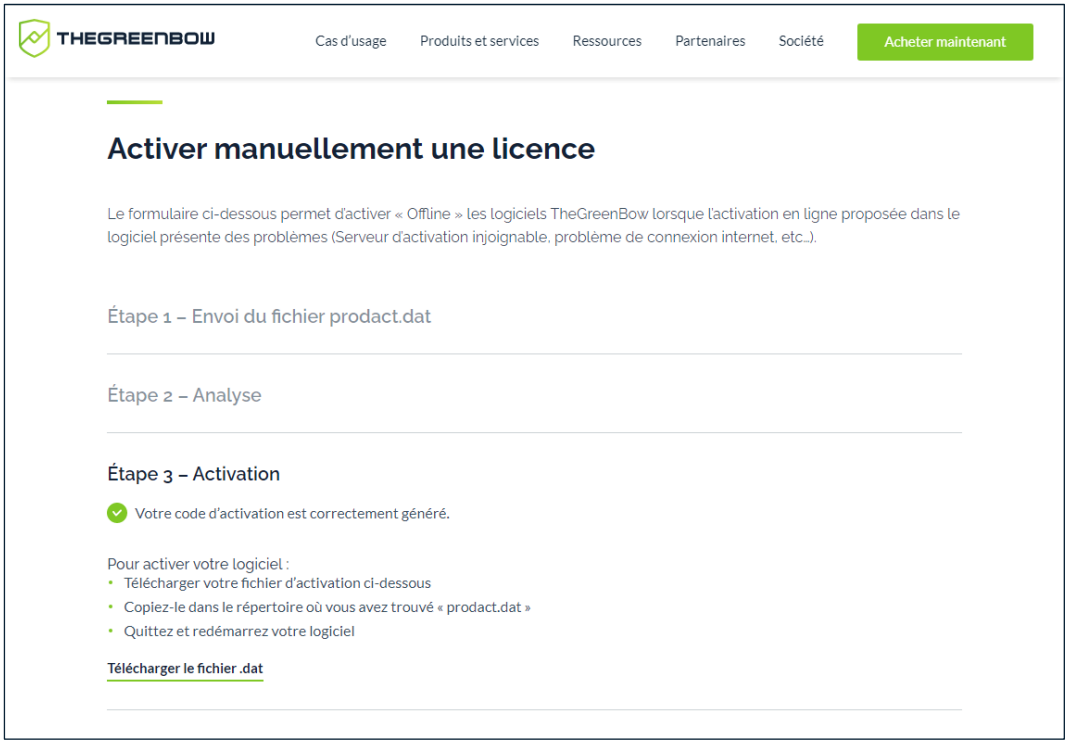


Les informations techniques correspondant au contenu du fichier d'activation `prodact.dat` sont copiées dans le presse-papier. Vous pouvez les envoyer par e-mail ou les enregistrer dans un fichier texte nommé `prodact.dat` directement sur le terminal mobile.

1. Récupérez le fichier `prodact.dat` sur un poste connecté à internet ou créez-le à partir des éléments récupérés du presse-papier. Le fichier `prodact.dat` doit être un fichier texte au format UTF-8.
2. Connectez-vous au serveur d'activation TheGreenBow accessible à l'adresse https://thegreenbow.com/fr/support/gestion-des-licences/activation-manuelle-dune-licence/.



3. Cliquez sur le bouton **Ajouter un fichier** et sélectionnez le fichier `prodact.dat` créé pour le terminal à activer.
4. Cliquez sur **Envoyer**. Le serveur d'activation vérifie la validité des informations du fichier `prodact.dat`.
5. Cliquez sur **Effectuer**. Le serveur d'activation présente en téléchargement le fichier contenant le code d'activation destiné au terminal mobile à activer.

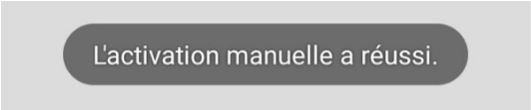


Ce fichier a un nom de la forme : `tgbcode_[date]_[code].dat` (par exemple : `tgbcode__20230415_1029.dat`).

6. Transférez le fichier `tgbcode_[date]_[code].dat` sur le terminal mobile que vous souhaitez activer.
7. Dans l'application TheGreenBow VPN sur le terminal mobile, ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Activation**, puis **Importer le fichier d'activation**.

   Le gestionnaire de fichiers s'ouvre, vous permettant de sélectionner le fichier à importer.

8. Un message d'information s'affiche pour confirmer que le fichier a été importé correctement et que l'activation manuelle a réussi :



Lorsque l'activation a réussi, le numéro de licence et la durée de validité de la licence sont affichés sur l'écran d'activation.

⚠ Le message affiché à l'écran lors de l'importation n'indique pas si l'importation a réussi. Lorsque vous importez un fichier quelconque ou que vous annulez l'importation, le même message confirmant que l'activation manuelle a été effectuée est toujours affiché.

☞ Pour connaître la signification des codes d'erreur d'activation, reportez-vous à la section 3.6 Erreurs d'activation.

☞ Pour savoir comment renouveler une licence activée manuellement, reportez-vous à la section 3.5 Renouvellement de la licence.

3.4 Activation à l'aide du TAS

Si vous disposez d'un serveur TAS pour la gestion des licences, vous pouvez importer un fichier d'activation contenant le numéro de licence et l'adresse du TAS avec lequel le Client VPN Android doit communiquer pour réaliser l'activation.

Vous pourrez alors soit activer la licence dans le réseau local si votre TAS se trouve sur ce réseau ou ouvrir un tunnel et vous connecter au TAS dans le tunnel pour activer la licence.

☞ Pour procéder à une activation à l'aide du serveur TAS, vous devez d'abord créer un fichier d'activation `vpnsetup.json`, reportez-vous à la section

3.4.1 Format et contenu du fichier vpnsetup.json pour savoir comment le faire.

Pour procéder à une activation dans un tunnel connecté à un serveur TAS, reportez-vous à la section 3.4.2 Activation dans un tunnel connecté à un serveur TAS.

Pour procéder à une activation sur le réseau local où se trouve le serveur TAS, reportez-vous à la section 3.4.3 Activation sur le réseau local où se trouve le serveur TAS.

Pour plus d'informations sur l'utilisation du serveur d'activation TAS, consultez la documentation afférente sur notre site : https://www.thegreenbow.com/fr/support/documentations-produits/.

3.4.1 Format et contenu du fichier vpnsetup.json

Lorsque l'activation se fait avec un serveur d'activation TAS que ce soit dans le tunnel ou sur le réseau local, les informations d'activation du Client VPN Android doivent être saisies dans un fichier `vpnsetup.json` au format ASCII.

Le nom du fichier est indifférent, mais l'extension `.json` est requise.

Pour cela, renseignez l'adresse e-mail de l'utilisateur et le numéro de licence qui vous a été fourni ainsi que les paramètres OSA du serveur TAS comme suit :

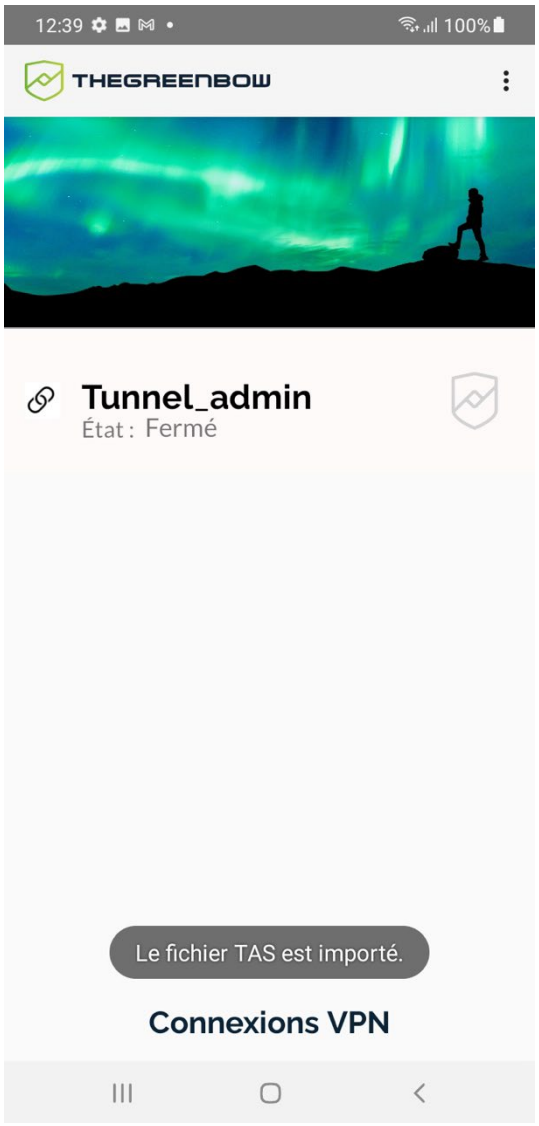
```
{
     "license" : "12345678901234567890123456",
     "email" : "nom.utilisateur@entreprise.com"
     "osaurl" : "192.168.217.102/osace_activation.php"
     "osaport" : "80"
     "osacert" : "MIICGjCCAYOgAwIBAgIBADANBg [........]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
}
```

Dans le paramètre `osaurl`, si l'URL contient `https`, le protocole sécurisé https sera utilisé. Sinon, le protocole utilisé sera http.

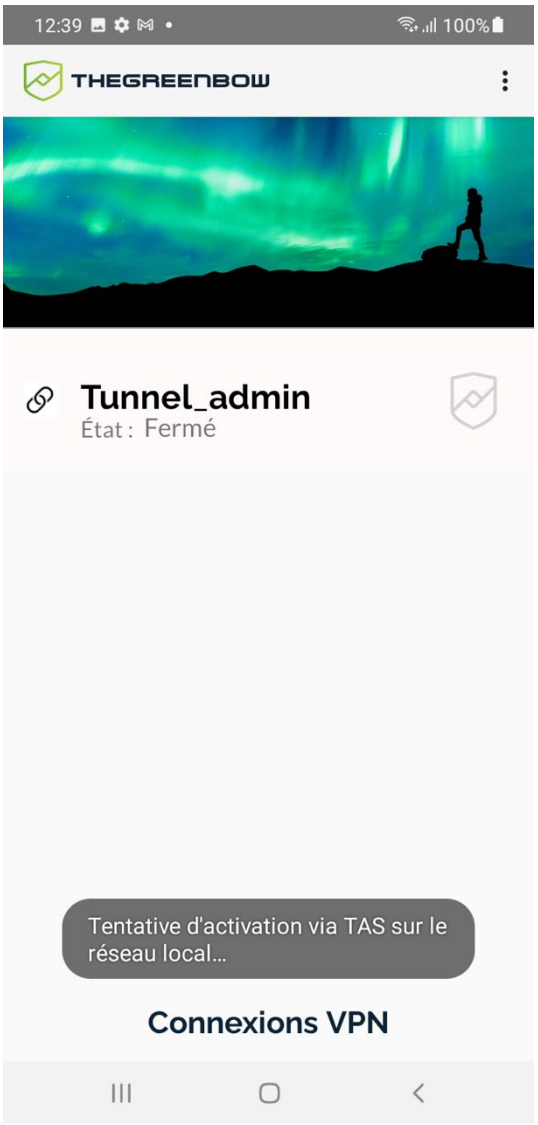
3.4.2 Activation dans un tunnel connecté à un serveur TAS

Pour procéder à une activation dans un tunnel connecté à un serveur TAS, suivez les étapes ci-dessous :

1. Créez le fichier d'activation vpnsetup.json (voir section 3.4.1 Format et contenu du fichier vpnsetup.json ci-dessus).
2. Récupérez le fichier d'activation TAS vpnsetup.json sur le terminal mobile.
3. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez Activation, puis Importer le fichier TAS. Le gestionnaire de fichiers s'ouvre, vous permettant de sélectionner le fichier à importer.
4. Sélectionnez le fichier à importer. Le fichier TAS est importé. Un message s'affiche pour confirmer le bon déroulement de l'opération.



5. Un message s'affiche pour indiquer que le Client VPN Android a tenté de se connecter au serveur TAS sur le réseau local, mais ne l'a pas trouvé.



6. Importez une configuration comportant une connexion vers le réseau sur lequel se trouve le serveur TAS (voir chapitre 8 Configuration des connexions VPN pour savoir comment la créer).
7. Ouvrez le tunnel de la connexion que vous venez de créer. Si le tunnel reste ouvert et qu'aucun message d'erreur ne s'affiche, l'activation a réussi. Vous pouvez consulter la fenêtre **À propos** pour le confirmer (voir section 6.3.4 Sous-menu À propos... pour savoir comment l'afficher).

Le Client VPN Android est activé.

Pour éviter toute modification inopinée du numéro de licence, lorsque la licence a été importée à partir d'un fichier TAS, l'option de menu **Activation** > **Entrer votre numéro de licence** est grisée.

