Client VPN Linux 3.4

Guide de l'administrateur

Dernière mise à jour : 5 décembre 2024
Référence du document : 20241205_AG_VLX_3.4_FR_1.3

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-02-07	Toutes	Version initiale	EBO, FB, BB
1.1	2024-09-23	3.3	Ajout de précisions relatives aux dépendances	EBO, BB
1.2	2024-11-13	14	Ajout du chapitre sur la sélection du noyau	EBO, BB
1.3	2024-12-05	2.2 & 2.3 6.2 14	Mise à jour des procédures de vérification du logiciel Précision concernant l'activation après mise à jour vers la version 3.4.4 Mise à jour du chapitre sur la sélection du noyau	EBO, BB

1 Présentation

1.1 Introduction

Merci d'avoir téléchargé le logiciel Client VPN Linux 3.4.

Le Client VPN Linux a été spécialement pensé pour répondre aux besoins des grands comptes, OIV/OSE et administrations civiles et gouvernementales. Procurant un niveau élevé de sécurisation des communications, il est facile à déployer, à intégrer et simple à utiliser.

Le Client VPN Linux bénéficie en outre d'un support personnalisé qui va d'un suivi dédié à la prise en compte d'évolutions spécifiques.

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 Linux est commercialisé sous forme d'abonnement annuel. Cet abonnement inclut un support dédié et la maintenance du logiciel.

1.2 Sécurité

Conçu pour équiper les postes nomades, le Client VPN Linux est un logiciel client VPN IPsec IKEv2 pour postes de travail Linux, qui permet d'établir des connexions avec le système d'information de l'entreprise via internet, de façon parfaitement sécurisée. Il implémente une large variété d'algorithmes de chiffrement et de hachage, ainsi que différentes méthodes d'authentification forte.

1.3 Ergonomie

Facile à installer, facile à configurer et à déployer, parfaitement transparent pour l'utilisateur, le Client VPN Linux est aujourd'hui reconnu pour son ergonomie inégalée.

1.4 Simplicité

Nos guides de configuration facilitent les opérations d'intégrations et de déploiement en accélérant la mise en place d'une solution VPN de bout en bout.

1.5 Universalité

Le Client VPN Linux fonctionne sous Ubuntu 22.04 (noyaux 5.x) & 24.04 (noyaux 6.x) et RedHat 9. Le logiciel est compatible avec de très nombreux pare-feux/passerelles IPsec du marché. La liste, en constante évolution, des pare-feux/passerelles testés dans notre laboratoire est disponible sur le site TheGreenBow.

1.6 Fonctionnalités

- Pilote réseau IPsec et module IKE développés par TheGreenBow
- Module IPsec intégré en mode noyau
- Prise en charge du protocole IKEv2
- Interopérable avec tous les pare-feux/passerelles VPN compatibles IKEv2
- Chiffrement : AES CBC, CTR et GCM 128 / 192 / 256 bits
- Hachage : SHA-2 256/384/512
- Groupes de clés : DH 14-21, 28
- Gestion des certificats X.509 : PEM/PFX, PKCS #12[1]
- Authentification : clé partagée, certificats, EAP, double authentification (certificat + EAP)
- Fragmentation IP
- Mode « tout le trafic dans le tunnel »
- Dead Peer Detection (DPD) : détection de trafic interrompu avec la passerelle
- Passerelle redondante
- Mode CP (Configuration Payload)
- Négociation automatique des algorithmes avec la passerelle
- Fragmentation IKEv2
- Mode NAT-Traversal automatique
- Local ID, Remote ID
- Importation de configurations VPN générées par le Client VPN Windows Enterprise de TheGreenBow
- Pilotage en ligne de commande ou par interface graphique
- Activation par licence
- Prise en charge du format et du protocole de journaux d'évènements syslog
- Deux paquets, chacun étant compatible avec l'une des versions de distributions Linux suivantes :
  - RedHat version 9, 64 bits
  - Ubuntu 22.04 (noyaux 5.x) & 24.04 (noyaux 6.x), 64 bits
- Intégration dans le menu système (systray)

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

1.7 Nouveautés de la version 3.4

1.7.1 Fonctionnalités

- Compatible avec la majorité des passerelles IPsec et SSL, y compris celles configurées en mode IPsec DR
- Prise en charge du RFC 6023 (Childless IKE Initiation) pour une sécurité accrue

1.7.2 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 3.4 du Client VPN Linux 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
- 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

2 Téléchargement et vérification du logiciel

2.1 Introduction

Le Client VPN Linux est disponible en téléchargement sur le site TheGreenBow.

Avant de procéder à l'installation du Client VPN Linux, il est important de vérifier l'authenticité du paquet logiciel téléchargé, afin de confirmer qu'il a bien été signé par TheGreenBow et qu'il n'a subi aucune altération.

2.2 Procédure de vérification sous RedHat

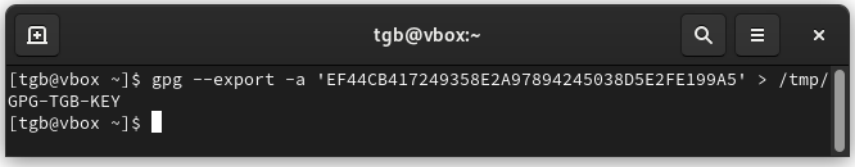
Pour vérifier l'authenticité du paquet RedHat, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal.
2. Exécutez la commande suivante pour télécharger la clé publique :

```
gpg --keyserver keys.openpgp.org --recv-keys
EF44CB417249358E2A97894245038D5E2FE199A5
```

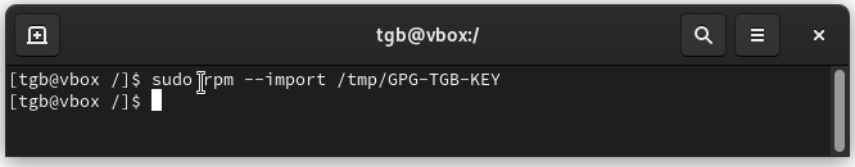
3. Exécutez la commande suivante pour exporter la clé vers un fichier temporaire :

```
gpg --export -a
'EF44CB417249358E2A97894245038D5E2FE199A5' > /tmp/GPG-
TGB-KEY
```



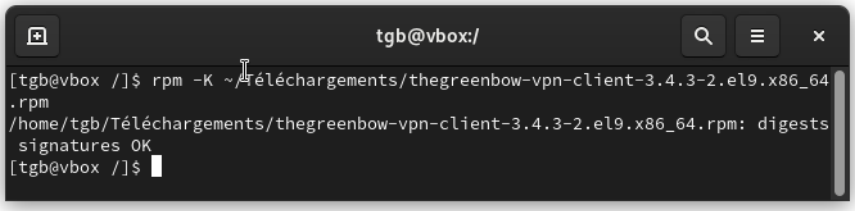
4. Exécutez la commande suivante pour importer la clé :

```
sudo rpm --import /tmp/GPG-TGB-KEY
```



5. Vérifiez le paquet logiciel en exécutant la commande suivante dans le répertoire où se trouve le paquet (ici `Téléchargements`, où r est le numéro de révision du logiciel et b le numéro de build du logiciel) :

```
rpm -K ~/Téléchargements/thegreenbow-vpn-client-3.4.r-b.el9.x86_64.rpm
```



6. Vérifiez que les informations en sortie sont bien les suivantes :

```
/home/[nom_utilisateur]/Téléchargements/thegreenbow-vpn-client-3.4.r-b.el9.x86_64.rpm: digests signatures OK
```

Si ce n'est pas le cas, contactez le support client : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

2.3 Procédure de vérification sous Ubuntu

Pour vérifier l'authenticité du paquet Ubuntu, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal (Ctrl + Alt + T).
2. Exécutez la commande suivante pour télécharger la clé publique et l'importer dans le magasin de clés GPG local :

```
gpg --keyserver keys.openpgp.org --recv-keys EF44CB417249358E2A97894245038D5E2FE199A5
```

3. Vérifiez le paquet logiciel en exécutant la commande suivante dans le répertoire où se trouve le paquet (remplacer le r par le numéro de révision du logiciel et le b par le numéro de build du paquet logiciel) :

```
gpg --verify thegreenbow-vpn-client-3.4.x-r.amd64.deb
```

4. Vérifiez que les informations en sortie sont bien les suivantes :

```
Bonne signature de « TGB Linux product manager
linux@thegreenbow.com »
```

Si ce n'est pas le cas, contactez le support client : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

2.4 Informations techniques

Le paquet d'installation est signé avec une clé RSA de 4096 bits. La clé publique correspondante est disponible sous ce lien : https://keys.openpgp.org/vks/v1/by-fingerprint/EF44CB417249358E2A97894245038D5E2FE199A5.

Identifiant de la clé : `EF44 CB41 7249 358E 2A97 8942 4503 8D5E 2FE1 99A5`.

Empreinte de la clé : `2FE199A5`.

2.4.1 Suppression de la clé sous RedHat

1. Exécutez la commande suivante pour récupérer l'identifiant complet de la clé :

```
rpm -q gpg-pubkey --qf
'%{NAME}-%{VERSION}-%{RELEASE}\t%{SUMMARY}\n'
```

Les informations en sortie doivent indiquer le nom de la clé avec ses numéros de version et de révision comme suit :

```
gpg-pubkey-2fe199a5-[numéro_révision]   TGB Linux
product manager linux@thegreenbow.com public key
```

2. Exécutez la commande suivante pour supprimer la clé en remplaçant le numéro de révision avec les résultats obtenus à l'étape précédente :

```
sudo rpm --erase gpg-pubkey-2fe199a5-[numéro_révision]
```

2.4.2 Suppression de la clé sous Ubuntu

Pour supprimer la clé publique du magasin de clés GPG local, exécutez la commande suivante :

```
gpg --delete-key
EF44CB417249358E2A97894245038D5E2FE199A5
```

3 Installation

3.1 Introduction

Après avoir téléchargé le Client VPN Linux à partir du site web TheGreenBow et vérifié son authenticité (voir chapitre 2 Téléchargement et vérification du logiciel), l'installation peut s'effectuer en ligne de commande.

3.2 Conditions d'installation

Pour installer le Client VPN Linux vous devez disposer des privilèges de super-utilisateur (ou *root*) sur la machine.

Par ailleurs, vous devrez créer un fichier de configuration à utiliser sur le poste Linux à l'aide du Client VPN Windows Enterprise.

3.3 Dépendances

Lors de l'installation le Client VPN Linux vérifie la présence des dépendances suivantes :

- `dkms`[1] et `systemd-resolved`[2] sous RedHat
- `dkms`[3] sous Ubuntu

Si l'un de ces paquets est absent lors de l'installation, le Client VPN n'est pas installé et un message d'erreur indique les paquets manquants.

Pour vérifier la présence de `systemd-resolved` sous RedHat, exécutez la commande suivante :

```
systemd-resolved --status
```

[1] La dépendance DKMS est fournie par EPEL. Les administrateurs ne souhaitant pas ajouter de dépendances externes à leur réseau peuvent contourner EPEL en ajoutant DKMS dans un dépôt interne.
[2] Ce paquet est requis pour la prise en charge du DNS dans une interface virtuelle.
[3] Ce paquet est installé par défaut sous Ubuntu.

Pour installer `systemd-resolved` sous RedHat, exécutez successivement les commandes suivantes :

```
dnf install systemd-resolved
systemctl enable systemd-resolved.service
ln -sf /run/systemd/resolve/stub-resolv.conf
/etc/resolv.conf
```

Si `systemd-resolved` est présent mais non activé, il suffit d'exécuter les deux dernières commandes ci-dessus.

