Connection Management Center 1.3

Guide de l'administrateur

Dernière mise à jour : 7 avril 2025
Référence du document : 20250407_AG_CMC_1.3_FR_1.0

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2025-04-07	Toutes	Version initiale	FBO, VMA, BB

1 Présentation

1.1 Introduction

Ce guide est destiné aux utilisateurs du Connection Management Center (CMC) pour l'administration des clients VPN.

Il suppose que le logiciel est déjà installé et s'utilise conjointement avec le « Guide de référence » du CMC. En effet, après la définition de quelques notions fondamentales (chapitre 2) et une présentation succincte de l'interface destinée à en faciliter la prise en main (chapitre 0), ce guide décrit les principales procédures d'administration du CMC (chapitre 4), de gestion des configurations VPN (chapitre 5), de gestion des licences (chapitre 6) et de supervision (chapitre 7).

Le « Guide de référence » du CMC, quant à lui, décrit en détail chaque champ sur les différents onglets et pages de la gestion des configurations VPN et apporte des informations complémentaires relatives à la gestion des certificats, la gestion des paramètres dynamiques, la gestion **du Panneau TrustedConnect** du Client VPN Windows Enterprise, les options d'automatisation et le choix IPv4/IPv6. Il présente en outre des recommandations de sécurité, l'architecture sécurisée du CMC et des notions élémentaires de cryptographie.

1.2 Nouveautés de la version 1.3

1.2.1 Compatibilité RedHat 9

Le CMC peut désormais être installé sur une machine fonctionnant sous le système d'exploitation RedHat 9.4 et 9.5.

1.2.2 Mode IPsec DR

Une option spécifique à activer lors de la création d'un tunnel, permet de restreindre les paramètres possibles pour ce tunnel à un sous-ensemble compatible avec le référentiel IPsec DR.

1.2.3 Compatibilité avec le Client VPN Quantum Safe 1.0

Le CMC permet désormais de créer des configurations VPN fondées sur une cryptographie résistante au quantique destinées à être utilisées avec le Client VPN Quantum Safe. La cryptographie post-quantique (*post-quantum cryptography* ou PQC en anglais) représente la solution la plus prometteuse

pour se prémunir contre la menace que constituent les ordinateurs quantiques capables de casser la cryptographie actuelle et ainsi de compromettre les données sensibles (*cryptographically relevant quantum computers* ou CRQC en anglais).

Le CMC est en mesure d'adopter une approche hybride, qui consiste à conserver la cryptographie actuelle dans l'échange de clés tout en ajoutant une protection supplémentaire par des algorithmes post-quantiques.

1.2.4 Personnalisation des ports

Le CMC peut désormais être installé avec un port dédié pour les flux suivants :

- Service d'activation de licences
- Remontée de logs provenant du parc de Clients VPN TheGreenBow, désormais obligatoirement chiffrée en authentification mutuelle mTLS

1.2.5 Authentification multiple

Le CMC permet désormais de mettre en place une authentification multiple avec plusieurs certificats, conformément à la RFC 4739.

L'authentification multiple par certificat plus EAP reste possible et il est en outre possible de configurer une authentification impliquant plusieurs certificats. Dans ce cas, la liste des authentifications par certificat peut être ordonnée.

1.2.6 Interface

Le parcours de création de tunnels a été repensé pour prendre en compte les évolutions du CMC. La sélection de la version du client VPN et éventuellement l'activation du mode DR sont opérées avant tout autre choix de configuration.

Les éléments d'authentification des tunnels IPsec/IKEv2 ont été regroupés sur un même onglet pour une meilleure vue d'ensemble.

1.3 Principales fonctionnalités et avantages du CMC

Pensé pour les administrateurs IT et les RSSI, le Connection Management Center (CMC ou Centre de gestion des connexions) est une console qui offre des services apportant la maîtrise, le contrôle et la visibilité nécessaires pour protéger efficacement les accès distants au SI.