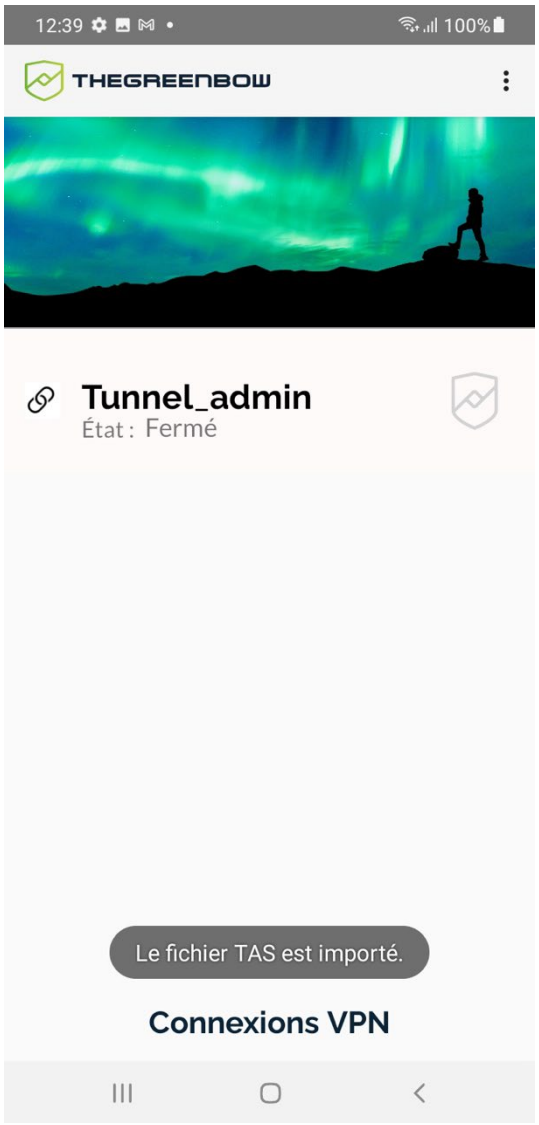
Pour connaître la signification des codes d'erreur d'activation, reportez-vous à la section 3.6 Erreurs d'activation.

Pour savoir comment renouveler une licence gérée par un serveur TAS, reportez-vous à la section 3.5 Renouvellement de la licence.

3.4.3 Activation sur le réseau local où se trouve le serveur TAS

Pour procéder à une activation sur le réseau local où se trouve le serveur d'activation TAS, procédez comme suit :

1. Créez le fichier d'activation `vpnsetup.json` (voir section 3.4.1 Format et contenu du fichier vpnsetup.json ci-dessus).
2. Transférez le fichier `vpnsetup.json` généré sur le terminal mobile que vous souhaitez activer.
3. Assurez-vous que le terminal mobile est connecté au réseau local sur lequel se trouve le serveur TAS.
4. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Activation**, puis **Importer le fichier TAS**. Le gestionnaire de fichiers s'ouvre, vous permettant de sélectionner le fichier à importer.
5. Sélectionnez le fichier à importer. Le fichier TAS est importé. Un message s'affiche pour confirmer le bon déroulement de l'opération.



6. Le Client VPN Android se connecte au TAS sur le réseau local. Si aucun message d'erreur ne s'affiche, l'activation a réussi. Vous pouvez consulter la fenêtre **À propos** pour le confirmer (voir section 6.3.4 Sous-menu À propos... pour savoir comment l'afficher).

Le Client VPN Android est activé.

Pour éviter toute modification inopinée du numéro de licence, lorsque la licence a été importée à partir d'un fichier TAS, l'option de menu **Activation** > **Entrer votre numéro de licence** est grisée.

Si le Client VPN Android ne trouve pas le serveur TAS sur le réseau local, un message s'affiche pour l'indiquer. Dans ce cas, vous devez indiquer l'adresse du serveur TAS dans le fichier d'activation `vpnsetup.json` et procéder à une activation dans le tunnel (voir section 3.4.2 Activation dans un tunnel connecté à un serveur TAS).

Pour connaître la signification des codes d'erreur d'activation, reportez-vous à la section 3.6 Erreurs d'activation.

Pour savoir comment renouveler une licence gérée par un serveur TAS, reportez-vous à la section 3.5 Renouvellement de la licence.

3.5 Renouvellement de la licence

Lorsque la validité de la licence arrive à échéance, un message s'affiche dans le Client VPN Android sept jours avant la date d'expiration pour vous rappeler qu'il est temps de la renouveler.

Le comportement du Client VPN Android diffère quelque peu selon que vous l'utilisez en mode interactif ou en mode permanent.

3.5.1 Mode interactif

Lorsque vous utilisez le Client VPN Android en mode interactif, c'est-à-dire que vous ouvrez et fermez manuellement le ou les tunnels configurés dans la liste des connexions, le comportement de l'application à partir de sept jours avant l'expiration de la licence est le suivant.

Lorsque vous ouvrez un tunnel, une requête d'activation est lancée dans le tunnel, puis :

- s'il reste moins de 6 jours avant l'expiration de la licence et que vous ne l'avez pas renouvelée, l'activation échoue, mais le tunnel reste ouvert ;
- s'il reste moins de 6 jours avant l'expiration de la licence et que vous l'avez renouvelée, l'activation est mise à jour dans le Client VPN avec la nouvelle date ;
- si la licence est expirée, le tunnel est fermé et un message s'affiche pour indiquer que la licence est expirée.

3.5.2 Mode permanent

Lorsque vous utilisez le Client VPN Android en mode permanent, c'est-à-dire que le tunnel configuré est ouvert en permanence (voir section 9.4 Activer la fonction VPN permanent), le comportement de l'application à partir de 7 jours avant l'expiration de la licence est le suivant.

Une requête d'activation est lancée dans le tunnel, puis :

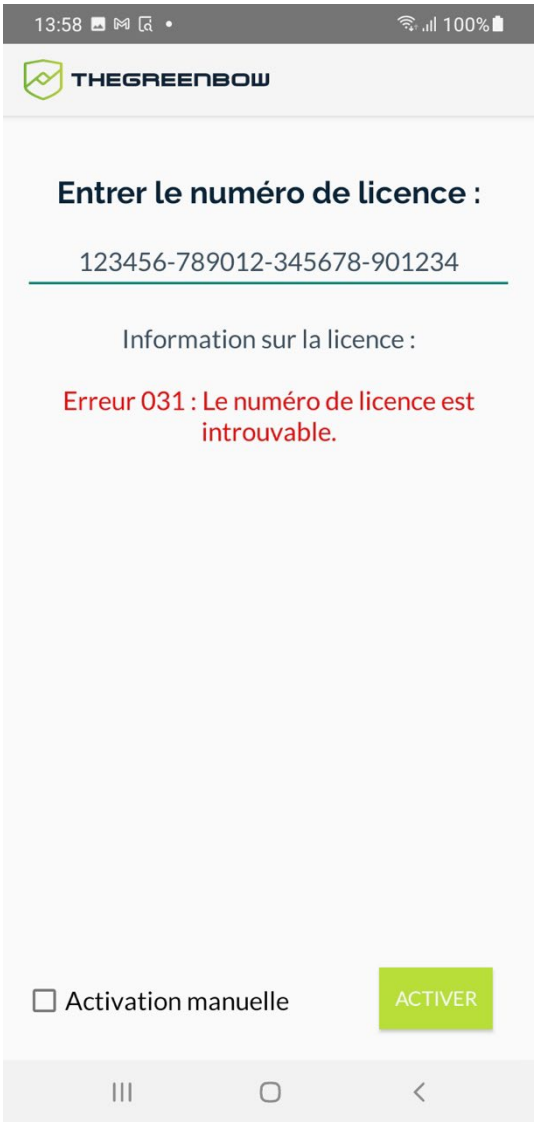
- s'il reste moins de 6 jours avant l'expiration de la licence et que vous ne l'avez pas renouvelée, le tunnel reste ouvert et un message indiquant le nombre de jours restant avant l'expiration de la licence s'affiche ;

- si la licence est expirée, le tunnel est fermé, un message s'affiche pour indiquer que la licence est expirée et l'icône en forme de clé dans la barre d'état repasse du côté gauche.

⚠ Vous devez désactiver le mode permanent et revenir en mode interactif pour renouveler la licence (voir section 9.4 Activer la fonction VPN permanent).

3.6 Erreurs d'activation

L'activation du logiciel peut ne pas aboutir pour différentes raisons. Lorsqu'une erreur se produit, un code d'erreur est indiqué sur l'écran d'activation suivi d'un bref message d'erreur :



TheGreenBow indique sur son site web toutes les erreurs d'activation ainsi que les procédures de résolution des problèmes d'activation.

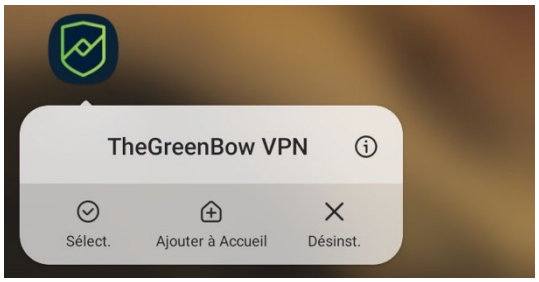
Les erreurs d'activation les plus courantes sont les suivantes :

N°	Signification	Résolution
31	Le numéro de licence n'est pas correct	Vérifier le numéro de licence.
33	Le numéro de licence est déjà activé sur un autre terminal	Désinstaller l'application du terminal mobile sur lequel a été activée la licence, ou contacter l'équipe commerciale TheGreenBow.
53, 54	La communication avec le serveur d'activation est impossible	Vérifier que le terminal mobile est bien connecté à internet. Vérifier que la communication n'est pas filtrée par un firewall ou pour un proxy.

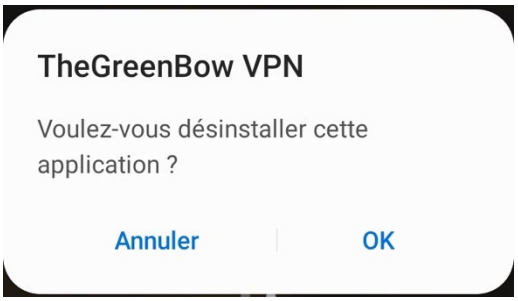
4 Désinstallation

La procédure de désinstallation de l'application est décrite ci-dessous :

1. Maintenez le doigt appuyé sur l'icône de l'application **TheGreenBow VPN**.



2. Sélectionnez l'option **Désinst.** dans le menu contextuel.



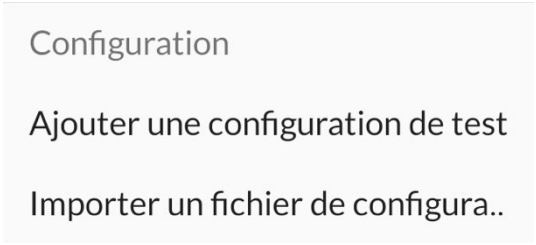
3. Appuyez sur **OK** pour confirmer.

5 Test du Client VPN

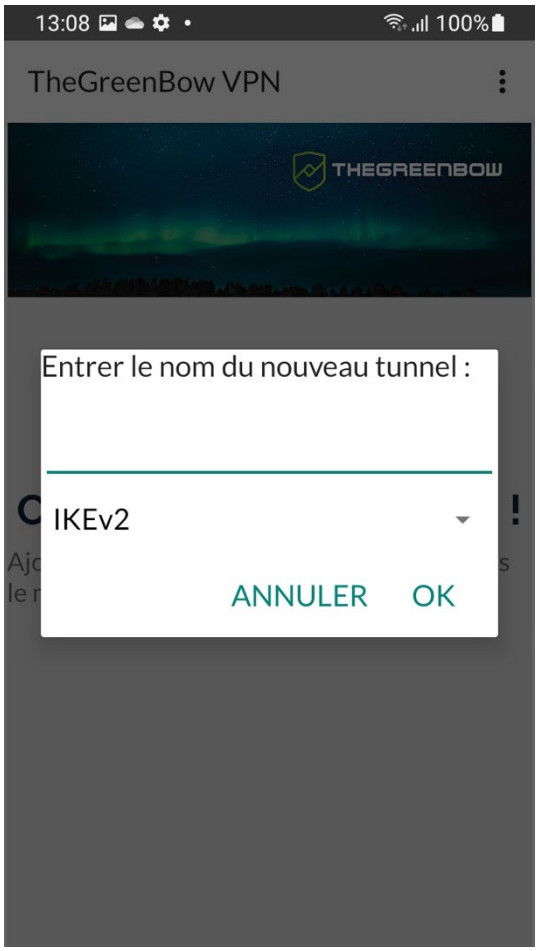
Cette section vous montre comment créer et ouvrir une connexion VPN de test qui se connectera au réseau VPN de test TheGreenBow.

Pour créer une connexion VPN de test procédez comme suit :

1. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Configuration**, puis **Ajouter une configuration de test**.