3.4 Contenu du paquet

Lors de l'installation du Client VPN Linux, les répertoires et fichiers suivants seront ajoutés sur le poste :

- `/usr/bin/tgbtray` : programme qui gère l'icône du Client VPN Linux dans le menu système (*systray*)
- `/usr/bin/tgbctl` : commande permettant de piloter le Client VPN Linux en ligne de commande
- `/usr/sbin/tgbiked` : daemon du Client VPN Linux qui tourne en tâche de fond
- `/lib/systemd/system/tgbiked.service` : fichier de configuration du daemon
- `/etc/tgb/conf.tgb` : fichier de configuration VPN, incluant un tunnel de test TheGreenBow
- `/etc/tgb/vpnsetup.json` : fichier de licence du Client VPN Linux
- `/usr/share/doc/thegreenbow/CLUF_VPN_TheGreenBow_vFR3.51.pdf` : document contenant le Contrat de Licence Utilisateur Final TheGreenBow
- `/usr/share/icons/thegreenbow` : dossier contenant les icônes utilisées par `tgbtray`
- `/usr/share/applications/thegreenbow.desktop` : lanceur de l'application
- `/usr/src/tgbtun-1.2` : dossier contenant les sources pour la gestion dynamique des modules noyau (DKMS)

3.5 Procédure d'installation

Le Client VPN Linux doit être installé en ligne de commande.

☞ Pour RedHat voir la section 3.5.1 Sous RedHat.

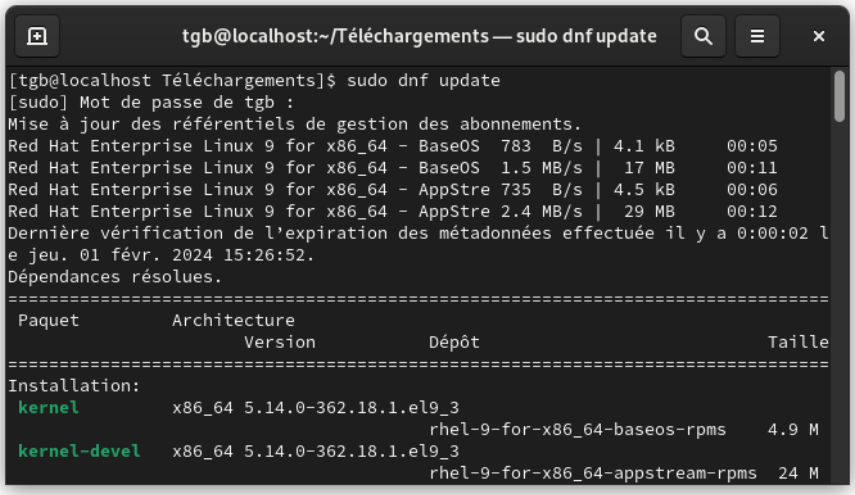
☞ Pour Ubuntu, voir la section 3.5.2 Sous Ubuntu.

3.5.1 Sous RedHat

Pour installer le Client VPN Linux sous RedHat, procédez de la manière suivante :

1. Si vous avez téléchargé le paquet logiciel à partir d'une autre machine que celle sur laquelle le Client VPN Linux doit être installé, copiez-le vers la machine de destination.
2. Ouvrez une fenêtre de terminal.
3. Exécutez la commande suivante pour mettre à jour les dépôts de paquets :

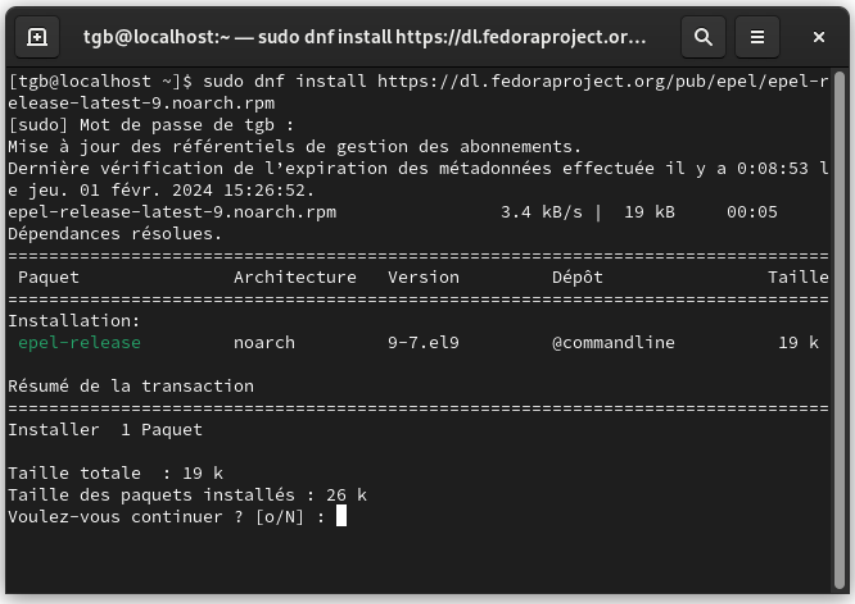
```
sudo dnf update
```



4. Exécutez la commande suivante pour installer le paquet complémentaire pour Linux Enterprise[1] :

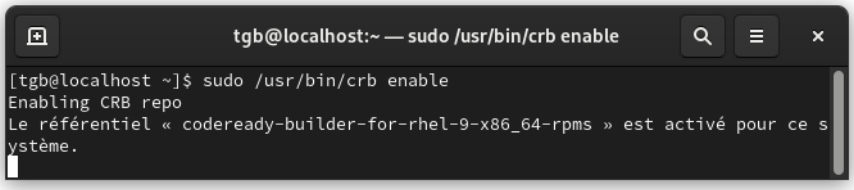
```
sudo dnf install
https://dl.fedoraproject.org/pub/epel/epel-release-
latest-9.noarch.rpm
```

[1] Si EPEL ne peut pas être installé sur le poste, il convient de placer les paquets `dkms`, `libappindicator3` et `libdbusmenu` dans le dépôt interne.



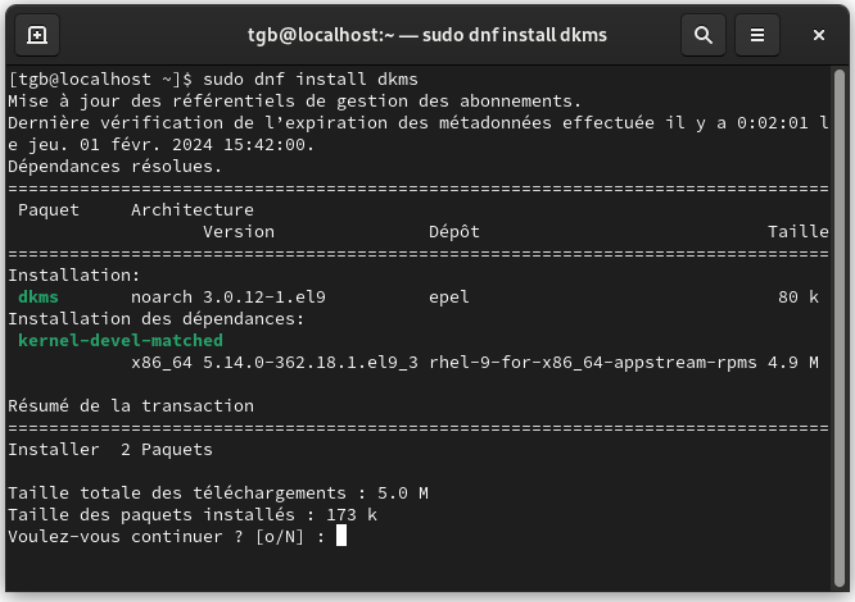
5. Exécutez la commande suivante pour activer le dépôt CRB :

```
sudo /usr/bin/crb enable
```



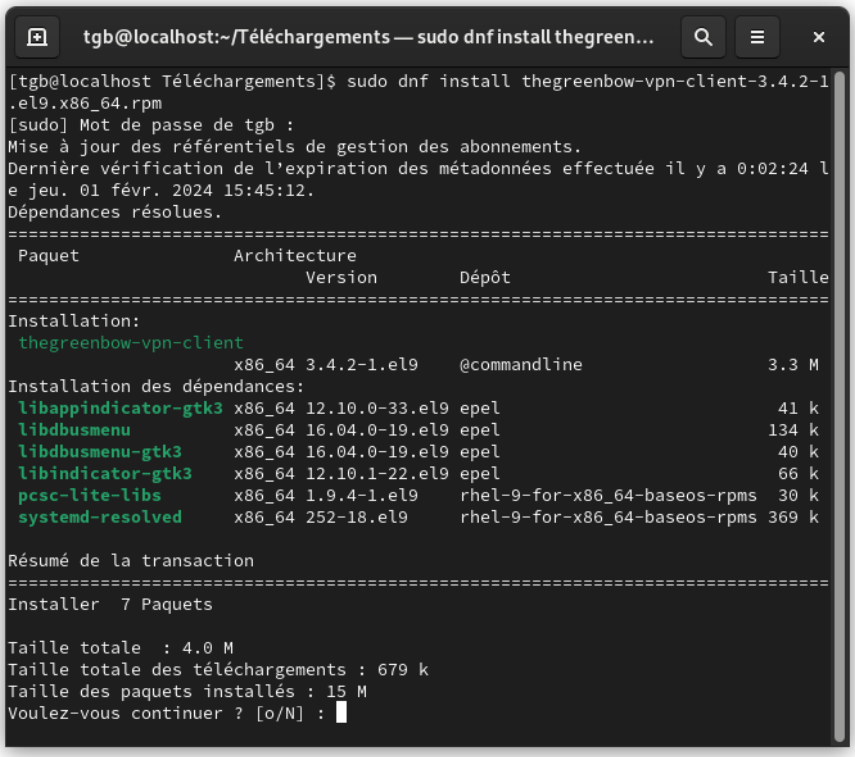
6. Exécutez une nouvelle fois la commande suivante pour installer le paquet `dkms` :

```
sudo dnf install dkms
```



7. Accédez au dossier contenant le paquet `thegreenbow-vpn-client-3.4.r-b.el9.x86_64.rpm` (où r est le numéro de révision du logiciel et b est le numéro de build du logiciel).
8. Exécutez la commande suivante pour installer le logiciel Client VPN Linux (où r est le numéro de révision du logiciel et b est le numéro de build du logiciel) :

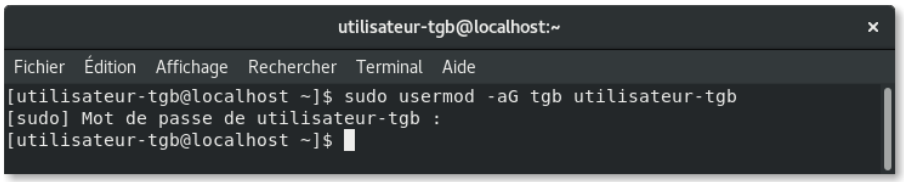
```
sudo dnf install thegreenbow-vpn-client-3.4.r-b.el9.x86_64.rpm
```



9. Ajoutez les utilisateurs du VPN au groupe `tgb` en exécutant la commande suivante :

```
sudo usermod -aG tgb $(whoami)
```

10. Saisissez le mot de passe du compte administrateur et appuyez sur Entrée.



11. Si vous utilisez des cartes à puce Safenet/Gemalto, exécutez la commande suivante :

```
sudo dnf install SafenetAuthenticationClient-10.8.1050-
1.el9.x86_64.rpm
```

12. Si vous souhaitez utiliser le Client VPN Linux immédiatement pendant une période d'évaluation de 30 jours (cf. section 4.2 Période d'évaluation), redémarrez la machine avant de lancer le logiciel, afin que l'ajout des utilisateurs soit pris en compte.

Le Client VPN Linux est installé. Vous pouvez l'utiliser gratuitement pendant une période d'évaluation de 30 jours :

- Pour lancer un tunnel de test, consultez le chapitre 8 Utilisation du tunnel de test.
- Pour installer l'icône **tgbtray** dans le menu système, consultez le chapitre 5 Icône tgbtray dans le menu système.
- Pour configurer des connexions VPN, consultez le chapitre 10 Configuration des connexions VPN.
- Pour connaître les commandes de pilotage du client, consultez le chapitre 9 Ligne de commande.
- Pour activer le produit, consultez le chapitre 4 Activation.
- Pour empêcher le démarrage du pilote avec un noyau non compatible, consultez le chapitre 14 Sélection du noyau.

3.5.2 Sous Ubuntu

Pour installer le Client VPN Linux en ligne de commande sous Ubuntu, procédez de la manière suivante :

1. Si vous avez téléchargé le paquet logiciel à partir d'une autre machine que celle sur laquelle le Client VPN Linux doit être installé, copiez-le vers la machine de destination.
2. Ouvrez une fenêtre de terminal (Ctrl + Alt + T).
3. Accédez au dossier contenant le paquet `thegreenbow-vpn-client-3.4.r-b.amd64.deb` (où r est le numéro de révision du logiciel et b est le numéro de build du logiciel).
4. Exécutez la commande d'installation suivante :

```
sudo apt install ./thegreenbow-vpn-client-3.4.r-b.amd64.deb
```

5. Ajoutez les utilisateurs du VPN au groupe `tgb` en exécutant la commande suivante :

```
sudo usermod -aG tgb $(whoami)
```

6. Saisissez le mot de passe du compte administrateur et appuyez sur Entrée.
7. Si vous souhaitez utiliser le Client VPN Linux immédiatement pendant une période d'évaluation de 30 jours (cf. section 4.2 Période d'évaluation), redémarrez la machine avant de lancer le logiciel, afin que l'ajout des utilisateurs soit pris en compte.

Le Client VPN Linux est installé. Vous pouvez l'utiliser gratuitement pendant une période d'évaluation de 30 jours :

- Pour lancer un tunnel de test, consultez le chapitre 8 Utilisation du tunnel de test.
- Pour installer l'icône **tgbtray** dans le menu système, consultez le chapitre 5 Icône tgbtray dans le menu système.
- Pour configurer des connexions VPN, consultez le chapitre 10 Configuration des connexions VPN.
- Pour connaître les commandes de pilotage du client, consultez le chapitre 9 Ligne de commande.
- Pour activer le produit, consultez le chapitre 4 Activation.
- Pour empêcher le démarrage du pilote avec un noyau non compatible, consultez le chapitre 14 Sélection du noyau.

4 Activation

4.1 Introduction

Vous pouvez utiliser le Client VPN Linux gratuitement avec toutes ses fonctionnalités pendant une période d'évaluation de 30 jours (cf. section 4.2 Période d'évaluation ci-dessous).

À l'issue de la période d'évaluation de 30 jours, vous ne pourrez plus utiliser le logiciel. Si vous souhaitez continuer à l'utiliser, nous vous invitons à acquérir une licence.

Les licences sont disponibles sous forme d'abonnement. Consultez la page du Client VPN Linux sur le site TheGreenBow pour en connaître tous les détails.

Pour activer le Client VPN Linux, vous devez disposer des privilèges de super-utilisateur (*root*) sur la machine. Vous devez également mettre à jour le fichier de licence nommé `vpnsetup.json` comme décrit ci-dessous à la section 4.4 Procédure d'activation.

4.2 Période d'évaluation

Le fichier de licence `vpnsetup.json` installé par défaut contient 000000000000000000000000 (24 zéros) à la place du numéro de licence et l'adresse e-mail du support TheGreenBow.

Ces informations sont suffisantes pour utiliser le logiciel pendant la période d'évaluation. Vous n'avez aucune intervention à faire sur ce fichier.

Le nombre de jours restant avant l'expiration de la période d'évaluation est indiqué à chaque fois que vous lancez une commande `tgbctl`. Lorsque la période d'évaluation est expirée, toute commande `tgbctl` retourne le code d'erreur suivant :

```
-1 days
```

Vous ne pourrez bénéficier de la période d'évaluation qu'une seule fois.

4.3 Format et contenu du fichier vpnsetup.json

Les informations d'activation du Client VPN Linux doivent être saisies dans un fichier `vpnsetup.json` au format ASCII.

Pour cela, renseignez l'adresse e-mail de l'utilisateur et le numéro de licence qui vous a été fourni comme suit :

```
{
     "license" : "12345678901234567890123456",
     "email" : "nom.utilisateur@entreprise.com"
}
```

Si vous utilisez un serveur d'activation TAS, il convient d'ajouter en outre les paramètres OSA du serveur 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 utilisé sera https. Sinon, le protocole utilisé sera http.

4.4 Procédure d'activation

4.4.1 Activation automatique

Pour activer le Client VPN Linux, suivez les étapes décrites ci-dessous :

1. Ouvrez une fenêtre de terminal.
2. Pour mettre à jour le fichier de licence `vpnsetup.json`, exécutez la commande suivante en remplaçant les X par le numéro de licence et `utilisateur@domaine.com` par l'adresse e-mail associée au numéro de licence :

```
echo -e "{\n\t\"license\" :
\"XXXXXXXXXXXXXXXXXXXXXXXXXX\",\n\t\"email\" :
\"utilisateur@domaine.com\"\n}" | sudo tee
/etc/tgb/vpnsetup.json
```

3. Exécutez la commande suivante pour redémarrer le service :

```
sudo systemctl restart tgbiked.service
```

4. Exécutez la commande suivante pour afficher un journal :

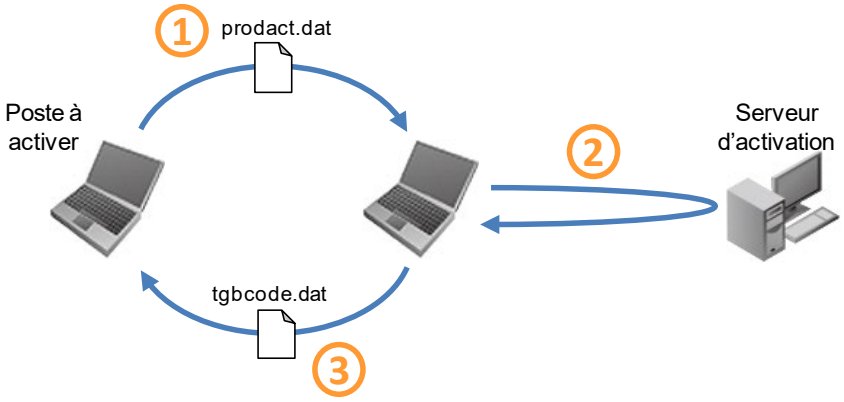
```
systemctl status tgbiked
```

5. Vérifiez que le message suivant est présent dans le journal « Activation succeeded with license number 12345678901234567890123 4. ».
6. Si vous ne l'avez pas déjà fait après l'installation du logiciel, redémarrez la machine.

Pour savoir comment afficher le journal, reportez-vous au chapitre 12 Journaux.

4.4.2 Activation manuelle

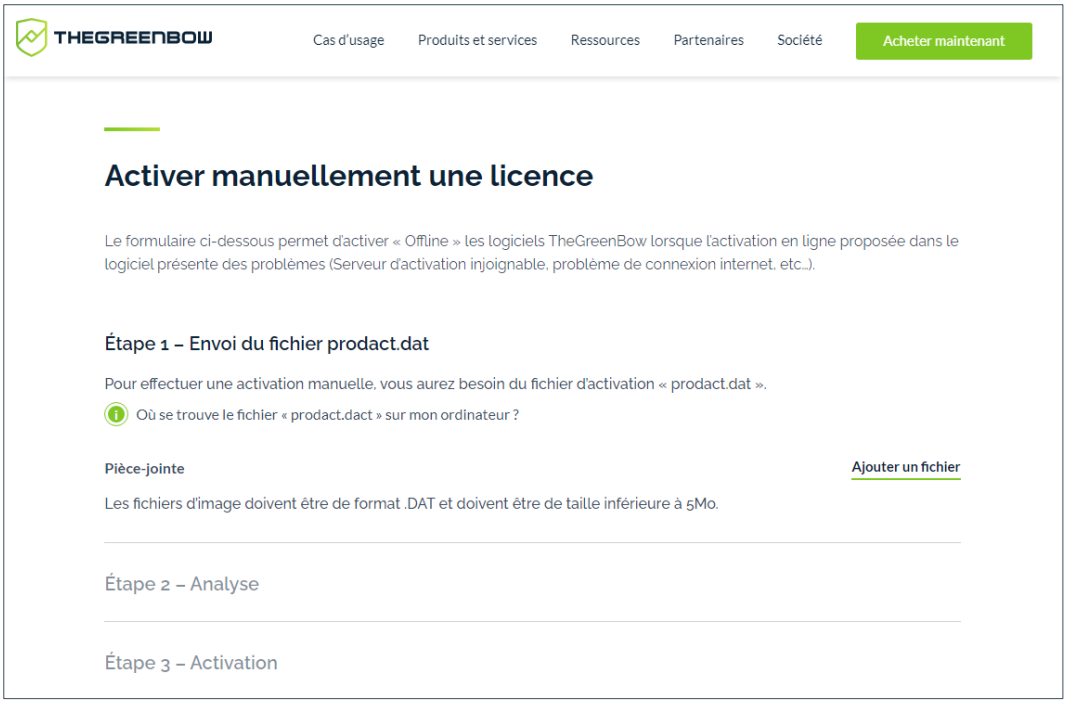
Lorsque l'activation échoue à cause d'un problème de communication avec le serveur d'activation, il est toujours possible d'activer manuellement le logiciel sur le site web TheGreenBow. La procédure est la suivante :



① Fichier `prodact.dat`	Sur le poste à activer, récupérez le fichier `prodact.dat` situé dans le répertoire `/etc/tgb/.osa`.[1]
② Activation	Sur un poste connecté au serveur d'activation[2], ouvrez la page d'activation manuelle[3], postez-y le fichier `prodact.dat` et récupérez le fichier `tgbcode` créé automatiquement par le serveur.
③ Fichier `tgbcode`	Copiez ce fichier `tgbcode` dans le répertoire `/etc/tgb/.osa` du poste à activer. Lancez le logiciel : il est activé.

Pour procéder à l'activation manuelle, suivez les étapes ci-dessous :

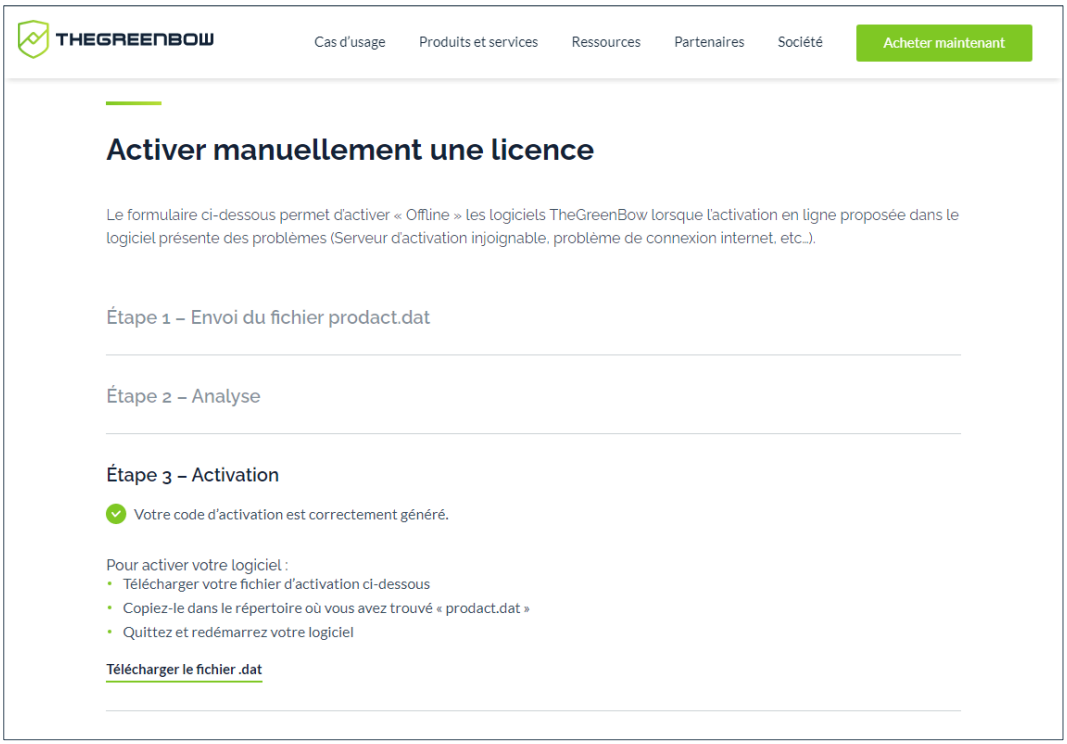
1. Sur un poste ayant une connexion au site web TheGreenBow ouvrez la page web suivante : https://thegreenbow.com/fr/support/gestion-des-licences/activation-manuelle-dune-licence/



2. Cliquez sur le bouton **Ajouter un fichier** et ouvrez le fichier `prodact.dat` créé sur le poste à activer.
3. Cliquez sur **Envoyer**. Le serveur d'activation vérifie la validité des informations du fichier `prodact.dat`.