Une boîte de dialogue s'affiche :



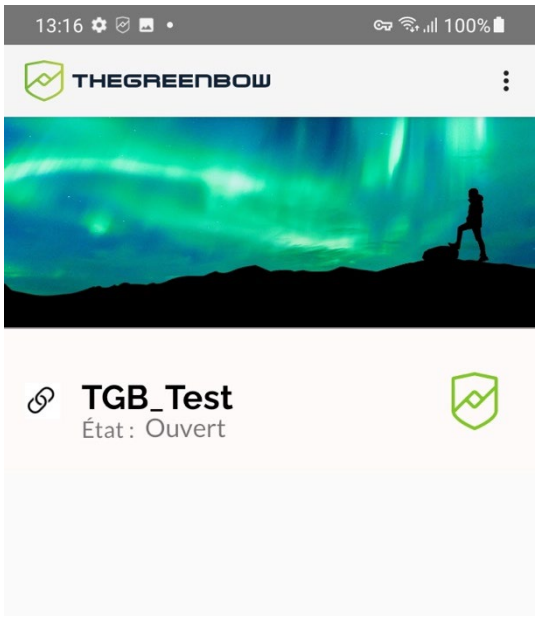
2. Saisissez un nom pour le nouveau tunnel, p. ex. TGB_Test. Le seul protocole disponible est IKEv2.

Les noms des connexions ne doivent pas contenir d'espaces. Vous pouvez insérer des caractères de soulignement pour séparer les mots.

3. Appuyez sur **OK**. La nouvelle connexion VPN de test est ajoutée à l'écran principal. Les paramètres de connexion au réseau VPN de test TheGreenBow sont renseignés automatiquement.
4. Appuyez sur le nom de la connexion de test que vous venez de créer. Le Client VPN Android lance la connexion.

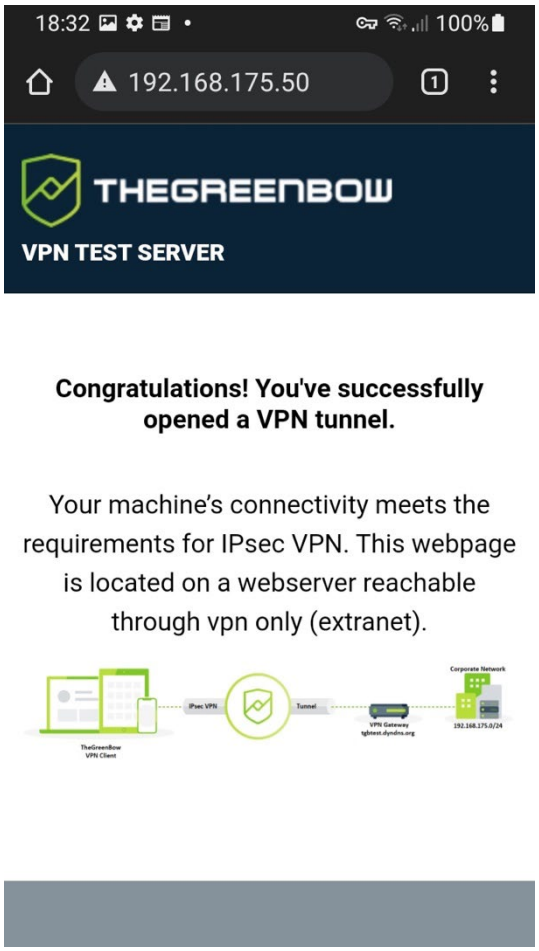
Lors de la première ouverture d'un tunnel, un message s'affiche vous demandant l'autorisation de configurer une connexion VPN. Appuyez sur **OK** pour accorder l'autorisation.

Lorsque la connexion a réussi, le logo TheGreenBow à côté du nom de la connexion devient vert et l'état de la connexion indique que le tunnel est **Ouvert**.



Une fois le tunnel ouvert, vous devriez pouvoir visiter la page web http://192.168.175.50/ dans votre navigateur.

Lorsque l'ouverture du tunnel de test a réussi, vous devriez voir la page suivante dans votre navigateur web :



Si l'ouverture du tunnel de test ne fonctionne pas, ouvrez un navigateur sur le terminal mobile pour vérifier la connexion à internet.

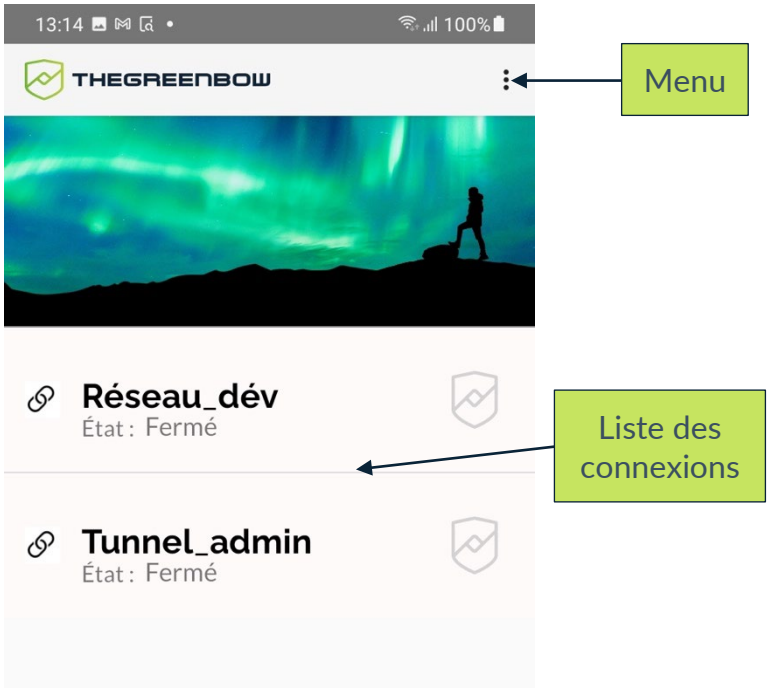
6 Prise en main de l'application

6.1 Introduction

L'interface du Client VPN Android est simple et intuitive. Elle est constituée d'un écran principal avec la liste des connexions VPN et d'un menu.

6.2 Écran principal

6.2.1 Présentation



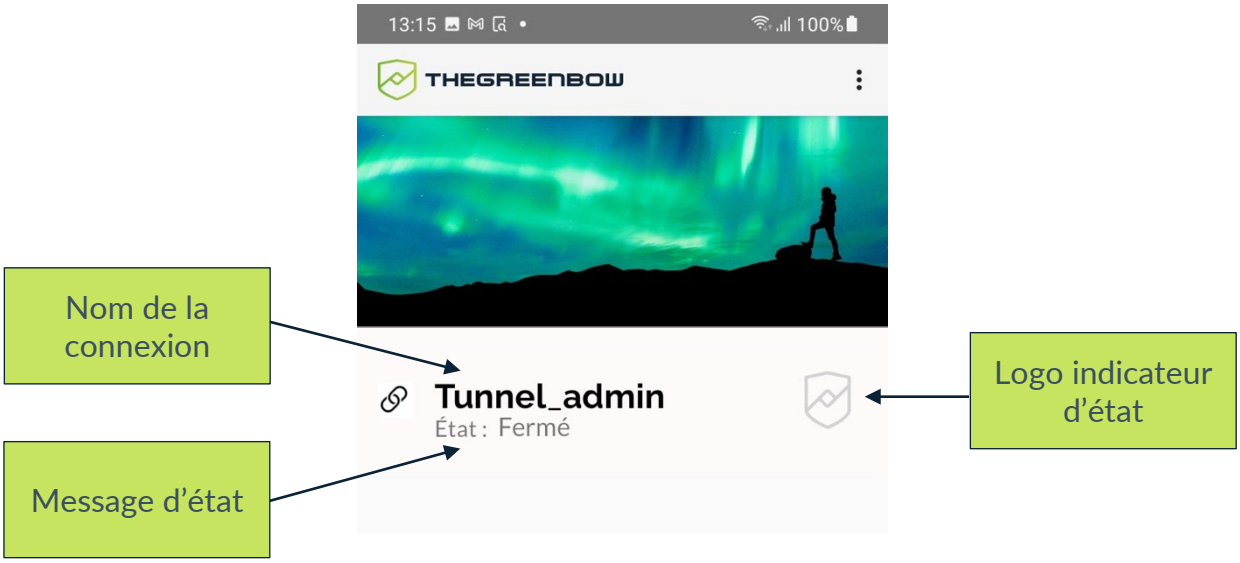
Lors du premier lancement de l'application, la liste des connexions est vide.

Pour ajouter une connexion VPN de test, reportez-vous au chapitre 5 Test du Client VPN.

Pour importer un fichier de configuration, reportez-vous à la section 8.2 Importer un fichier de configuration VPN.

6.2.2 Gestion des connexions

Dès que vous ajoutez une connexion VPN, celle-ci s'affiche dans la liste des connexions.



Chaque connexion comporte les éléments suivants dans son bandeau :

- un nom,
- un message d'état et
- un logo TheGreenBow indiquant l'état de la connexion.

Un appui sur le nom de la connexion lance l'établissement de la connexion.

Un appui long sur le nom de la connexion ouvre la fenêtre de configuration de la connexion.

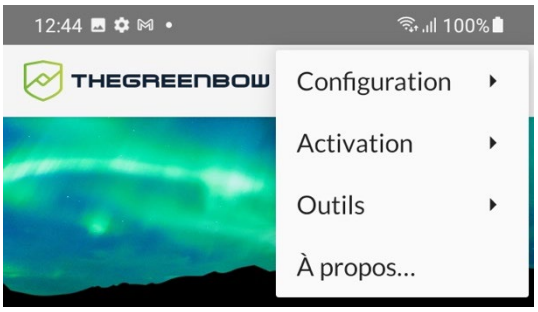
Pour en savoir davantage sur la configuration d'une connexion VPN, reportez-vous au chapitre 8 Configuration des connexions VPN.

Pour découvrir comment ouvrir une connexion VPN, reportez-vous au chapitre 9 Ouverture d'une connexion VPN.

6.3 Menu principal à trois points verticaux

Le menu à trois points verticaux situé en haut à droite de l'écran comporte les entrées suivantes :

- Configuration
- Activation
- Outils
- À propos...

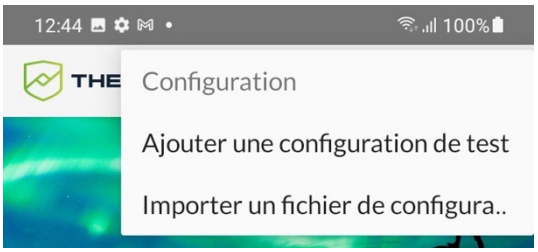


Pour plus d'informations sur chacun de ces sous-menus, reportez-vous aux sections suivantes.

6.3.1 Sous-menu Configuration

Le sous-menu **Configuration** comporte les entrées suivantes :

- Ajouter une configuration de test
- Importer un fichier de configuration



Pour ajouter une connexion VPN de test, reportez-vous au chapitre 5 Test du Client VPN.

Pour importer un fichier de configuration, reportez-vous à la section 8.2 Importer un fichier de configuration VPN.

6.3.2 Sous-menu Activation

Le sous-menu **Activation** comporte les entrées suivantes :

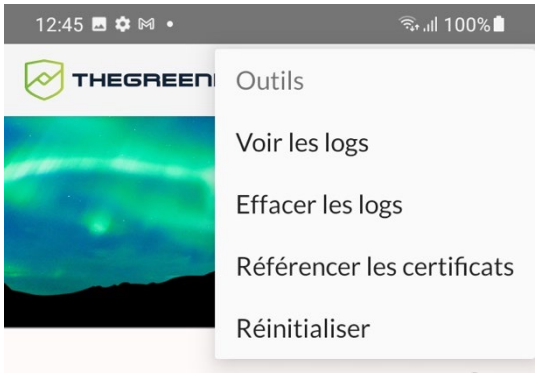
- Entrer votre numéro de licence
- Importer le fichier TAS
- Importer le fichier d'activation

Pour plus d'informations sur l'activation de l'application, reportez-vous au chapitre 3 Activation de l'application.

6.3.3 Sous-menu Outils

Le sous-menu **Outils** comporte les entrées suivantes :

- Voir les logs
- Effacer les logs
- Référencer les certificats
- Réinitialiser



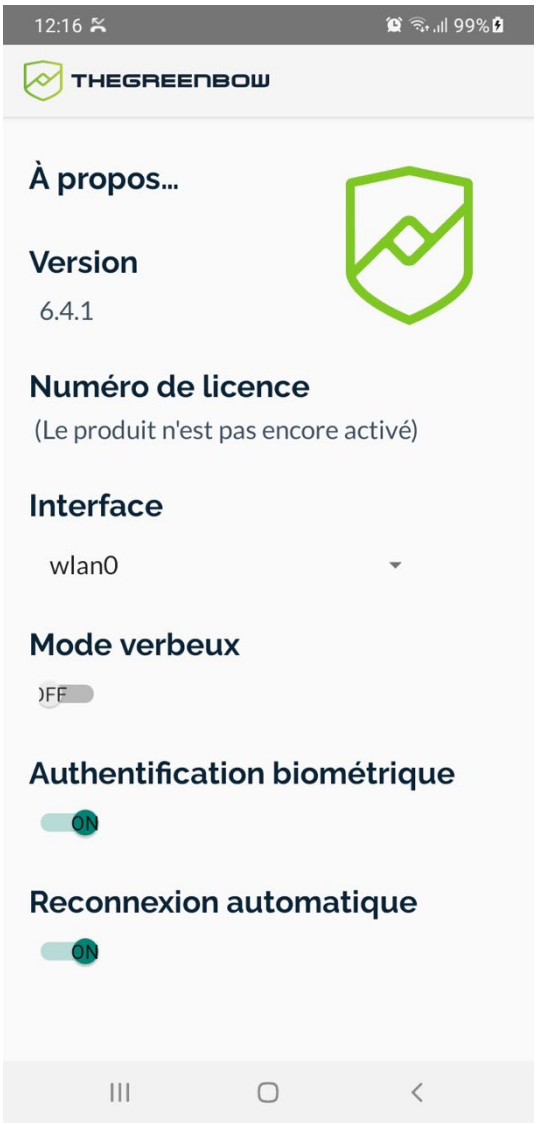
Pour plus d'informations sur les logs (ou journaux), reportez-vous au chapitre 10 Journalisation.