[1] Le fichier `prodact.dat` est un fichier texte qui contient les éléments du poste utilisés pour l'activation. Si ce fichier n'existe pas dans le répertoire **Documents**, effectuer sur le poste une activation : même si elle échoue, elle a pour effet de créer ce fichier.
[2] Le serveur d'activation est le serveur TheGreenBow, accessible sur internet.
[3] Reportez-vous à la procédure détaillée ci-dessous.

4. Cliquez sur **Effectuer**. Le serveur d'activation présente en téléchargement le fichier contenant le code d'activation destiné au poste à activer.



Ce fichier a un nom de la forme : `tgbcode_[date]_[code].dat` (par exemple : `tgbcode__20231015_1029.dat`).

5. Copiez le fichier généré par le site web vers le chemin `/etc/tgb/.osa` en prenant soin de le renommer `tgbcode_0x19_1.dat`.

```
sudo cp tgbcod__yyyymmdd_xxxx.dat
/etc/tgb/.osa/tgbcode_0x19_1.dat
```

6. Pensez à régler le groupe ayant accès au fichier, ici le groupe `tgb`, en utilisant la commande CLI suivante :

```
sudo chown root:tgb /etc/tgb/.osa/tgbcode_0x19_1.dat
```

7. Procédez à un redémarrage du service :

```
sudo systemctl restart tgbiked.service
```

Les commandes ci-dessus sont valables aussi bien pour RedHat que pour Ubuntu.

4.4.3 Activation réussie

Vous êtes désormais prêt à utiliser le logiciel. Vous pouvez poursuivre avec les étapes suivantes :

- Pour commencer à utiliser le Client VPN Linux avec un tunnel de test, reportez-vous au chapitre 8 Utilisation du tunnel de test.
- Pour ajouter une icône dans le menu système, reportez-vous au chapitre 5 Icône tgbtray dans le menu système.
- Pour créer votre connexion VPN, reportez-vous au chapitre 10 Configuration des connexions VPN.

4.5 Erreurs d'activation

Lorsque l'activation a échoué, l'icône **tgbtray** peut malgré tout être affichée dans le menu système. Dans ce cas, un message d'erreur s'affiche et l'icône devient orange.

Si le journal contient le message `Cancel starting UI Thread, product not activated` et/ou `Activation failed: no activation parameters`, l'activation a échoué. Le Client VPN Linux s'arrête immédiatement.

5 Icône tgbtray dans le menu système

Le Client VPN Linux permet d'afficher une icône dans le menu système (*systray*).

5.1 Ajout de l'icône au menu système

☞ Pour ajouter l'icône sous RedHat, voir la section 5.1.1 Sous RedHat.

☞ Pour ajouter l'icône sous Ubuntu, voir la section 5.1.2 Sous Ubuntu.

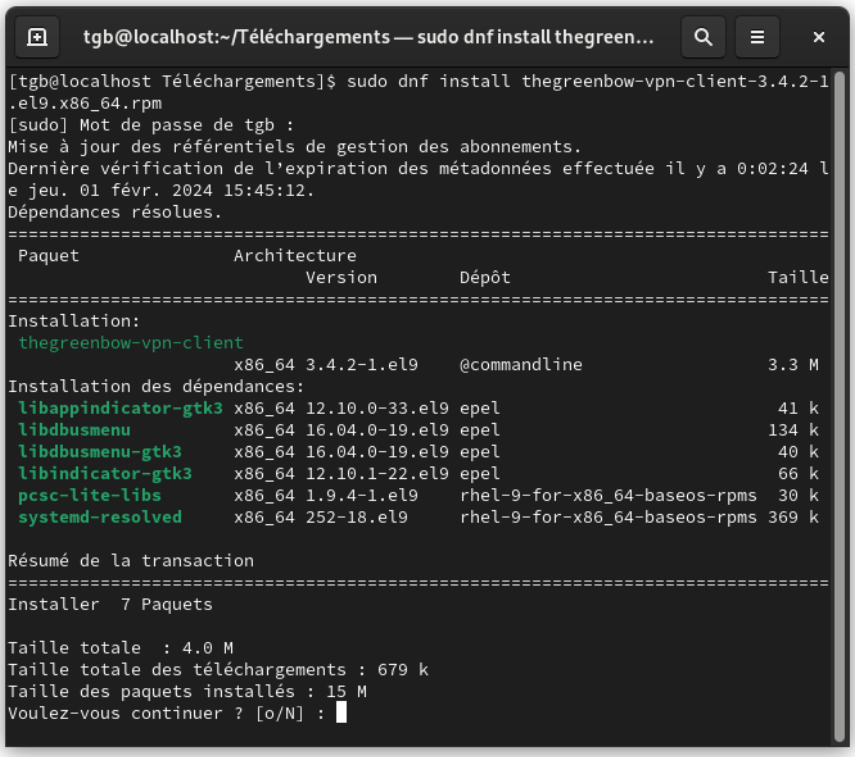
5.1.1 Sous RedHat

Pour ajouter l'icône **tgbtray** au menu système sous RedHat, vous devez d'abord lancer l'environnement de bureau par défaut GNOME[1]. Suivez ensuite les étapes ci-dessous :

1. Ouvrez une fenêtre de Terminal et lancez la commande suivante :

```
sudo dnf install gnome-extensions-app gnome-shell-
extension-appindicator
```

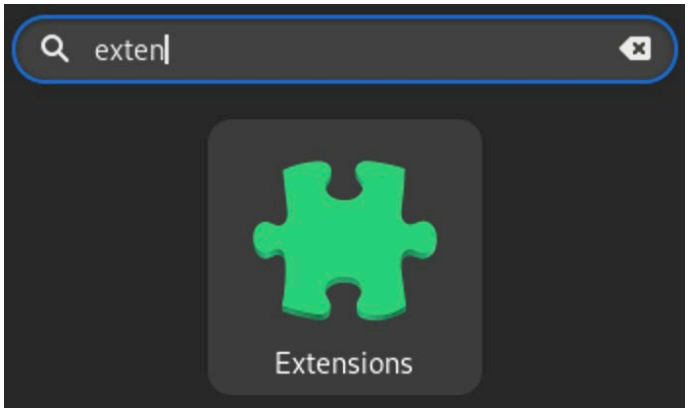
[1] S'il n'est pas installé, reportez-vous à la documentation RedHat pour savoir comment procéder.



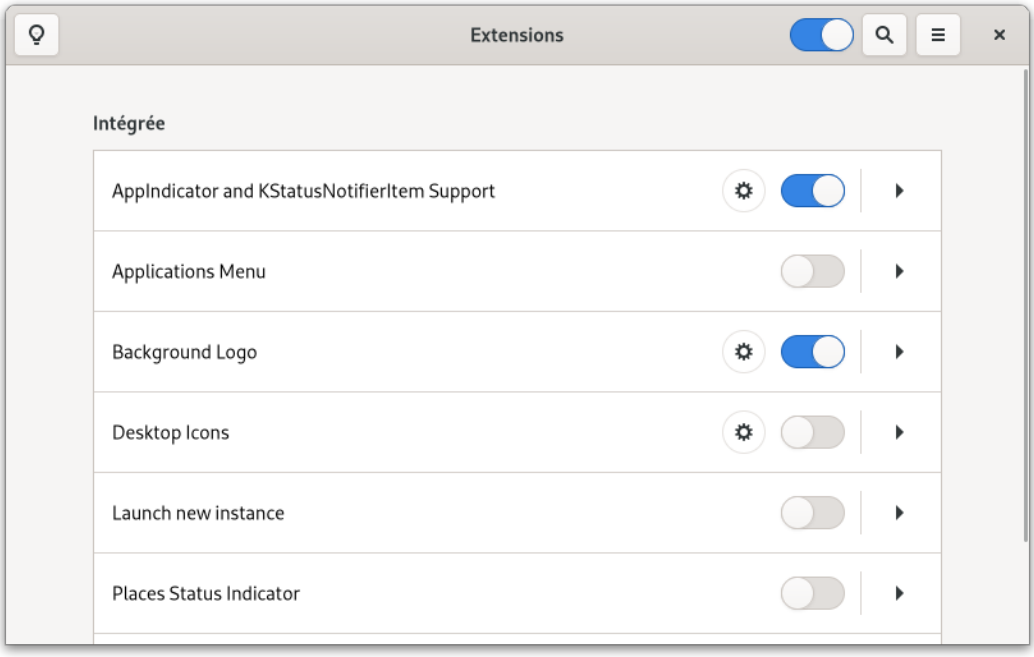
2. Si vous ne l'avez pas déjà fait à l'issue de l'installation, ajoutez les utilisateurs du VPN au groupe `tgb` en exécutant la commande suivante :

```
sudo usermod -aG tgb $(whoami)
```

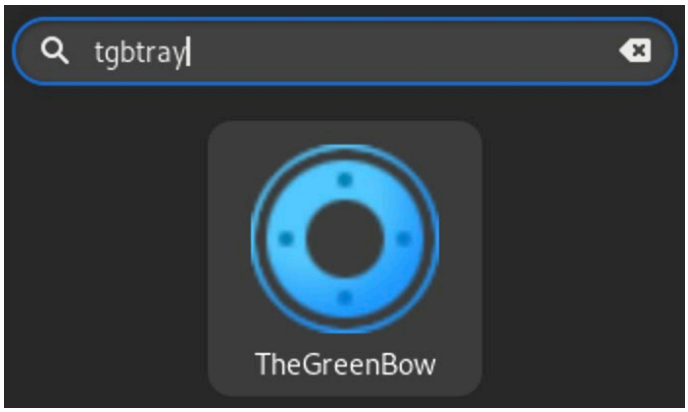
3. Redémarrez le poste.
4. Lancez l'application **Extensions**, p. ex. en effectuant une recherche à partir de l'**Aperçu des activités**.



5. Activez **AppIndicator and KStatusNotifierItem Support**.



6. Lancez l'application **tgbtray**, p. ex. en effectuant une recherche à partir de l'**Aperçu des activités**.



Vous pourrez ensuite utiliser l'icône dans le menu système.

5.1.2 Sous Ubuntu

Pour ajouter l'icône au menu système sous Ubuntu, cliquez sur l'icône TheGreenBow dans les applications ou appuyez sur Alt + F2 pour ouvrir la boîte de dialogue **Lancer une commande** et exécutez la commande `tgbtray`.

Vous pouvez également ajouter l'icône en exécutant la commande `tgbtray` dans une fenêtre de terminal.

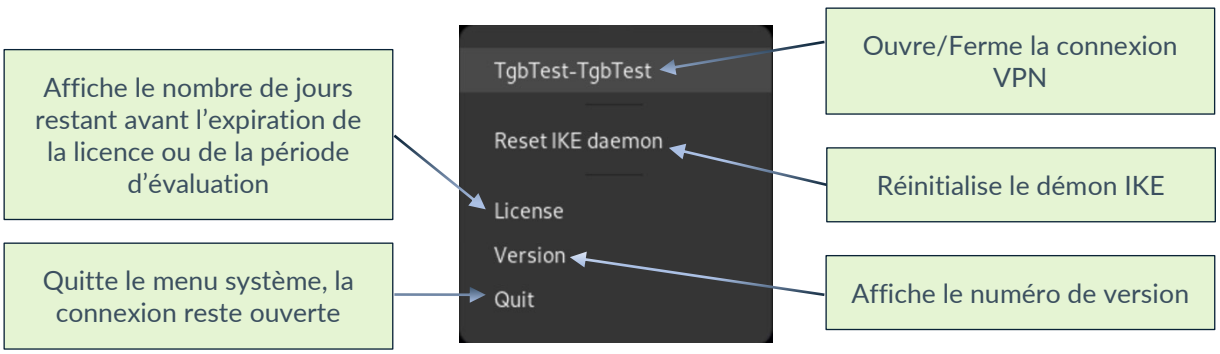
5.2 État de l'icône du menu système

L'icône du Client VPN Linux dans le menu système change de couleur en fonction de l'état de la connexion VPN :

	Icône bleue : aucune connexion VPN n'est active.
	Icône avec flèches tournantes : le tunnel est en cours d'ouverture
	Icône orange : l'ouverture du tunnel a échoué
	Icône verte : une connexion VPN est active.

5.3 Menu contextuel de l'icône dans le menu système

Cliquez sur l'icône pour développer le menu contextuel. Il comporte la liste des connexions VPN configurées ainsi que les commandes suivantes :



Sélectionnez une connexion VPN dans la liste pour l'activer. Vous ne pouvez sélectionner qu'une seule connexion à la fois.

L'icône devient verte dès lors qu'une connexion VPN est active et une coche s'affiche devant le nom de la connexion VPN active.

Si l'icône **tgbtray** du menu système ne répond plus, il est possible de la réinitialiser (voir section 9.10 Réinitialiser l'icône tgbtray).

6 Mise à jour

Si une version précédente du Client VPN Linux est déjà installée sur votre poste, vous pouvez effectuer une mise à jour en ligne de commande.

⚠ Avant de procéder à une mise à jour il convient d'effectuer une sauvegarde du fichier de configuration `conf.tgb` (cf. section 6.1 Sauvegarde du fichier de configuration ci-dessous).

⚠ Dans la version 2.0 du Client VPN Linux, le fichier d'activation était nommé `vpnsetup.ini`. Ce fichier n'est plus compatible avec la version 3.4. Il convient désormais d'utiliser le fichier `vpnsetup.json` comme indiqué dans la procédure de mise à jour ci-dessous.

6.1 Sauvegarde du fichier de configuration

Pour sauvegarder puis restaurer le fichier de configuration `conf.tgb`, procédez comme suit :

1. Copiez le fichier de configuration `conf.tgb` sous `/etc/tgb/` vers un dossier distinct sécurisé.
2. Procédez à la mise à jour.
3. Remplacez le fichier `conf.tgb` installé par celui que vous avez sauvegardé.

⚠ Si vous effectuez une mise à jour à partir d'une version 2.1 ou supérieure du logiciel, il convient également de sauvegarder le fichier de licence `vpnsetup.json`.

6.2 Mise à jour en ligne de commande

Une fois le fichier de configuration sauvegardé (cf. section 6.1 Sauvegarde du fichier de configuration ci-dessus), vous pouvez mettre à jour le Client VPN Linux en ligne de commande.

☞ Pour effectuer la mise à jour sous RedHat, voir la section 6.2.1 Sous RedHat.

☞ Pour effectuer la mise à jour sous Ubuntu, voir la section 6.2.2 Sous Ubuntu.

6.2.1 Sous RedHat

Pour mettre à jour le Client VPN Linux en ligne de commande sous RedHat, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal.
2. Naviguez dans le dossier où se trouve le paquet d'installation que vous avez téléchargé, p. ex. `~/Téléchargements/`.
3. Procédez à l'installation comme décrit à la section 3.5 Procédure d'installation.
4. Copiez le fichier de configuration `conf.tgb` depuis le répertoire de sauvegarde vers le répertoire `/etc/tgb/`.

Si vous effectuez une mise à jour à partir d'une version 2.1 ou supérieure du logiciel, il convient également de restaurer le fichier de licence `vpnsetup.json`. L'identifiant machine utilisé pour l'activation de la machine ayant évolué, il convient de procéder à une activation lors d'une mise à jour vers la version 3.4.4.

5. Procédez à l'activation comme décrit à la section 4.4 Procédure d'activation.

Le Client VPN Linux a été mis à jour. Vous pouvez commencer à utiliser le logiciel.

Pour empêcher le démarrage du pilote avec un noyau non compatible, consultez le chapitre 14 Sélection du noyau.

6.2.2 Sous Ubuntu

Pour mettre à jour le Client VPN Linux en ligne de commande sous Ubuntu, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal (Ctrl + Alt + T).
2. Naviguez dans le dossier où se trouve le paquet d'installation que vous avez téléchargé, p. ex. `~/Téléchargements/`.
3. Procédez à l'installation comme décrit à la section 3.5 Procédure d'installation.
4. Copiez le fichier de configuration `conf.tgb` depuis le répertoire de sauvegarde vers le répertoire `/etc/tgb/`.

Si vous effectuez une mise à jour à partir d'une version 2.1 ou supérieure du logiciel, il convient également de restaurer le fichier de licence `vpnsetup.json`. L'identifiant machine utilisé pour l'activation de la machine ayant évolué, il convient de procéder à une activation lors d'une mise à jour vers la version 3.4.4.

5. Procédez à l'activation comme décrit à la section 4.4 Procédure d'activation.

Le Client VPN Linux a été mis à jour. Vous pouvez commencer à utiliser le logiciel.

Pour empêcher le démarrage du pilote avec un noyau non compatible, consultez le chapitre 14 Sélection du noyau.

7 Désinstallation

Lorsque vous ne souhaitez plus utiliser le Client VPN Linux, vous pouvez le désinstaller en ligne de commande.

☞ Pour RedHat voir la section 7.1 Sous RedHat.

☞ Pour Ubuntu, voir la section 7.2 Sous Ubuntu.

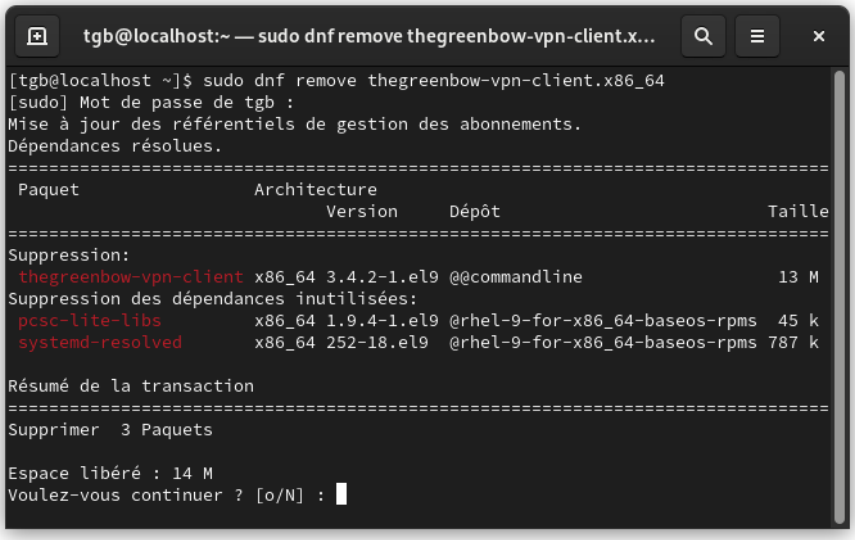
7.1 Sous RedHat

Pour désinstaller le Client VPN Linux sous RedHat, procédez de la manière suivante :

1. Ouvrez une fenêtre de terminal.
2. Exécutez la commande suivante :

```
sudo dnf remove thegreenbow-vpn-client.x86_64
```

Cette commande supprime les fichiers et les paquets dépendants ajoutés lors de l'installation et qui ne sont plus utilisés. Les fichiers de configuration ajoutés par la suite, p. ex. `config.tgb` ne sont pas supprimés.



Le Client VPN Linux a été désinstallé.

7.2 Sous Ubuntu

Pour désinstaller le Client VPN Linux sous Ubuntu, procédez de la manière suivante :

1. Ouvrez une fenêtre de terminal (Ctrl + Alt + T).
2. Exécutez l'une des commandes suivantes :

```
sudo apt remove thegreenbow-vpn-client
```

Ou :

```
sudo apt purge thegreenbow-vpn-client
```

Cette commande supprime les fichiers ajoutés lors de l'installation, ainsi que les fichiers de configuration ajoutés par la suite, p. ex. `config.tgb`, si celui-ci a été modifié. Les autres paquets dépendants ajoutés lors de l'installation ne sont pas supprimés.

La différence entre la commande `remove` et la commande `purge` est qu'avec cette dernière on délègue au système la tâche de suppression de tous les éléments existants.

3. Le cas échéant, exécutez la commande suivante :

```
sudo apt autoremove
```

Cette commande supprime les paquets ajoutés lors de l'installation, et qui ne sont plus utilisés.

Le Client VPN Linux a été désinstallé.

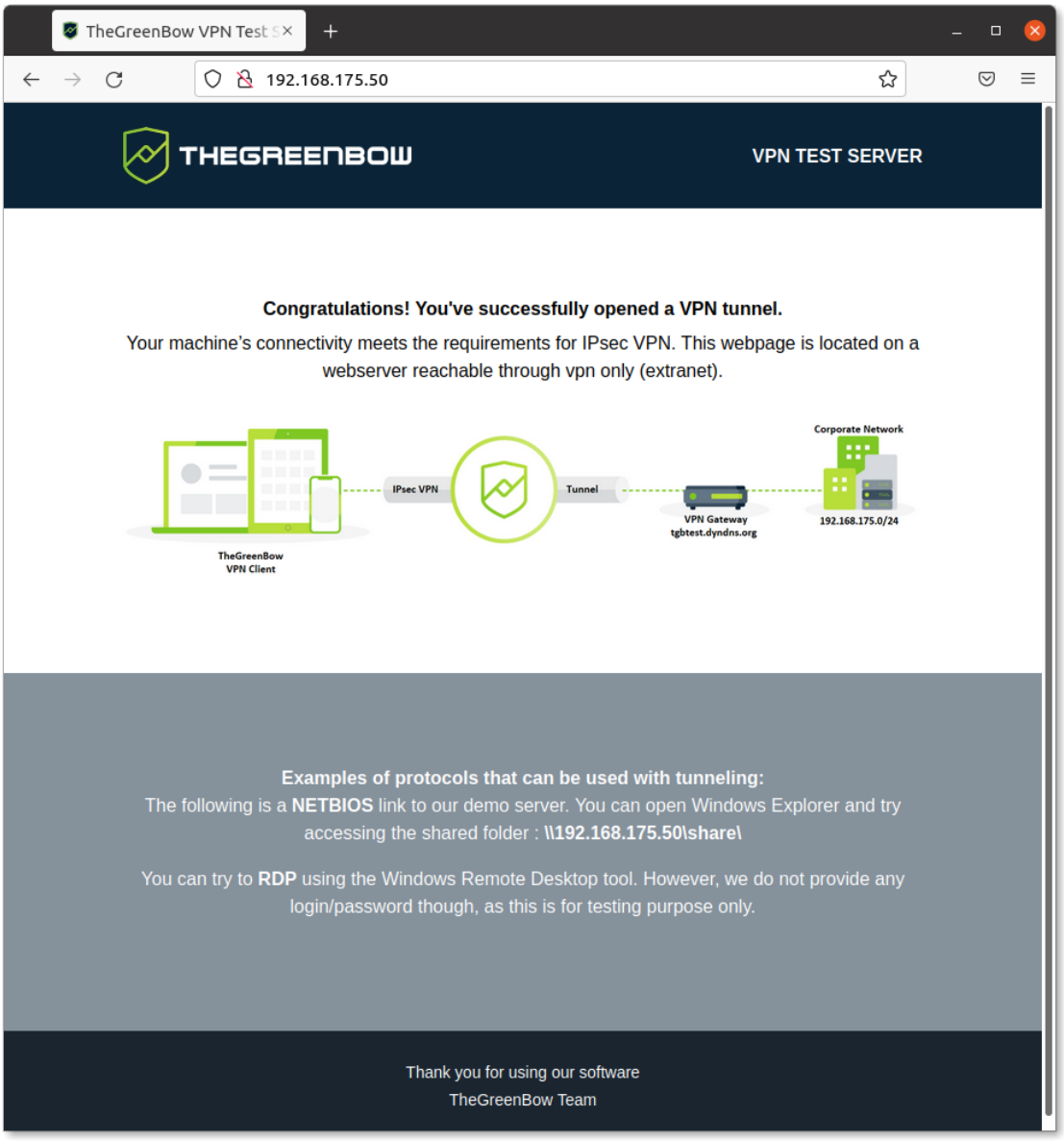
8 Utilisation du tunnel de test

Une configuration VPN contenant un tunnel VPN de test appelé « TgbTest » est fournie dans le fichier `conf.tgb` qui se trouve dans le répertoire `/etc/tgb/`.