Pour plus d'informations sur le référencement des certificats, reportez-vous au chapitre 7 Utilisation des certificats en magasin.

Pour plus d'informations sur la réinitialisation et la résolution des problèmes, reportez-vous au chapitre 11 Dépannage.

6.3.4 Sous-menu À propos...

Le sous-menu **À propos...** affiche directement la fenêtre **À propos...**



Celle-ci comporte des informations sur la version de l'application et le numéro de licence lorsque celui-ci a été renseigné.

Elle comporte en outre une liste déroulante **Interface**, permettant de sélectionner l'interface réseau à utiliser, et les trois boutons bascule suivants :

- **Mode verbeux**, permettant d'activer ou de désactiver ce mode pour les logs ;

Depuis la version 6.2 du Client VPN Android, le mode verbeux est quelque peu moins volumineux que dans les précédentes versions.

- **Authentification biométrique**, permettant d'activer ou désactiver l'authentification biométrique au lancement du Client VPN et au bout d'un certain temps d'inactivité ;
- **Reconnexion automatique**, permettant de reconnecter automatiquement la connexion après une coupure ou une interruption

à la suite d'un changement d'interface réseau (p. ex. passage du Wi-Fi à la 5G).

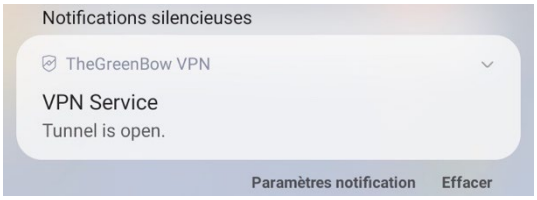
La reconnexion automatique s'arrête au bout de trois tentatives infructueuses.

Pour plus d'informations sur le mode verbeux et les logs (ou journaux), reportez-vous au chapitre 10 Journalisation.

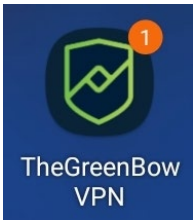
6.4 Notifications

Depuis la version 6.3 du Client VPN Android, l'application envoie des notifications silencieuses sur les états et les erreurs du VPN vers le tiroir de notifications. Celles-ci peuvent porter sur les éléments suivants :

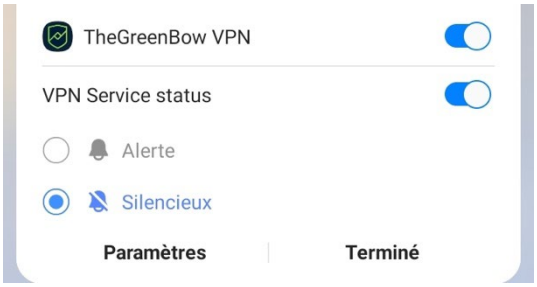
- l'état du tunnel, s'il est ouvert ou fermé ;
- l'expiration de la licence ;
- des problèmes réseau ;
- les erreurs affichées sur l'écran VPN permanent dans la précédente version.



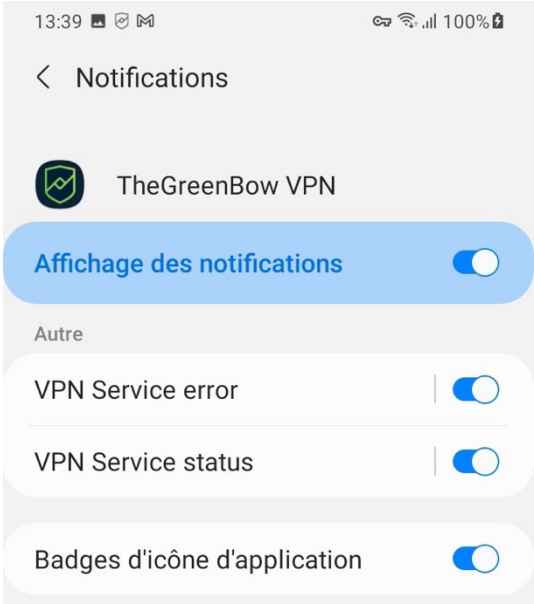
De plus une pastille de notification s'affiche sur l'icône de l'application lorsque de nouvelles notifications ont été reçues.



Vous pouvez modifier les réglages relatifs aux notifications dans les paramètres de l'application. Pour cela, effectuez un appui long sur une notification et effectuez les modifications souhaitées.

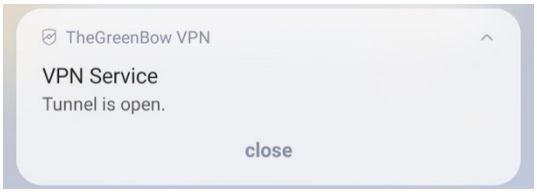


Appuyez sur **Paramètres** pour accéder aux paramètres de notification de l'application dans les paramètres système.



En fonction du type de notification, différentes actions sont possibles à partir de la notification. Par exemple, lorsqu'un tunnel est ouvert et que l'application est fermée, il suffit d'appuyer sur la notification pour ouvrir l'application.

Pour développer une notification, appuyez sur la flèche vers le bas ⌄. Vous pourrez alors effectuer une action directement depuis la notification.



Pour un tunnel ouvert en mode interactif, vous pouvez appuyer sur **close** pour fermer le tunnel, par exemple.

Les notifications apportent de nombreuses autres facilités que nous ne pouvons pas toutes décrire ici. Elles sont généralement suffisamment intuitives pour être explicites par elles-mêmes.

6.5 Icônes d'état

Depuis la version 6.3 du Client VPN Android, l'état du VPN est indiqué par une icône TheGreenBow en plus de l'icône VPN en forme de clé fournie par le système d'exploitation.

L'icône TheGreenBow s'affiche dans la partie gauche de la barre d'état. Elle peut prendre les formes suivantes :

Icône	Signification
	L'ouverture d'un tunnel est en cours.
	Le tunnel est monté.
	Le VPN a rencontré un problème.

L'icône en forme de clé s'affiche dans la barre d'état du terminal mobile. Elle indique l'état du tunnel et du trafic comme suit :

Icône	Signification
	Icône creuse à droite : un tunnel est monté et le trafic chiffré est acheminé.
	Icône pleine à gauche : le tunnel est en défaut et aucun trafic chiffré n'est acheminé.

7 Utilisation des certificats en magasin

7.1 Introduction

Depuis la version 6.2 du Client VPN Android, les certificats peuvent être gérés de plusieurs manières. Ils peuvent être stockés :

- soit dans la configuration de la connexion
- ou dans le magasin de certificats du terminal mobile.

Vous pouvez également importer un certificat dans une configuration existante à partir d'un fichier de certificat présent sur le terminal mobile (voir section 8.4 Importer un certificat dans la configuration d'une connexion).

Si le certificat est inclus dans la configuration de la connexion, il n'est pas possible d'utiliser la configuration avec un des certificats stockés dans le magasin de certificats du terminal mobile.

L'utilisation de certificats stockés dans le magasin de certificats du terminal mobile est plus sécurisée que de charger un certificat à partir d'un fichier.

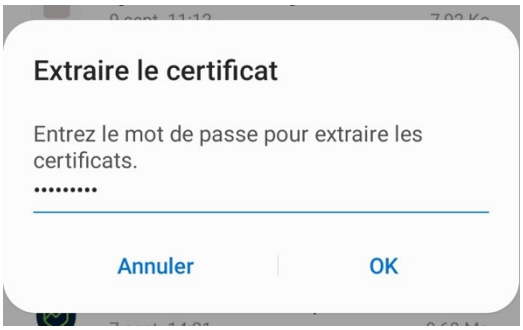
Il est recommandé de supprimer le fichier de certificat après l'avoir importé.

Pour utiliser un certificat stocké dans le magasin de certificats du terminal mobile, vous devez d'abord importer le certificat dans le magasin de certificats du terminal mobile avant de le référencer dans la liste de certificats du Client VPN Android. Vous pourrez ensuite importer une configuration qui utilise ce certificat. Il sera alors automatiquement associé à cette configuration. Ces étapes sont détaillées dans les sections ci-dessous.

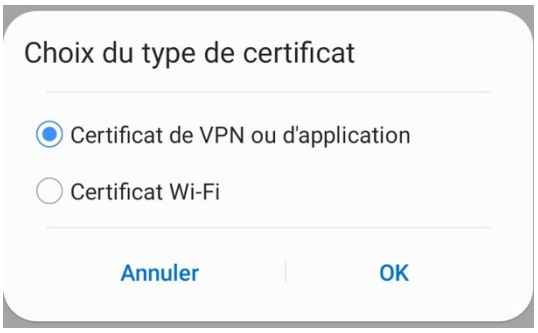
7.2 Importer un certificat dans le magasin de certificats du terminal mobile

Pour importer un certificat dans le magasin de certificats du terminal mobile, procédez de la manière suivante :

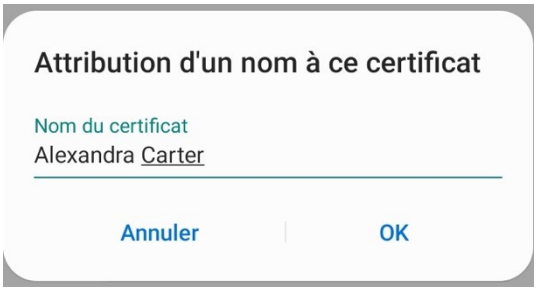
1. Transférez le certificat au format P12 ou PFX sur le terminal mobile.
2. Dans le gestionnaire de fichiers du terminal mobile, naviguez vers l'endroit où vous avez transféré le certificat.
3. Appuyez sur le fichier de certificat. Une boîte de dialogue s'affiche vous demandant de saisir un mot de passe pour extraire le certificat.



4. Saisissez le mot de passe associé au certificat, puis appuyez sur **OK**. Une nouvelle boîte de dialogue s'affiche vous demandant de choisir le type de certificat.



5. Sélectionnez le type **Certificat de VPN ou d'application**, puis appuyez sur **OK**. Une nouvelle boîte de dialogue s'affiche vous demandant d'attribuer un nom au certificat. Vous pouvez garder le nom par défaut contenu dans le certificat ou attribuer un autre nom.



Vous pouvez importer un même certificat autant de fois que vous le souhaitez en lui attribuant un nom différent à chaque fois.

6. Un message s'affiche brièvement pour indiquer que l'importation du certificat a réussi.

Vous pouvez visualiser les certificats utilisateurs importés dans le magasin de certificats du terminal mobile. Pour cela, ouvrez les **Paramètres** du terminal mobile. Ensuite, en fonction de la version d'Android et de l'interface personnalisée du fabricant, sélectionnez les options suivantes pour accéder à la liste de certificats utilisateurs : **Données biométriques et sécurité** > **Autres paramètres de sécurité** > **Certificats utilisateur**.

Vous pouvez aussi rechercher le terme « certificat » dans les paramètres du terminal mobile pour afficher tous les paramètres liés aux certificats.

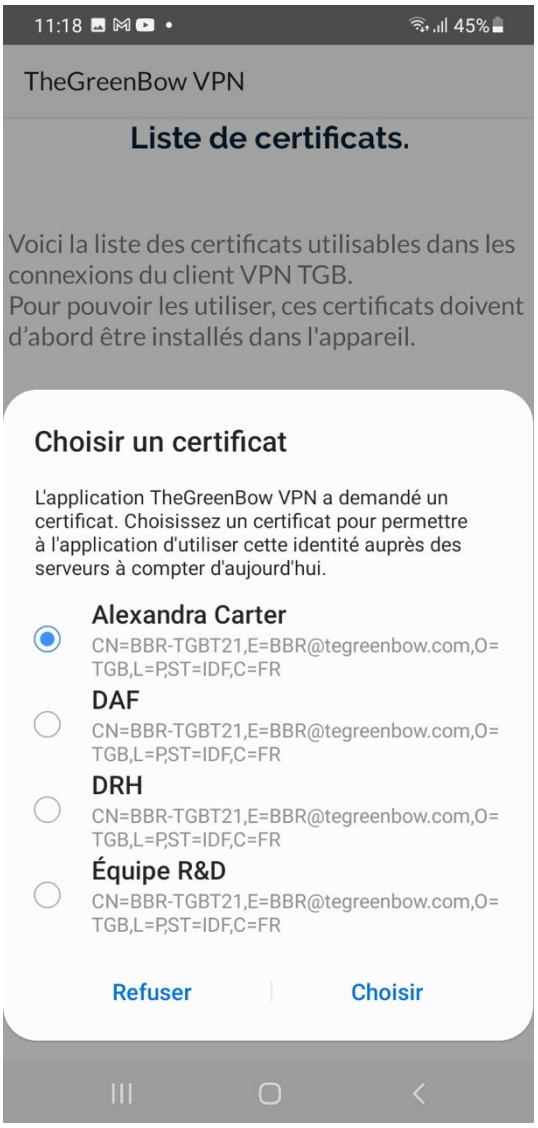
7.3 Référencer un certificat dans le Client VPN Android

Dès lors que vous avez importé un ou plusieurs certificats dans le magasin de certificats du terminal mobile, vous pouvez les référencer dans la liste de certificats du Client VPN Android. Pour cela, procédez de la manière suivante :

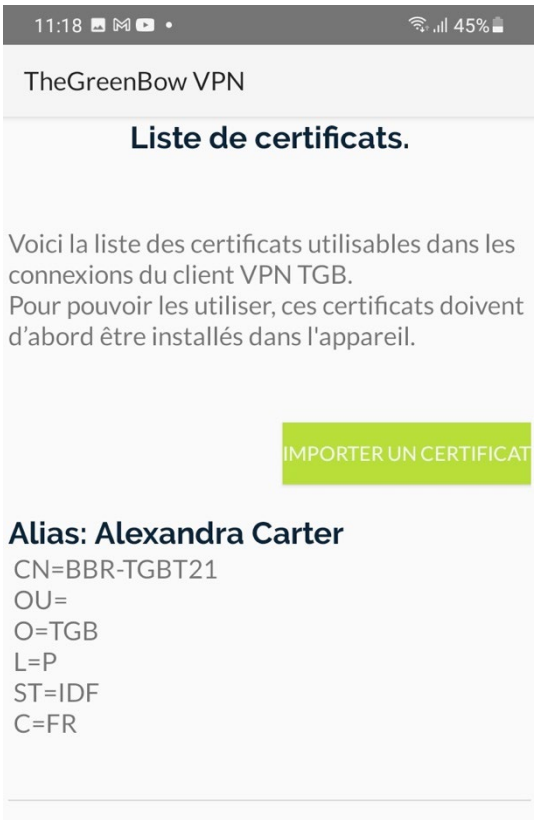
1. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Outils**, puis **Référencer les certificats**.

2. Appuyez sur le bouton **IMPORTER UN CERTIFICAT**. Une boîte de dialogue s'affiche vous invitant de choisir un certificat parmi la liste de certificats du magasin de certificats du terminal mobile.

Importer signifie ici que le certificat est simplement référencé dans le Client VPN à partir du magasin de certificats Android. Le certificat doit au préalable avoir été importé dans ce dernier (voir section 7.2 Importer un certificat dans le magasin de certificats du terminal mobile).



3. Sélectionnez le certificat souhaité, puis appuyez sur **Choisir**. Le certificat est ajouté à la liste de certificats du Client VPN Android. Vous pouvez désormais importer une configuration qui utilise ce certificat.


11:18
45%
TheGreenBow VPN
Liste de certificats.
Voici la liste des certificats utilisables dans les connexions du client VPN TGB.
Pour pouvoir les utiliser, ces certificats doivent d'abord être installés dans l'appareil.
IMPORTER UN CERTIFICAT
Alias: Alexandra Carter
CN=BBR-TGBT21
OU=
O=TGB
L=P
ST=IDF
C=FR

8 Configuration des connexions VPN

8.1 Introduction

Pour vous connecter à votre propre réseau distant, le Client VPN Android doit comporter une configuration VPN créée à l'aide d'un Client VPN Windows TheGreenBow sur un ordinateur de bureau ou portable.

Pour savoir comment créer un fichier de configuration VPN, reportez-vous au Guide de l'administrateur de votre Client VPN Windows.

Une fois que vous avez créé une configuration VPN et que vous l'avez exportée dans un fichier de configuration VPN, celui-ci doit être importé dans le Client VPN Android.

Vous pouvez également modifier, exporter ou supprimer une configuration VPN existante.

8.2 Importer un fichier de configuration VPN

Pour importer une configuration VPN créée à l'aide d'un Client VPN Windows TheGreenBow sur un poste de travail, procédez comme suit :

1. Transférez le fichier de configuration VPN de l'ordinateur vers le terminal mobile.
2. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Configuration**, puis **Importer un fichier de configuration**.
3. Sélectionnez le fichier à importer dans l'explorateur de fichiers qui s'affiche.

La nouvelle connexion VPN est ajouté à la liste des connexions.

Pour savoir comment créer un fichier de configuration VPN, reportez-vous au Guide de l'administrateur de votre Client VPN Windows.

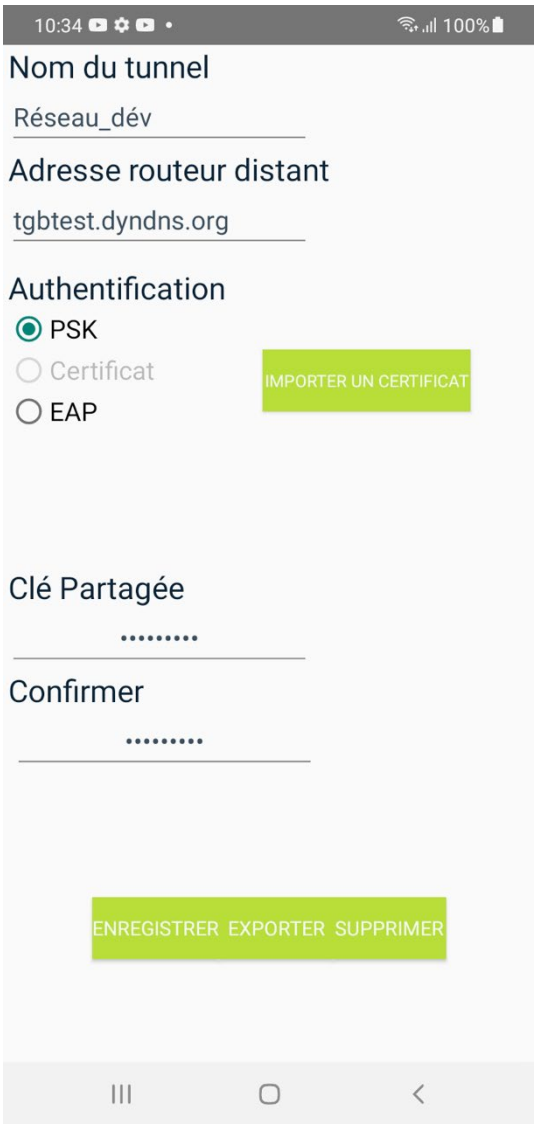
Si une erreur se produit lors de l'importation, il est probable que le fichier de configuration n'est pas correctement paramétré. Par exemple, le Client VPN Android n'accepte pas le protocole IKEv1. Dans ce cas, il convient de corriger le paramétrage du fichier de configuration VPN dans le Client VPN Windows et de l'importer à nouveau.

8.3 Modifier la configuration d'une connexion VPN

Dès lors que vous avez importé une configuration VPN, vous pouvez la modifier à partir de la liste des connexions VPN. Pour ce faire :

4. À partir de la liste des connexions VPN, effectuez un appui long sur la connexion VPN dont vous souhaitez modifier la configuration.

   La configuration de la connexion VPN s'affiche :



   Vous pouvez modifier les éléments suivants :

   - le nom du tunnel,
   - l'adresse du routeur distant,
   - le type d'authentification et
   - la clé partagée.

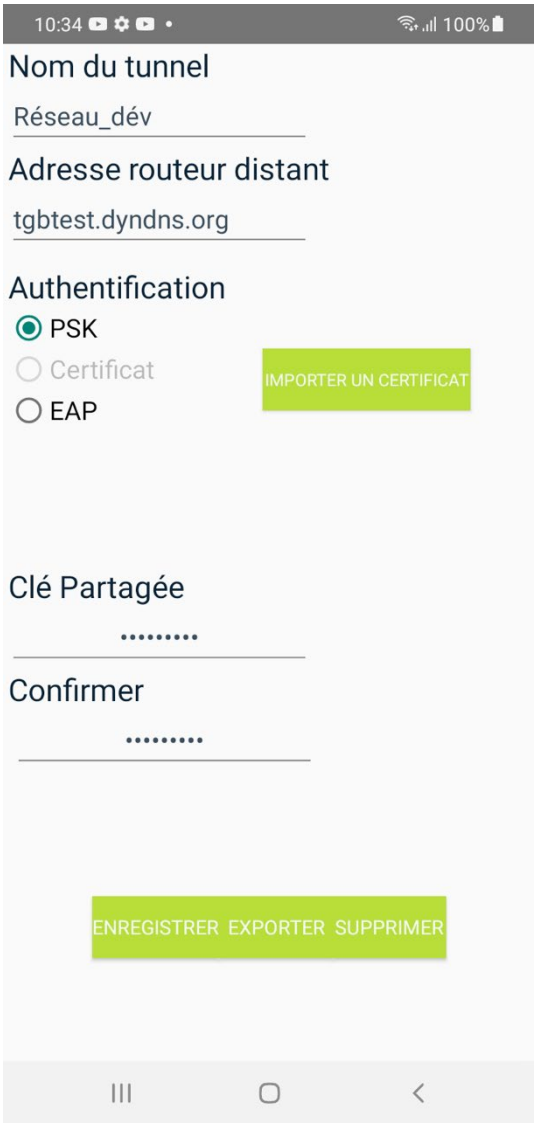
   Vous pouvez également importer un certificat au format P12 ou PFX (voir section 8.4 Importer un certificat dans la configuration d'une connexion ci-dessous).

5. Appuyez sur **ENREGISTRER** pour enregistrer vos modifications.

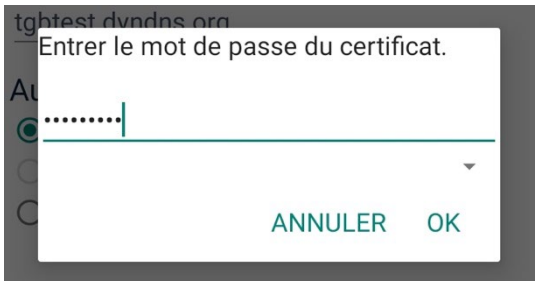
8.4 Importer un certificat dans la configuration d'une connexion

Un certificat peut être importé dans la configuration d'une connexion à partir d'un fichier de certificat stocké sur le terminal mobile. Pour cela, suivez les étapes ci-dessous :

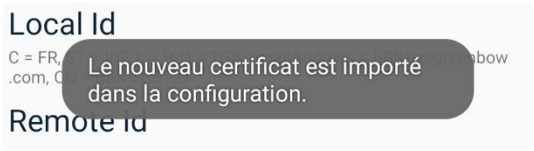
1. Effectuez un appui long sur une connexion pour l'ouvrir en mode édition. L'écran d'édition de la configuration s'affiche.



2. Appuyez sur le bouton **IMPORTER UN CERTIFICAT**. Une fenêtre de gestionnaire de fichiers s'affiche vous permettant de sélectionner le fichier de certificat.
3. Sélectionnez le fichier souhaité. Une boîte de dialogue s'affiche vous demandant de renseigner le mot de passe associé au certificat.



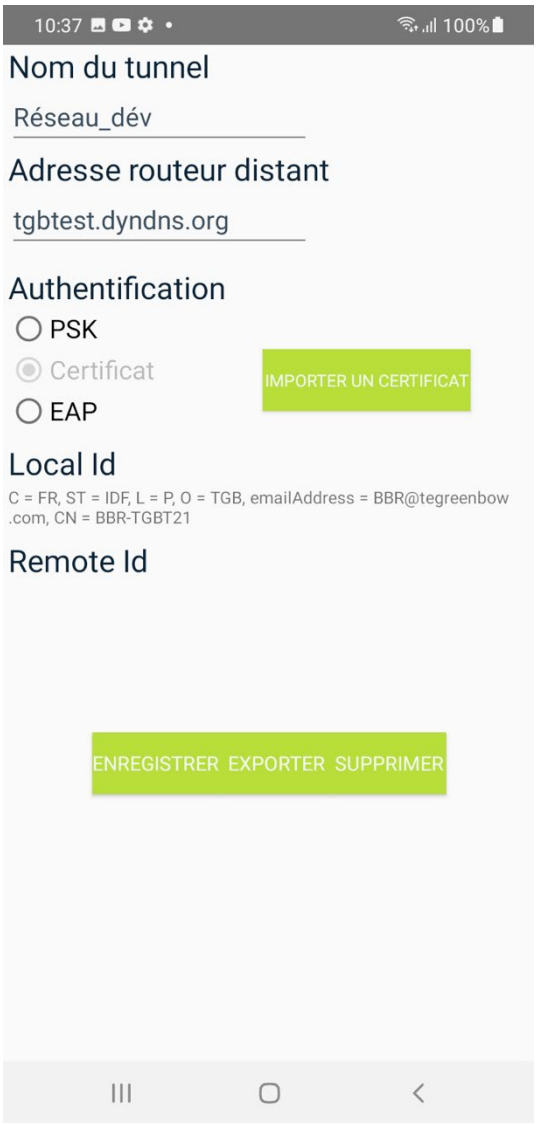
4. Saisissez le mot de passe. Un message s'affiche pour indiquer que l'importation du certificat a réussi.