Elle est importée par défaut et vous permet de tester le Client VPN Linux en vous connectant à une passerelle de test.

Cette configuration de test peut être utilisée pour vérifier que le Client VPN Linux est opérationnel.

Une fois le tunnel ouvert, vous devriez pouvoir envoyer une requête ping à l'adresse IP 192.168.175.50 ou visiter la page Web http://192.168.175.50/ dans votre navigateur Web.



9 Ligne de commande

9.1 Introduction

Le Client VPN Linux propose une interface en ligne de commande permettant de réaliser les opérations suivantes :

- Afficher l'aide
- Afficher la version du logiciel
- Afficher le nombre de jours restant avant l'expiration de la licence ou de la période d'évaluation
- Lister les connexions VPN configurées
- Ouvrir une connexion VPN
- Fermer une connexion VPN
- Afficher l'état de la connexion VPN

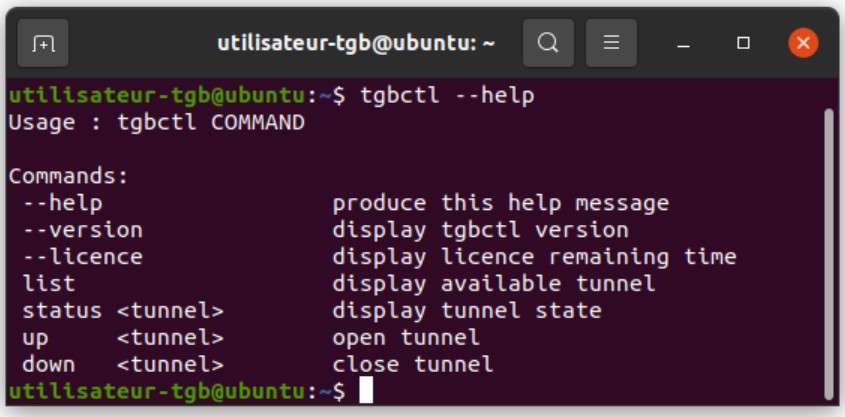
Lorsque vous utilisez le Client VPN Linux sans licence, le nombre de jours restants avant l'expiration de la période d'évaluation s'affiche chaque fois que vous lancez une commande `tgbctl`.

Les commandes de pilotage du Client VPN Linux sont identiques quelle que soit la distribution Linux utilisée.

9.2 Afficher l'aide

Pour afficher l'aide, ouvrez une fenêtre de terminal et exécutez la commande suivante :

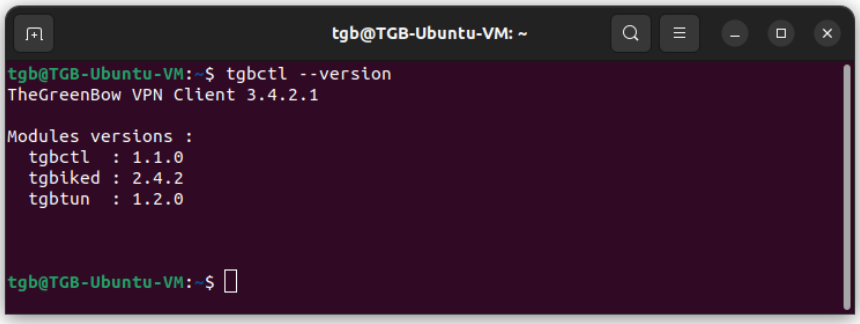
```
tgbctl --help
```



9.3 Afficher la version du logiciel

Pour afficher la version du logiciel et des modules, ouvrez une fenêtre de terminal et exécutez la commande suivante :

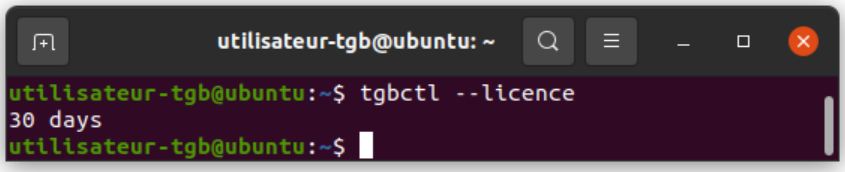
```
tgbctl --version
```



9.4 Afficher le nombre de jours restant avant l'expiration de la licence ou de la période d'évaluation

Pour afficher le nombre de jours restant avant l'expiration de la licence ou du de la période d'évaluation, ouvrez une fenêtre de terminal et exécutez la commande suivante :

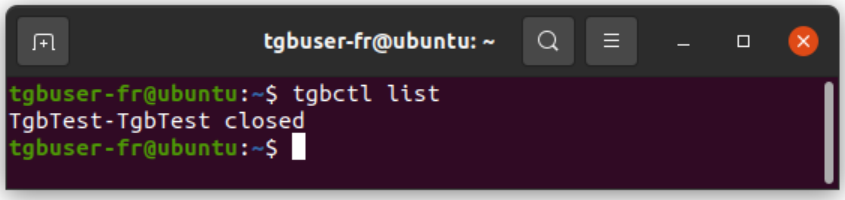
```
tgbctl --licence
```



9.5 Lister les connexions VPN configurées

Pour lister les connexions VPN configurés, ouvrez une fenêtre de terminal et exécutez la commande suivante :

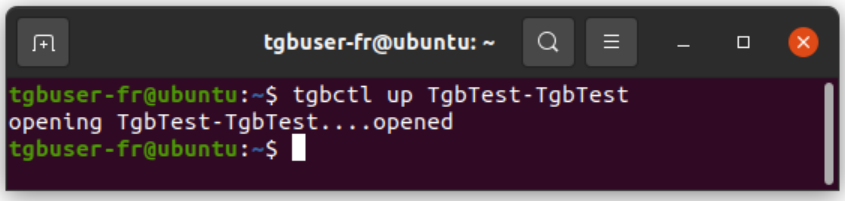
```
tgbctl list
```



9.6 Ouvrir une connexion VPN

Pour ouvrir une connexion VPN, ouvrez une fenêtre de terminal et exécutez la commande suivante :

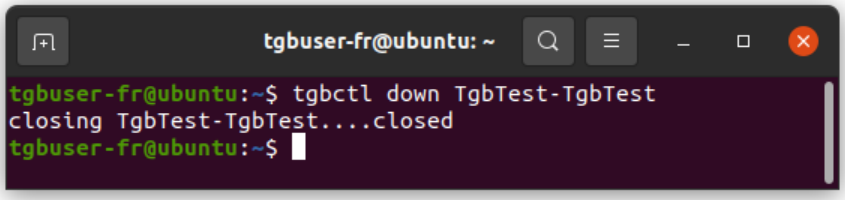
```
tgbctl up [nom_connexion]
```



9.7 Fermer une connexion VPN

Pour fermer une connexion VPN, ouvrez une fenêtre de terminal et exécutez la commande suivante :

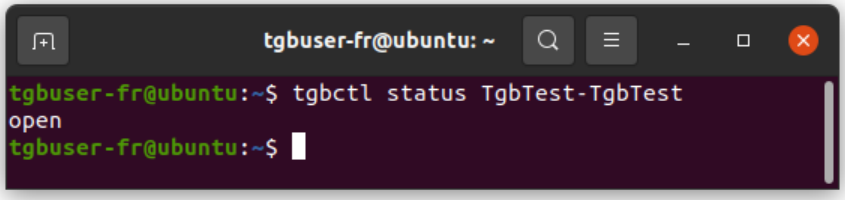
```
tgbctl down [nom_connexion]
```



9.8 Afficher l'état de la connexion VPN

Pour afficher l'état de la connexion VPN, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
tgbctl status [nom_connexion]
```



9.9 Définir un code PIN

Pour automatiser l'ouverture d'un tunnel, l'argument `--pincode` permet de renseigner le code PIN d'une carte à puce directement en ligne de commande :

```
tgbctl up [nom_tunnel] --pincode [code_PIN]
```

9.10 Réinitialiser l'icône tgbtray

Pour réinitialiser l'icône **tgbtray** du menu système, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
tgbtray reset
```

Lancez cette commande lorsque vous souhaitez forcer le rechargement de l'icône du menu système.

Tout utilisateur peut lancer cette commande sans avoir besoin des droits d'administration.

9.11 Réinitialiser le démon IKE

Pour réinitialiser le démon IKE, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
tgbctl reset
```

Lancez cette commande lorsque le tunnel tombe et que vous n'arrivez pas à le relancer.

Tout utilisateur peut lancer cette commande sans avoir besoin des droits d'administration.

10 Configuration des connexions VPN

10.1 Introduction

Les clients VPN TheGreenBow s'appuient sur une configuration VPN qui définit la liste des connexions VPN mises à disposition par l'administrateur pour l'utilisateur du poste. Ce fichier s'appelle aussi fichier de configuration et son extension est `.conf`.

Le Client VPN Linux ne propose pas d'IHM permettant de fabriquer ou modifier la configuration VPN.

Cette fonctionnalité est assurée par le Client VPN Windows Enterprise.

☞ Voir le Guide de déploiement du Client VPN Windows Enterprise (cf. chapitre 17 Documents connexes à consulter).

Si vous êtes administrateur, vous devez utiliser le Client VPN Windows Enterprise pour générer une configuration VPN comme indiqué dans la section 10.4 Mise à jour de la configuration VPN.

10.2 Protection de la configuration VPN

Le Client VPN Linux s'appuie sur le système d'exploitation Linux pour protéger la configuration. Le fichier de configuration est uniquement accessible aux utilisateurs bénéficiant des privilèges de super-administrateur.

Aucun autre utilisateur ne peut modifier le fichier de configuration ou en injecter un nouveau, ce qui en garantit l'authenticité et l'intégrité.

Le fichier de configuration VPN est stocké dans le fichier `conf.tgb` sous le répertoire `/etc/tgb/`.

Les droits sur ce fichier sont `-rw-------, owner root`. Un utilisateur standard ne peut donc pas accéder à la configuration VPN que ce soit en lecture ou en écriture.

10.3 Gestion des certificats

Le Client VPN Linux offre un ensemble de fonctions permettant l'exploitation de certificats de toute nature, issus de PKI / IGC de tout type et stockés sur différents types de supports : carte à puce, token ou fichier de configuration.

Le Client VPN Linux implémente en particulier les facilités suivantes :

- accès aux cartes à puce et aux tokens en PKCS#11 ;
- sélection multicritère des certificats à utiliser en fonction du sujet et du key usage ;
- validation des certificats côté utilisateur (côté client VPN), comme des certificats de la passerelle VPN, incluant la vérification des dates de validité, des chaînes de certification, des certificats racines et intermédiaires ;
- gestion des autorités de certification (Certificate Authority : CA).

La configuration et la caractérisation des certificats s'effectue dans le Client VPN Windows Enterprise.

☞ Consultez le Guide de l'administrateur correspondant (cf. chapitre 17 Documents connexes à consulter).

Pour utiliser un certificat, procédez comme suit :

1. Dans le Client VPN Windows Enterprise, importez le certificat utilisateur et les CA associés dans votre configuration (cf. « Guide de l'administrateur » du Client VPN Windows Enterprise).
2. Suivez la procédure de mise à jour de la configuration décrite à la section 10.4 Mise à jour de la configuration VPN ci-dessous.

Le certificat a été importé dans la configuration du Client VPN Linux.

10.4 Mise à jour de la configuration VPN

Afin de modifier la configuration de votre Client VPN Linux, procédez de la manière suivante :

1. Générez la configuration à l'aide du Client VPN Windows Enterprise.
2. Exportez la configuration au format TGB, sans la protéger par mot de passe, sous le nom `conf.tgb`.
3. Remplacez le fichier `conf.tgb` dans le répertoire `/etc/tgb/` sur la machine sur laquelle vous souhaitez importer la configuration.
4. Exécutez la commande suivante pour redémarrer le service :