5. Le mode d'authentification **Certificat** est sélectionné et grisé. Les caractéristiques du certificat figurent sous **Local ID** et/ou **Remote ID**.

Le **Local ID** est l'identifiant de la phase d'authentification que le Client VPN envoie à la passerelle VPN distante. Le **Remote ID** est l'identifiant de la phase d'authentification que le Client VPN s'attend à recevoir de la passerelle VPN distante. Reportez-vous au Guide de l'administrateur du Client VPN Windows Enterprise pour plus de détails.

Le **Local ID** sur le routeur est le **Remote ID** sur le Client VPN et inversement !

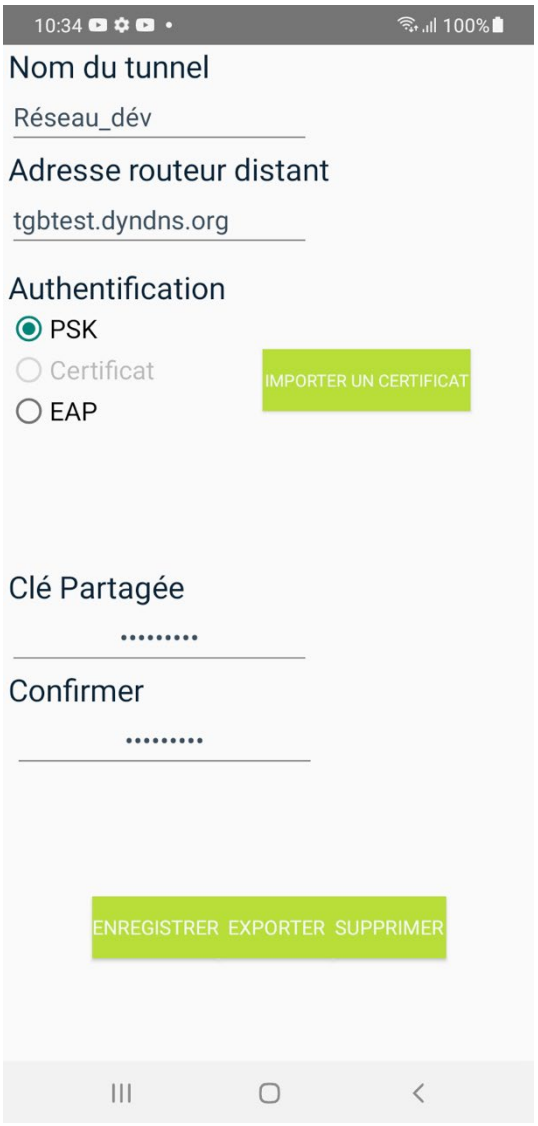


8.5 Exporter la configuration d'une connexion VPN

Pour exporter une configuration VPN, procédez comme suit :

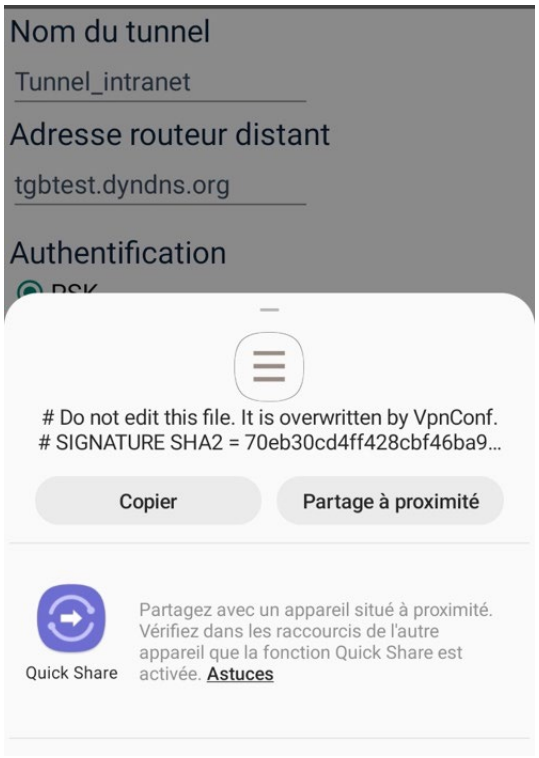
1. À partir de la liste des connexions VPN, effectuez un appui long sur la connexion VPN dont vous souhaitez exporter la configuration.

La configuration de la connexion VPN s'affiche :



2. Appuyez sur le bouton **EXPORTER** en bas de l'écran.

Le volet **Partager** de l'appareil mobile s'affiche :



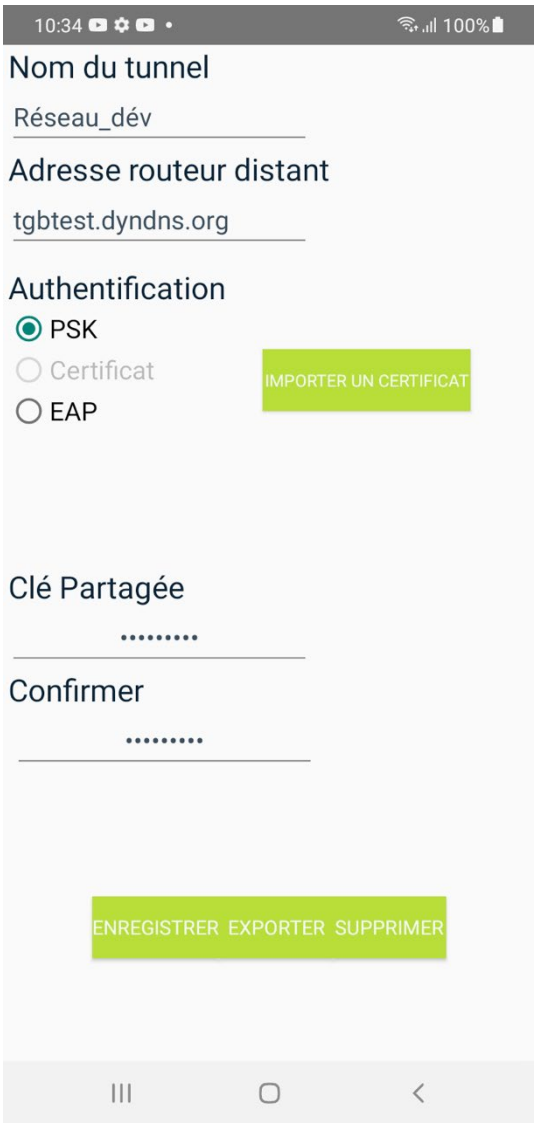
3. Vous pouvez copier la configuration et la coller dans un document ou l'envoyer directement par e-mail ou toute autre application de messagerie disponible dans le volet **Partager**.

8.6 Supprimer une connexion VPN

Pour supprimer une connexion VPN, procédez comme suit :

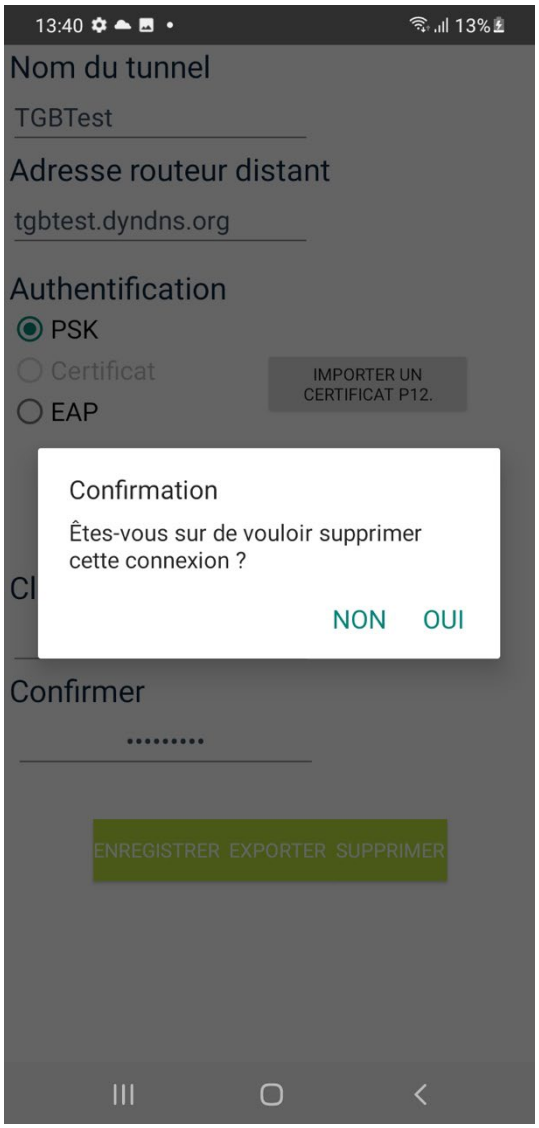
1. À partir de la liste des connexions VPN, effectuez un appui long sur la connexion VPN que vous souhaitez supprimer.

La configuration de la connexion VPN s'affiche :



2. Appuyez sur le bouton **SUPPRIMER** en bas de l'écran.

Une fenêtre pop-up s'affiche vous demandant de confirmer la suppression :



3. Appuyez sur **OUI** pour confirmer la suppression. La configuration est supprimée et la connexion disparaît de la liste des connexions.

9 Ouverture d'une connexion VPN

9.1 Introduction

Dès que vous avez configuré une ou plusieurs connexions VPN, il suffit d'appuyer sur le nom de la connexion pour l'ouvrir.

Par défaut, le Client VPN Android fonctionne en mode interactif. Depuis la version 6.2 du logiciel, vous pouvez activer la fonction **VPN permanent**. Dans ce cas, le VPN sera activé en permanence même lorsque vous quittez l'application ou que vous redémarrez le terminal mobile.

9.2 Ouvrir une connexion VPN IKEv2

Pour ouvrir une connexion IKEv2, appuyez sur le nom de la connexion que vous souhaitez ouvrir dans la liste des connexions VPN.

La première fois que vous ouvrez une connexion IKEv2, un mot de passe ne sera requis que si **EAP** a été configuré. Dans ce cas, entrez le mot de passe associé à l'identifiant lorsque vous y êtes invité.

9.3 Ouvrir une connexion VPN SSL

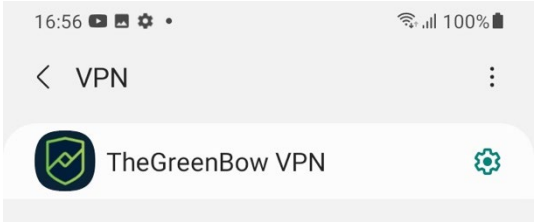
Pour ouvrir une connexion SSL, appuyez sur le nom de la connexion dans la liste des connexions VPN.

La première fois que vous ouvrez une connexion SSL, un mot de passe ne sera requis que si **Extra Auth** a été configuré. Dans ce cas, entrez le mot de passe Extra Auth lorsque vous y êtes invité.

9.4 Activer la fonction VPN permanent

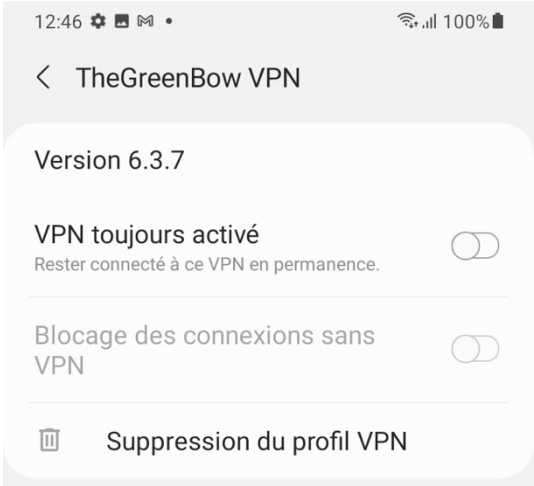
Depuis la version 6.2 du Client VPN Android, vous pouvez activer le VPN de manière permanente de telle sorte qu'il reste activé y compris lorsque vous quittez l'application ou que vous redémarrez le terminal mobile. Pour ce faire, suivez les étapes ci-dessous :

1. Assurez-vous qu'aucune connexion n'est ouverte dans le Client VPN Android et que la connexion que vous souhaitez utiliser en permanence se trouve en haut de la liste des connexions.
2. Accédez aux **Paramètres** du terminal mobile, en fonction de la version d'Android et de l'interface du fabricant, sélectionnez ensuite **Connexions**, puis **Plus de paramètres de connexion** et enfin **VPN**. Une liste d'applications VPN présentes dans le terminal mobile s'affiche.



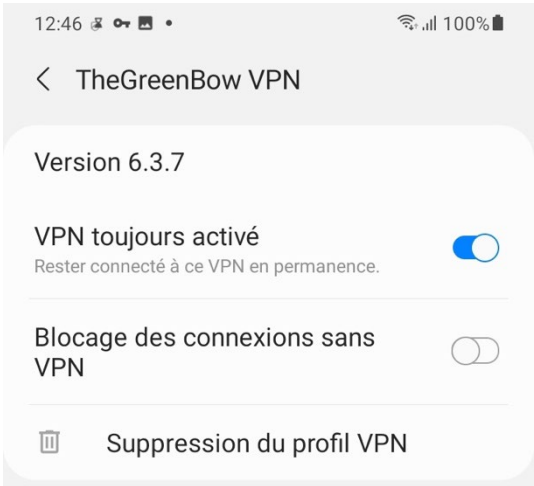
Vous pouvez aussi ouvrir les **Paramètres** du terminal mobile, puis recherchez le terme « VPN » pour afficher tous les paramètres relatifs aux VPN.