```
sudo systemctl restart tgbiked.service
```

La configuration VPN a été mise à jour dans le Client VPN Linux.

La réinitialisation par une commande `tgbctl reset` ou `tgbtray reset` ne permet pas de charger la configuration après sa mise à jour.

11 Utilisation de tokens et cartes à puce

11.1 Introduction

Le Client VPN Linux permet désormais une authentification par token ou carte à puce. Pour cela, il convient de :

- le cas échéant, configurer la machine virtuelle ;
- installer le middleware du fabricant du token ou de la carte à puce, ou un middleware compatible ;
- générer le fichier `vpnconf.ini` qui permet au client VPN d'utiliser le token ou la carte à puce.

Un grand nombre de tokens et de cartes à puce permettant une authentification forte multi-facteurs (MFA) est pris en charge par le Client VPN Linux via l' API PKCS#11.

PKCS#11 est une API d'accès aux tokens ou aux cartes à puce standardisée par RSA Labs. La plupart des tokens ou cartes à puce sont compatibles PKCS#11. L'utilisation de l'API PKCS#11 par le Client VPN Linux requiert l'installation préalable sur le poste cible d'un middleware fourni par le fabricant du token ou de la carte à puce.

Les tokens et cartes à puce compatibles avec le Client VPN Linux sont ceux qui sont listés sur le site TheGreenBow à l'adresse https://thegreenbow.com/fr/support/guides-dintegration/tokens-vpn-compatibles/ et pour lesquels l'élément PKC est précédé d'un point vert et suivi de la mention « Testé et qualifié ».

En principe, tout token ou carte à puce pour lequel il existe un middleware PKCS#11 peut être utilisé avec le Client VPN Linux.

Pour pouvoir utiliser les tokens ou cartes à puce avec le Client VPN Linux, il convient de spécifier leurs caractéristiques dans un fichier d'initialisation PKCS#11 appelé `vpnconf.ini`, décrit ci-après.

11.2 Fichier vpnconf.ini

Pour permettre au Client VPN Linux de prendre en charge des tokens ou cartes à puces non reconnus en standard, un fichier `vpnconf.ini` doit être crée dans le répertoire d'installation du Client VPN (par défaut : `/etc/tgb/`). Il peut être établi avec un éditeur texte classique (p. ex. nano).

Les paramètres à indiquer dans le fichier `vpnconf.ini` sont répartis dans une succession de sections `ATR` qui permettent de définir les attributs de tokens ou cartes à puce qui ne sont pas reconnus en standard par le logiciel.

ATR signifie « Answer To Reset ». C'est un identifiant retourné par le token ou la carte à puce sur commande de réinitialisation. Cet identifiant est lié au fabricant et au modèle de token ou de carte à puce.

Chaque section ATR décrit les caractéristiques nécessaires pour accéder à un token ou une carte à puce, ou à une famille de tokens ou de cartes à puce qui ne sont pas encore connues du logiciel.

Les paramètres à indiquer dans la section ATR sont détaillés dans la table suivante :

Paramètre	Signification
`[ATR#]`	ATR du token ou de la carte à puce à ajouter
`mask`	Masque à utiliser avec cet ATR[1]
`scname`	Nom du token ou de la carte à puce (champ purement descriptif)
`manufacturer`	Nom du constructeur (champ purement descriptif)
`pkcs11dllname`	Nom de la librairie partagée PKCS#11 (champ purement descriptif)
`dllpath`	Chemin d'accès à la librairie partagée PKCS#11. Le chemin est le chemin complet. Il doit contenir aussi le nom de la librairie partagée.[2]

Il convient de procéder avec précaution en renseignant le chemin d'accès à la librairie partagée PKCS#11 dans la paramètre `dllpath`. Si le chemin renseigné n'est pas correct, cela peut provoquer un comportement indésirable du logiciel.

Pour récupérer des informations sur un token connecté à la station de travail, il est possible d'utiliser la commande `pcsc_scan` (accessible via le package pcsc-tools).

[1] Les informations relatives aux ATR et aux masques des ATR sont fournies par les fabricants de tokens ou de cartes à puce. En cas de doute, un masque ne contenant que FF peut être configuré. Les longueurs de l'ATR et du masque doivent être identiques. La ligne `mask` peut ainsi prendre la forme suivante : `mask=FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF`

[2] Le paramètre `dllpath` doit obligatoirement être défini.

Exemple

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Nom de la carte"
manufacturer="Nom de la société"
pkcs11dllname="mdlw.so"
dllpath="/usr/lib/mdlw.so"
```

11.3 Installation du middleware

Consultez la documentation de l'éditeur du middleware pour les instructions d'installation.

Exemple de OpenSC sous Ubuntu

OpenSC est un middleware ouvert (*open source*) qui prend en charge différents tokens et cartes à puce.

Pour installer le middleware OpenSC sous Ubuntu, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal (Ctrl + Alt + T).
2. Exécutez successivement les commandes suivantes :

```
sudo apt-get update -y
sudo apt-get install -y opensc
sudo apt-get install -y opensc-pkcs11
```

Une fois le middleware OpenSC installé, vous devez définir le paramètre `pin_cache_ignore_user_consent` sur `true` dans le fichier `opensc.conf`.

Exemple pour `/etc/opensc.conf` :

```
app default {
     # debug = 3;
     # debug_file = opensc-debug.txt;
        framework pkcs15 {
                pin_cache_ignore_user_consent = true;
        }
}
```

Vous pouvez ensuite procéder à la création du fichier `vpnconf.ini`.

11.4 Création du fichier vpnconf.ini

Pour pouvoir utiliser le Client VPN Linux avec un token ou une carte à puce, vous devez :

- créer le fichier `vpnconf.ini` à l'aide d'un traitement de texte,
- y ajouter les informations relatives au token ou à la carte à puce et
- le déposer dans le répertoire `/etc/tgb/`.

Exemple pour le token Yubikey 5 NFC

Les informations à renseigner dans le fichier `vpnconf.ini` pour un token Yubikey 5 NFC sont les suivantes :

```
[3B:FD:13:00:00:81:31:FE:15:80:73:C0:21:C0:57:59:75:62:69:4B:65:79:4
0]
mask="FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF
:FF:FF"
scname="Yubikey 5 NFC
manufacturer="Yubico"
pkcs11DllName="yubikey"
dllpath="/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so"
```

Vous pouvez désormais utiliser le token Yubikey 5 NFC comme moyen d'authentification avec le Client VPN Linux.

12 Journaux

12.1 Introduction

Les journaux du daemon IKE sont stockés à l'aide de la gestion des journaux `systemd`.

Pour accéder aux journaux du daemon IKE, exécutez la commande suivante dans une fenêtre de terminal :

```
journalctl -t tgbiked
```

12.2 Export au format texte

Pour exporter le contenu du journal au format texte, exécutez la commande suivante dans une fenêtre de terminal :

```
journalctl -t tgbiked > [mon_fichier_de_log.log]
```

Ce fichier sert de base pour le support client.

Dans le cas où il vous est demandé, afin que l'équipe support dispose de l'ensemble des informations dont elle a besoin, il convient également de lui communiquer les éléments suivants :

- version du paquet binaire utilisé,
- version de la distribution Linux,
- version du noyau Linux (*kernel*),
- version de la bibliothèque GNU C (glibc).

Pour obtenir les informations concernant la distribution et le noyau, exécutez la commande suivante dans une fenêtre de terminal :

```
uname -a
```

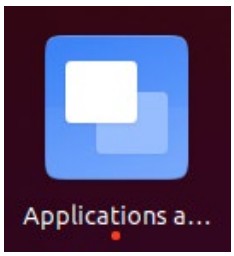
Pour obtenir les informations concernant la bibliothèque `glibc`, exécutez la commande suivante dans une fenêtre de terminal :

```
ldd --version
```

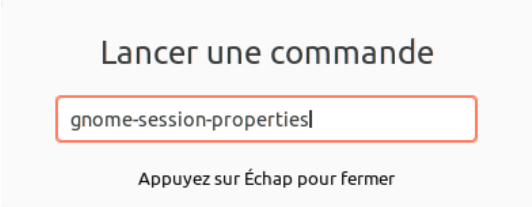
13 Lancement automatique

Sous Ubuntu, le Client VPN Linux permet de lancer automatiquement l'application au démarrage du système. Pour cela, vous pouvez utiliser le **gestionnaire de démarrage** en suivant les étapes ci-dessous :

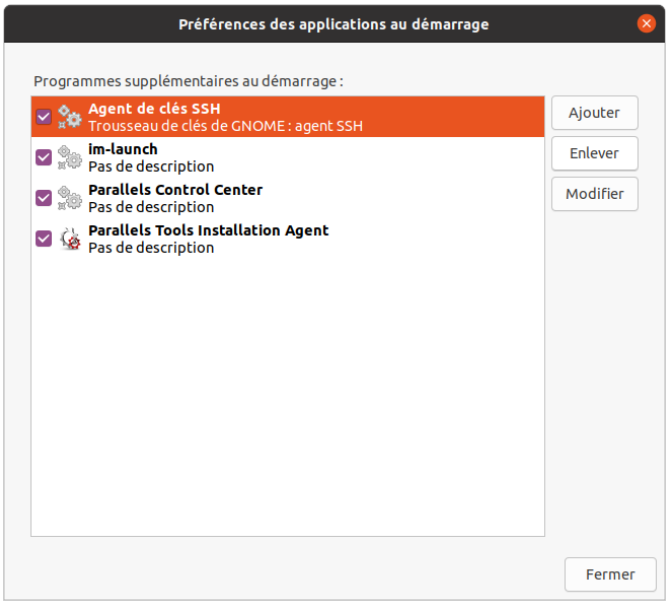
1. Ouvrez la liste des applications en cliquant sur le bouton **Afficher les applications** dans le coin inférieur gauche de votre écran, puis cliquez sur l'icône des **Applications au démarrage**.



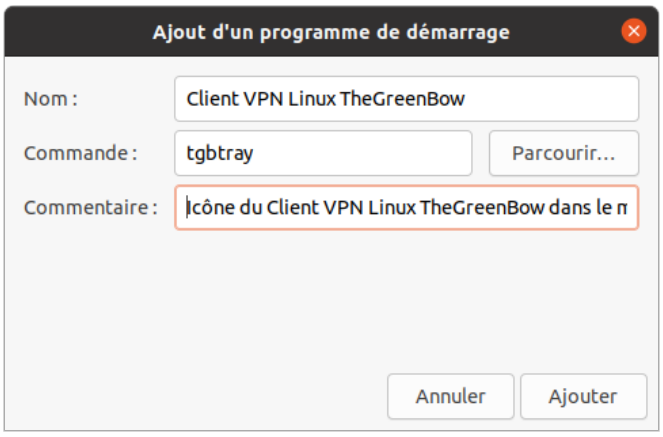
Alternative : appuyez sur Alt + F2 pour ouvrir la boîte de dialogue **Lancer une commande**, et exécutez la commande `gnome-session-properties`.



La fenêtre **Préférences des applications au démarrage** s'affiche.



2. Cliquez sur **Ajouter**. La fenêtre **Ajout d'un programme de démarrage** s'affiche.



3. Renseignez un nom, p. ex. Client VPN Linux.
4. Renseignez la commande `tgbtray`.
5. Ajoutez un commentaire, p. ex. icône du Client VPN Linux dans le menu système.
6. Cliquez sur **Ajouter**.

La prochaine fois que vous ouvrez une session, le Client VPN Linux se lance automatiquement et son icône s'affiche dans le menu système.

14 Sélection du noyau

Dans les versions 3.4.1 et antérieures du Client VPN Linux, le pilote `tgbtun` était lancé automatiquement au démarrage du système. Afin de prévenir le démarrage du pilote avec une version de noyau non compatible et un éventuel blocage du système, à partir de la version 3.4.4 du Client VPN Linux, le pilote est démarré avant le démarrage du service `tgbiked` et après contrôle de la version du noyau.

En vue d'anticiper une mise à jour du poste utilisateur avec un noyau qui n'est pas compatible avec la version du Client VPN Linux installée, vous pouvez définir le noyau souhaité dans le fichier `/etc/tgb/tgbtun.params`. Cela permettra notamment d'empêcher le démarrage du service sous Ubuntu 22.04 avec un noyau 6.x.

Le fichier `/etc/tgb/tgbtun.params` doit contenir une seule ligne commençant par `requires` suivi d'un numéro de noyau sous la forme d'une expression régulière, par exemple :

```
requires=5.14.*.el9_4.x86_64
```

15 Limitations actuelles

La version actuelle du Client VPN Linux comporte les limitations suivantes :

- Il n'est pas possible d'importer une configuration chiffrée.
- Une seule connexion VPN peut être ouverte à la fois.

16 Gestion des erreurs

16.1 L'utilisateur doit appartenir au groupe « tgb »

Si vous n'avez pas ajouté l'utilisateur courant au groupe d'utilisateurs `tgb`, le message d'erreur suivant s'affiche lorsque vous exécutez des commandes :

```
ERROR: User must belong to "tgb" group
```

Pour ajouter l'utilisateur au groupe `tgb`, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
sudo usermod -aG tgb $(whoami)
```

Il est nécessaire de fermer/rouvrir la session, voire redémarrer le système, pour que cette commande soit prise en compte par Ubuntu. Nous vous recommandons de faire un redémarrage du système dans tous les cas.

16.2 Impossible de récupérer la liste des connexions VPN

Lorsque vous exécutez la commande `tgbctl up [nom_connexion]`, l'erreur suivante peut s'afficher :

```
Error: Can't get tunnel list, check if tgbiked service
is started can't be open: check status
```

Pour vérifier que l'utilisateur a bien été ajouté au groupe `tgb`, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
id
```

Si le groupe `tgb` ne figure pas dans la liste, redémarrez la machine pour que l'ajout soit pris en compte.

16.3 Échec d'ouverture de la connexion VPN

Lorsque le Client VPN Linux n'arrive pas à ouvrir une connexion VPN, le message d'erreur suivant s'affiche :

```
Opening [nom_connexion] ..... failed
```

Lorsque l'ouverture de la connexion VPN a échoué, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
journalctl -r -t tgbiked
```

Vous pouvez analyser le journal vous-même (voir chapitre 12 Journaux) ou contacter l'équipe support : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

16.4 Les utilisateurs standard ne doivent pas avoir accès au fichier de configuration

Lorsque le Client VPN Linux n'arrive pas à ouvrir une connexion VPN après avoir remplacé le fichier `/etc/tgb/conf.tgb` par une nouvelle configuration, consultez le journal pour voir s'il contient le message suivant : « Non-root users must not be able have access to file /etc/tgb/conf.tgb ». En effet, le fichier de configuration ne doit pas être accessible en lecture aux utilisateurs autres que les super-utilisateurs (*root*).

Si c'est le cas, exécutez la commande suivante :

```
sudo chmod 600 /etc/tgb/conf.tgb
```

16.5 Vérification du pilote

Pour vérifier que le pilote (ou *driver*) est chargé, exécutez la commande suivante :

```
lsmod | grep tgb
```

La commande doit retourner le message suivant :

```
tgbtun        [identifiant] 0
```

Si ce n'est pas le cas, suivez les étapes ci-dessous :

1. Vérifiez que le driver `tgbtun.ko.xz` est présent dans :
   - `/lib/modules/`uname -r`/extra/`[1] pour Red Hat ;
   - `/lib/modules/`uname -r`/updates/dkms`[2] pour Ubuntu.
2. Vérifiez que le répertoire `/usr/src/tgbtun-1.2` est présent.

[1] Sur certains systèmes, il est préférable de spécifier `/usr/lib/modules`.
[2] idem

3. Si le driver n'est pas installé, reportez-vous à la section suivante pour l'installer.

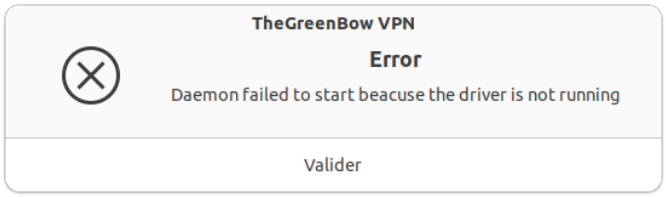
Si le problème persiste, contactez l'équipe support en fournissant le résultat des commandes suivantes :

- `modinfo tgbtun`
- `dkms status tgbtun`

Pour contacter l'équipe support, veuillez utiliser le formulaire suivant : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

16.6 Impossible de démarrer le démon IKE

Si après avoir installé le programme le logiciel retourne l'erreur suivante :



Vous pouvez vérifier le fonctionnement du pilote et, le cas échéant, l'installer manuellement en suivant les étapes ci-dessous :

1. Vérifiez le pilote comme décrit à la section 16.5 Vérification du pilote.
2. Si la commande ne retourne rien, exécutez les commandes suivantes successivement pour installer le pilote :

```
cd /usr/src/tgbtun-1.2
sudo dkms install tgbtun/1.2
```

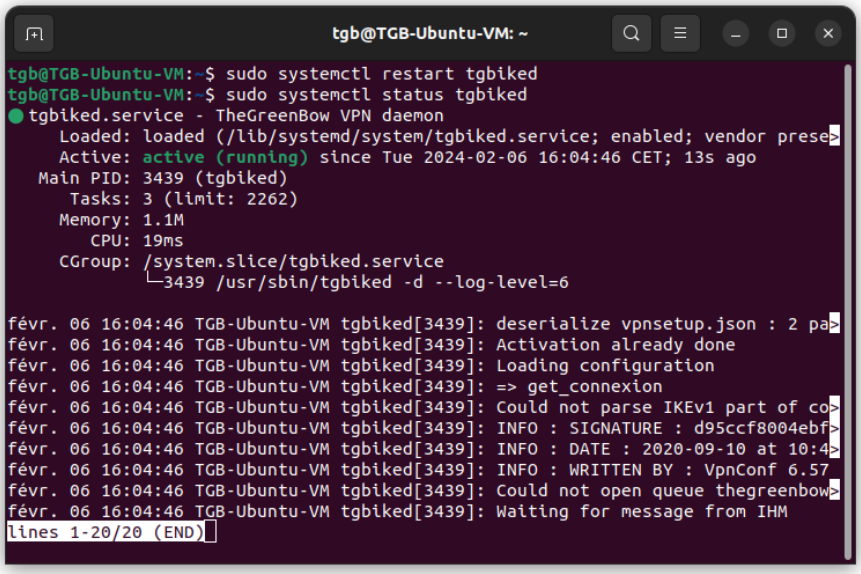
3. Sous Ubuntu, exécutez la commande suivante, sous RedHat passez à l'étape suivante :

```
sudo insmod /lib/modules/`uname -
r`/updates/dkms/tgbtun.ko
```

4. Exécutez ensuite successivement les commandes suivantes pour redémarrer le démon IKE et afficher son état :

```
sudo systemctl restart tgbiked
sudo systemctl status tgbiked
```

Vous devriez recevoir en retour des informations similaires à ce qui est indiqué ci-dessous :



Vous pouvez alors poursuivre l'installation en ajoutant l'icône **tgbtray** au menu système (cf. chapitre 5 Icône tgbtray dans le menu système), puis ouvrir un tunnel de test (cf. chapitre 8 Utilisation du tunnel de test).

Si vous n'arrivez toujours pas à démarrer le démon IKE, veuillez contacter l'équipe support pour comprendre ce qui s'est passé : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

16.7 Blocage du daemon IKE

Si jamais le daemon IKE ne répond pas, ce qui peut arriver après un changement d'interface réseau, ou après avoir débranché et rebranché le câble réseau, lancez la commande suivante pour le redémarrer :

```
sudo kill -9 $(pidof tgbiked)
```

16.8 Erreurs token ou carte à puce

Lorsque l'utilisateur saisit un mauvais code PIN, l'IHM utilisée pour demander l'ouverture de la connexion VPN l'informe que le code PIN fourni n'est pas valide.

Lorsque l'utilisateur verrouille le token ou la carte à puce en entrant plusieurs fois un code PIN incorrect, l'IHM informe l'utilisateur que le token ou la carte à puce est verrouillé.

Par ailleurs, le Client VPN Linux peut retourner les erreurs suivantes en lien avec l'utilisation de tokens et de cartes à puce :

- `no smartcard plugged` : le token ou la carte à puce n'est pas connectée
- `wrong pin code` : le code PIN entré par l'utilisateur est incorrect
- `smartcard is locked` : le token ou la carte à puce est verrouillée

16.9 Token ou carte à puce non reconnu par la machine virtuelle

Si le système d'exploitation est exécuté dans une machine virtuelle VMware, il convient de suivre au préalable la procédure ci-dessous :

1. Arrêtez la machine virtuelle.
2. Localisez le fichier de configuration `*.vmx` de la machine virtuelle (cf. article VMware à ce sujet, non disponible en français).
3. Ouvrez le fichier de configuration dans un traitement de texte.
4. Ajoutez les deux lignes suivantes au fichier et l'enregistrer :

```
usb.generic.allowHID = "TRUE"
usb.generic.allowLastHID = "TRUE"
```

La machine virtuelle est désormais prête pour l'utilisation du token ou de la carte à puce. Vous pouvez procéder à l'installation du middleware.

Si vous utilisez un autre logiciel de virtualisation, le principe reste le même : il convient de s'assurer que la machine virtuelle puisse accéder au token ou la carte à puce par USB.

17 Documents connexes à consulter

Pour savoir comment générer le fichier de configuration à utiliser avec le Client VPN Linux, nous vous invitons à consulter le « Guide de l'administrateur » du Client VPN Windows Enterprise. Vous le trouverez sur le site de TheGreenBow sous la rubrique Documentations produits.

Retrouvez la liste des pare-feux/passerelles VPN compatibles et les guides de configuration correspondants sur le site TheGreenBow : https://www.thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

Vous pouvez télécharger une configuration de démonstration et ouvrir un tunnel de test en suivant les indications sur le site TheGreenBow : https://www.thegreenbow.com/fr/faq/#deeplink-2226.

Vous trouverez plus d'informations sur les produits TheGreenBow sur notre site internet : https://thegreenbow.com/.

18 Licence OpenSSL

OpenSSL est distribué sous la licence Apache 2.0 reproduite ci-dessous.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A

PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

19 Contact

19.1 Information

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

19.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

19.3 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