3. Dans la liste, recherchez l'application TheGreenBow VPN et appuyez sur l'engrenage à droite du nom. Les options du profil VPN s'affichent.



4. Dans les réglages de l'application TheGreenBow VPN, activez l'option **VPN toujours activé**.

Dans d'autres version d'Android, cette option s'appelle aussi **VPN permanent**.

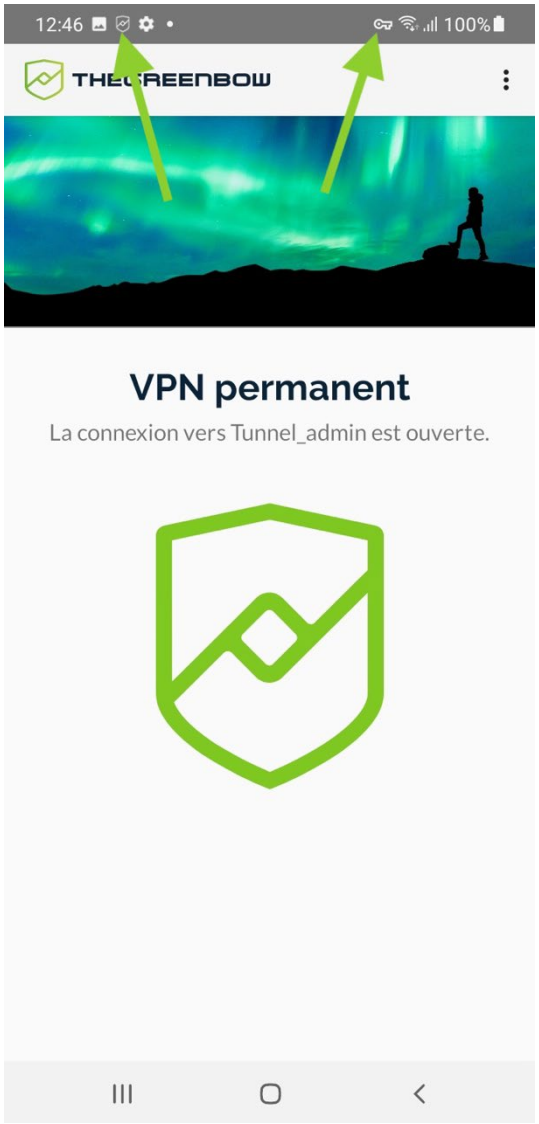


La fonction **VPN permanent** est désormais activée.

⚠ Si vous activez l'option **VPN toujours activé** dans les paramètres système alors qu'une connexion est ouverte dans le Client VPN Android, cela pourrait entraîner un fonctionnement incorrect de l'application.

ℹ Vous pouvez aussi activer l'option **Blocage des connexions sans VPN**. Dans ce cas, aucune autre connexion à part celle passant par le VPN ne pourra être établie.

Lorsque vous ouvrez l'application TheGreenBow VPN, à la place de la liste de connexions, vous verrez un message indiquant que la fonction **VPN permanent** est activée ainsi que le nom de la connexion ouverte.



Par ailleurs, deux icônes s'affichent dans la barre d'état du terminal mobile.

Pour en savoir davantage sur les icônes affichées dans la barre d'état, reportez-vous à la section 6.5 Icônes d'état.

Lorsque vous activez la fonction **VPN permanent** et que plusieurs connexions sont présentes dans la liste des connexions, le Client VPN Android sélectionne la première connexion de la liste. Assurez-vous que celle-ci correspond bien à la connexion que vous souhaitez activer en permanence.

9.5 Désactiver la fonction VPN permanent

Pour désactiver la fonction suivez les étapes ci-dessous :

1. Accédez aux **Paramètres** du terminal mobile, en fonction de la version d'Android et de l'interface du fabricant, sélectionnez ensuite **Connexions**, puis **Plus de paramètres de connexion** et enfin **VPN**. Une liste d'applications VPN présentes dans le terminal mobile s'affiche.
2. Dans la liste, recherchez l'application **TheGreenBow VPN** et appuyez sur l'engrenage à droite du nom. Les options du profil VPN s'affichent.
3. Dans les réglages de l'application TheGreenBow VPN, désactivez l'option **VPN toujours activé**.

La connexion est fermée. Les icônes TheGreenBow et clé disparaissent de la barre d'état. Vous pouvez utiliser le Client VPN Android en mode VPN interactif.

10 Journalisation

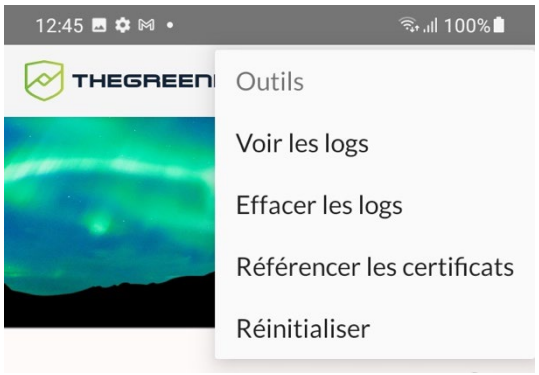
Le Client VPN Android propose une facilité de journalisation qui vous permet d'effectuer les opérations suivantes :

- afficher les entrées de journalisation dans l'interface utilisateur,
- partager les entrées de journalisation avec d'autres utilisateurs et
- effacer les entrées de journalisation actuelles.

10.1 Afficher les logs

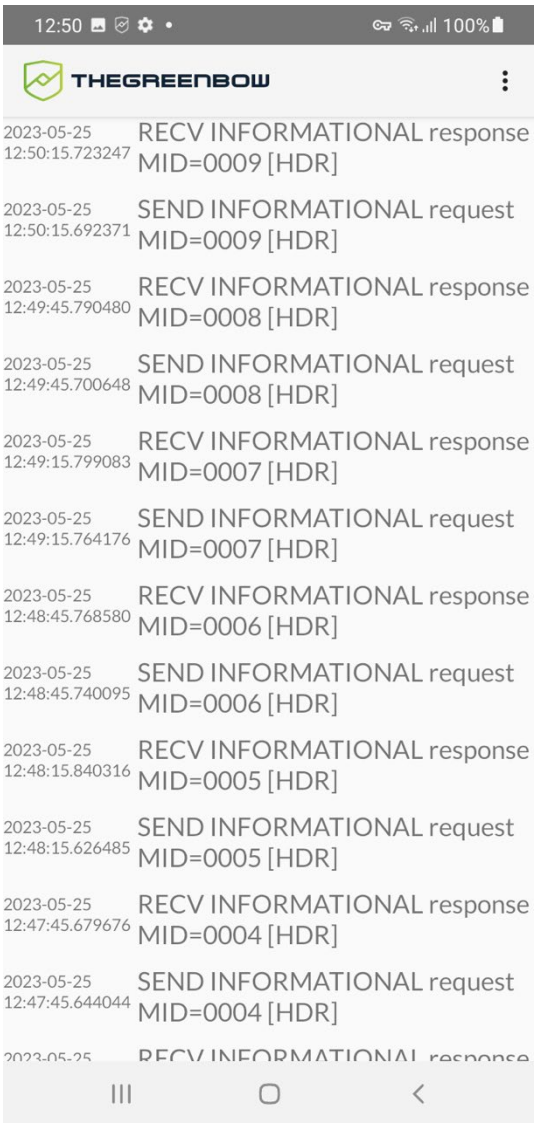
La facilité de journalisation fournit des informations détaillées sur les étapes d'ouverture et de fermeture des tunnels VPN. Les administrateurs peuvent utiliser ces informations pour identifier d'éventuels problèmes de connexion.

Pour afficher les entrées de journalisation, ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Outils**, puis **Voir les logs**.



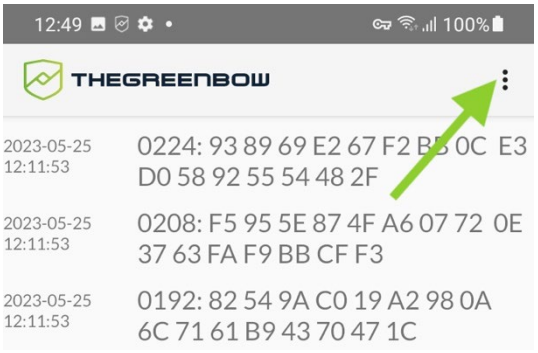
Vous pouvez activer un mode verbeux pour obtenir des journaux plus détaillés. Pour cela, sélectionnez l'option **Mode verbeux** dans le menu contextuel de la fenêtre des logs (voir ci-dessous) ou activez le bouton correspondant dans la fenêtre **À propos** (voir section 6.3.4 Sous-menu À propos...).

Les entrées de journalisation s'affichent à l'écran :



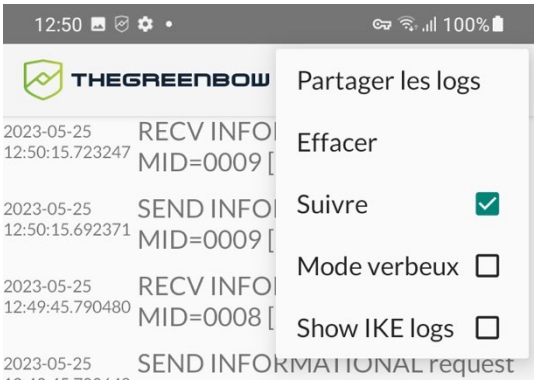
Les entrées de journalisation affichées sont celles de la dernière connexion VPN que vous avez ouverte.

Depuis la version 6.3 du Client VPN Android, un menu contextuel s'affiche à la place du menu à trois points verticaux sur la fenêtre des logs.

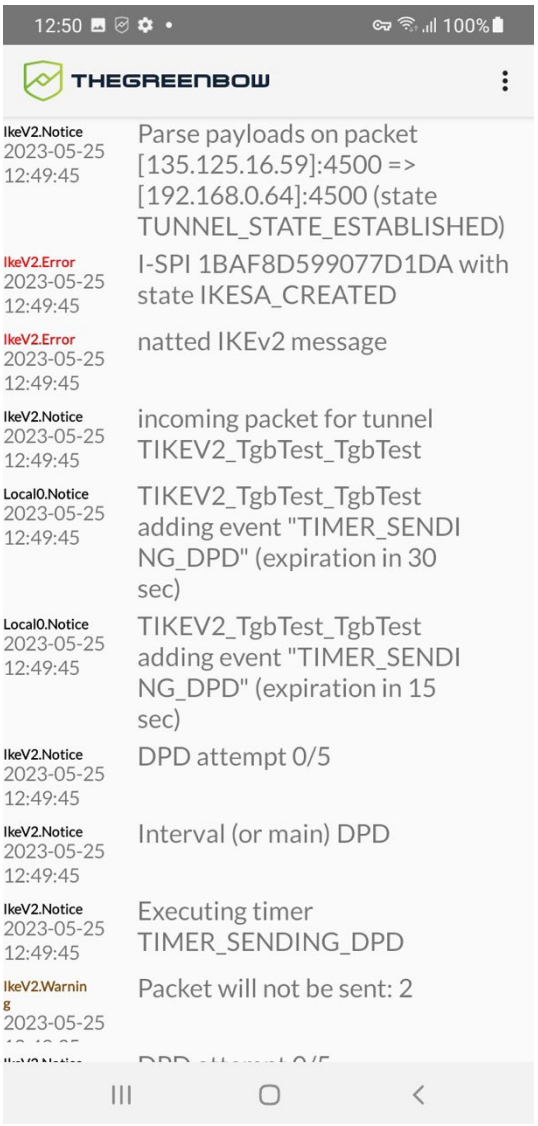


Ce menu contient les options suivantes :

- **Partager les logs**, voir section 10.2 Partager les logs ci-dessous ;
- **EFFACER**, voir section 10.3 Effacer les logs ci-dessous ;
- **Suivre**, permet d'arrêter ou relancer le défilement des entrées de journalisation ;
- **Mode verbeux**, permet d'activer et désactiver le mode verbeux (cette option est également disponible dans la fenêtre **À propos**) ;
- **Show IKE logs**, permet d'afficher les entrées de journalisation IKE.



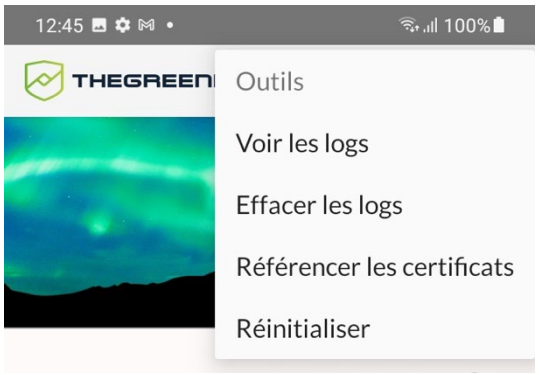
Lorsque l'option **Show IKE logs** est sélectionnée, la fenêtre des logs se présente comme suit :



10.2 Partager les logs

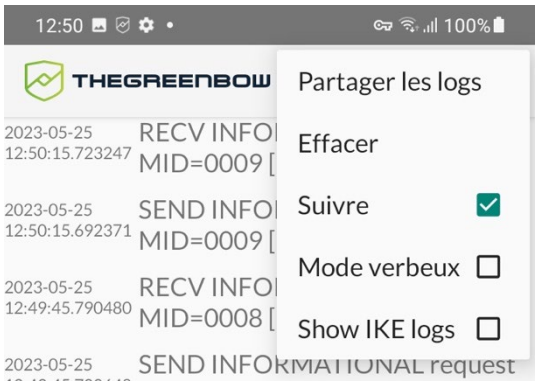
Pour exporter les entrées de journalisation et les partager avec d'autres utilisateurs, p. ex. le support technique, procédez comme suit :

1. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Outils**, puis **Voir les logs**.



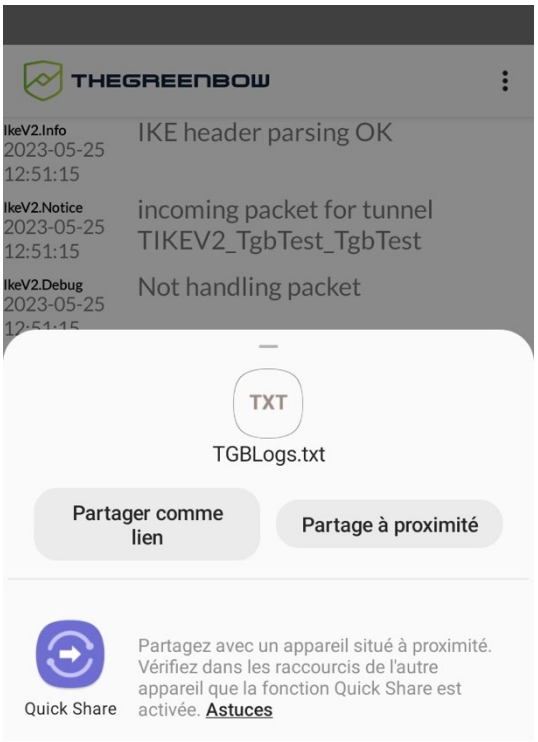
La fenêtre des logs s'affiche.

2. Ouvrez le menu situé en haut à droite de la vue (trois points verticaux). Le menu contextuel s'affiche.



3. Sélectionnez l'option **Partager les logs**.

Le volet **Partager** de l'appareil mobile s'affiche :

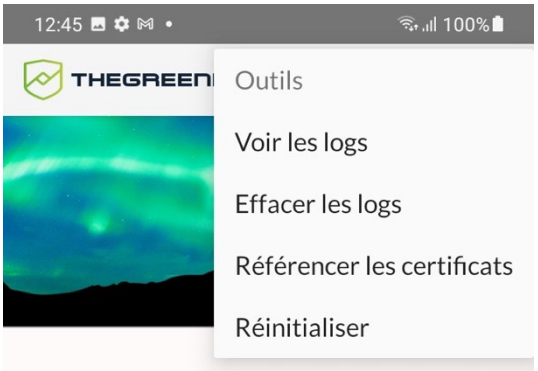


4. Les entrées de journalisation sont consignées dans un fichier journal appelé `TGBLogs.txt` que vous pouvez partager par tous les moyens disponibles dans le volet **Partager**.

10.3 Effacer les logs

Pour effacer les entrées de journalisation actuellement chargée dans l'interface utilisateur, procédez comme suit :

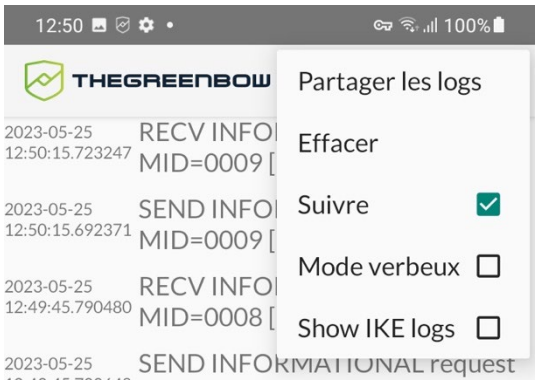
1. Ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Outils**, puis **Effacer les logs**.



Les entrées de journalisation sont effacées. Si vous affichez la fenêtre des logs, l'écran est vide. Dès que vous lancez une nouvelle connexion, les nouvelles entrées de journalisation générées seront visibles.

Vous pouvez également effacer les entrées de journalisation à partir du menu contextuel de la fenêtre des logs. Pour cela, procédez comme suit :

2. Ouvrez le menu situé en haut à droite de la vue (trois points verticaux). Le menu contextuel s'affiche.



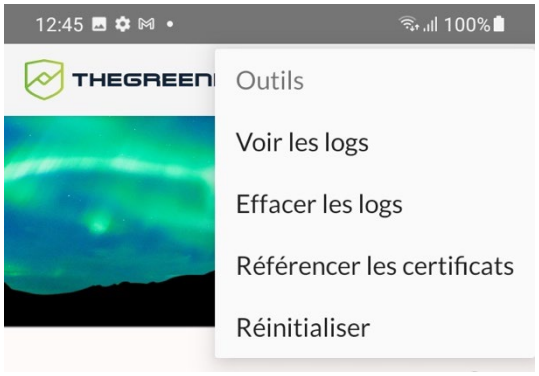
3. Sélectionnez l'option **EFFACER**.

11 Dépannage

11.1 Réinitialiser l'application

Lorsque vous n'arrivez pas à fermer un tunnel, qu'un tunnel se trouve dans un état instable ni ouvert ni fermé ou que le Client VPN ne répond plus, vous pouvez réinitialiser l'application. Les traitements qu'elle réalise en arrière-plan seront alors remis à l'état initial. L'arrêt des processus sera forcé afin de repartir sur des bases saines.

Pour ce faire, ouvrez le menu situé en haut à droite de l'écran principal (trois points verticaux), sélectionnez **Outils**, puis **Réinitialiser**.



L'application est réinitialisée et l'écran principal s'affiche.

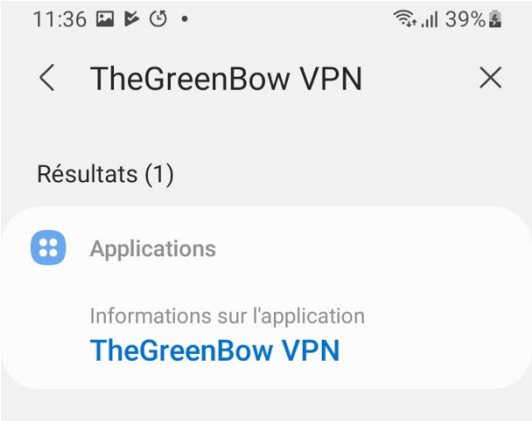
11.2 Supprimer les données de l'application

Dans certains cas, notamment lorsque vous rencontrez des difficultés avec l'activation, le support technique peut vous demander de supprimer les données de l'application.

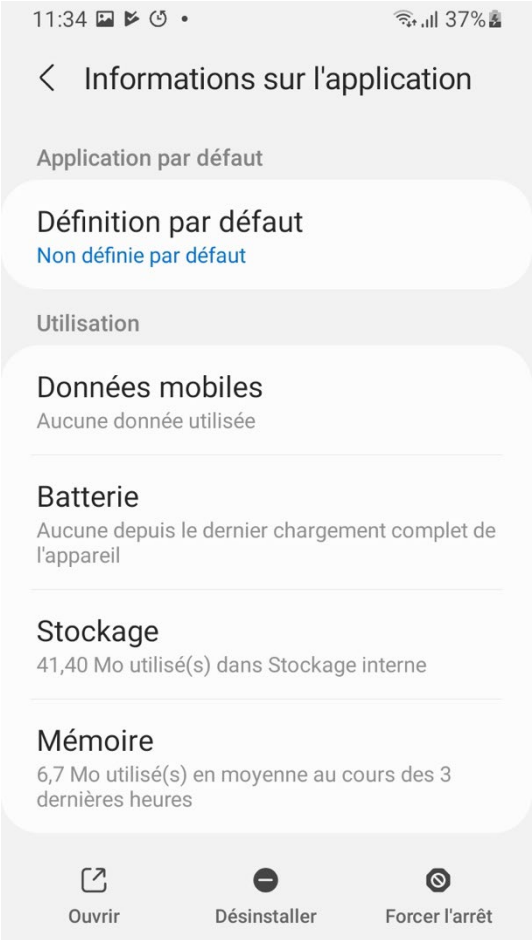
Toutes les données de l'application que vous avez configurées, à savoir les connexions, les données d'activation et les fichiers journaux seront supprimées du terminal mobile. L'application se comportera alors comme lors de la première installation.

Pour supprimer les données de l'application, procédez comme suit :

1. Recherchez l'application TheGreenBow VPN dans les paramètres du terminal.

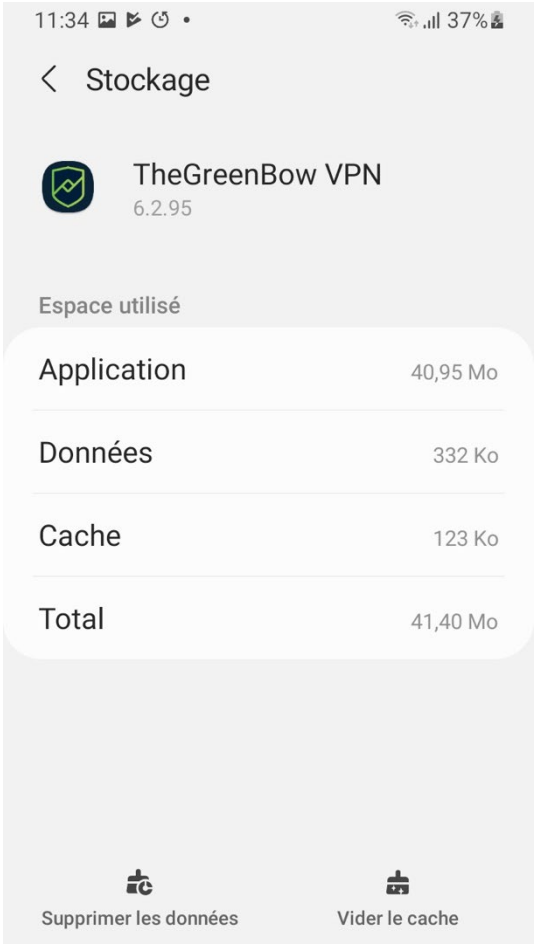


2. Appuyez sur **TheGreenBow VPN** dans les résultats de la recherche.



3. Sélectionnez **Stockage**.

Les informations de stockage s'affichent :



4. Appuyez sur **Supprimer les données**, puis appuyez sur **OK** pour valider le message de confirmation qui s'affiche.

Toutes les données de l'application sont supprimées.

12 Caractéristiques techniques

12.1 Général

Version de l'OS	Android 10 et supérieur
Langues	Français, anglais

12.2 Connexion / Tunnel

Mode de connexion	Peer-to-Gateway (voir la liste des passerelles qualifiées et leurs guides de configuration)
Protocoles	SSL : OpenVPN IPsec : IKEv2
Mode Configuration Payload (CP)	Récupération automatique des paramètres réseaux depuis la passerelle VPN

12.3 Cryptographie et authentification

Chiffrement, Groupes de clé, Hachage (IKEv2)	• Symétrique : AES CBC/CTR/GCM 128/192/256 bits • Groupes de clé Diffie-Hellman : DH 14 (MODP 2048), DH 15 (MODP 3072), DH 16 (MODP 4096), DH 17 (MODP 6144), DH 18 (MODP 8192), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (ECP 521), DH 28 (BrainpoolP256r1) • Algorithme de hachage : SHA-2 (256/384/512 bits, IKEv2 uniquement)
Chiffrement, Hachage (OpenVPN)	Symétrique : AES-128-CBC, AES-192-CBC, AES-256-CBC Hachage : SHA-2 (224/256/384/512 bits)

Suites de sécurité TLS (OpenVPN)	TLS 1.2 – Medium TLS 1.2 – High TLS 1.3 : • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Authentification	• IKEv2 : certificats X.509, EAP-MSCHAPv2, clé partagée, Multiple Auth (certificat + EAP) • SSL : certificats X509, Extra-Auth (certificat + identifiant et mot de passe)
Méthodes d'authentification des certificats (IKEv2)	• Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296] • Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754] • Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754] • Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754] • Méthode 14 : signature numérique RSASSA-PSS et RSASSA-PKCS1-v1_5 [RFC 7427] • Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits)
IGC / PKI	• Prise en charge des certificats X509 • Import de certificats au format PKCS#12, PFX • Multi-support : magasin de certificats Android, fichier de configuration • Vérification complète de la chaîne des certificats « utilisateur » et « passerelle » (avec CA racine dans la configuration)

13 Contact

13.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : https://thegreenbow.com/.

13.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

13.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/assistance/support-technique/.

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com