Le CMC est un logiciel serveur qui réalise les cinq principales fonctionnalités suivantes :

- gestion centralisée des configurations VPN à déployer en fonction des différentes versions des Clients VPN du parc ;
- gestion et déploiement aisés de l'activation des Clients VPN TheGreenBow par l'intégration d'un service d'activation ;
- centralisation des traces d'audit provenant de l'ensemble du parc de Clients VPN TheGreenBow ;
- gestion des utilisateurs du CMC ;
- visualisation de la santé du système pour un suivi avancé.

Pour réaliser ces fonctionnalités, le CMC communique avec les Clients VPN TheGreenBow soit directement, soit via un agent appelé Secure Connection Agent.

1.4 Recommandations ANSSI relatives au principe d'installation dans un milieu sécurisé

Voici quelques recommandations générales concernant le principe d'installation dans un milieu sécurisé basées sur les principes de sécurité informatique promus par l'ANSSI.

Ces recommandations peuvent évoluer, il est donc conseillé de consulter directement les documents officiels de l'ANSSI pour les informations les plus à jour.

- Environnement physique sécurisé : l'installation de systèmes d'information doit se faire dans un environnement physique sécurisé pour protéger l'équipement contre les accès non autorisés, les dommages physiques et les interférences du milieu ambiant.
- Contrôle d'accès : mettre en place des mécanismes de contrôle d'accès pour limiter l'accès aux équipements et aux données aux seules personnes autorisées. Cela inclut la gestion des identités et des habilitations, ainsi que la mise en œuvre de moyens d'authentification forte.
- Séparation des environnements : isoler les environnements de production des environnements de test et de développement pour réduire les risques de propagation des incidents de sécurité et d'exposition des données sensibles.
- Chiffrement des données : utiliser des techniques de chiffrement pour protéger les données stockées et transmises, en particulier lorsque celles-ci traversent des environnements moins sécurisés ou des réseaux publics.
- Surveillance et journalisation : mettre en place des systèmes de surveillance et de journalisation pour détecter et enregistrer les

activités suspectes ou malveillantes. Cela permet une réaction rapide en cas d'incident de sécurité.

- Mises à jour et correctifs de sécurité : s'assurer que tous les systèmes et logiciels sont régulièrement mis à jour avec les derniers correctifs de sécurité pour protéger contre les vulnérabilités connues.
- Politiques et procédures : définir et mettre en œuvre des politiques et procédures de sécurité claires pour la gestion des équipements et des données dans l'environnement sécurisé. Cela inclut la formation et la sensibilisation des utilisateurs aux bonnes pratiques de sécurité.

Ces recommandations sont des principes d'ordre général servant de lignes directrices. Pour des conseils spécifiques et détaillés, n'hésitez pas à consulter nos équipes techniques spécialisées.

2 Notions fondamentales

2.1 Introduction

Ce chapitre introduit quelques notions fondamentales destinées à vous aider à mieux comprendre ce qu'est le Connection Management Center (CMC) et comment TheGreenBow utilise certains termes clés du secteur de la cybersécurité.

2.2 Ce que le CMC peut faire pour vous

En tant que Centre de gestion des connexions, le rôle principal du Connection Management Center (CMC) est de gérer les configurations VPN de votre parc VPN. En effet, dès lors que votre parc installé dépasse quelques dizaines de postes, la gestion des configurations VPN peut vite s'avérer complexe.

Outre la gestion centralisée des configurations VPN, le CMC propose également de gérer les licences du parc ainsi que leur activation en intégrant les fonctionnalités d'un service d'activation.

Ces deux fonctionnalités peuvent être associées pour faciliter le déploiement des clients VPN sur un ensemble de postes.

Pour faciliter encore davantage la gestion centralisée du parc, le CMC peut agréger les traces d'audit remontées par les Clients VPN TheGreenBow en vue de leur analyse.

Cette fonctionnalité peut être associée à un contrôle de la santé du poste destiné à restreindre l'accès aux seuls postes conformes aux règles de sécurité ZTNA de l'entreprise.

Enfin, à travers différents rôles et niveaux d'accès, le CMC propose une administration centralisée des utilisateurs et groupes d'utilisateurs du CMC.

2.3 Comment administrer efficacement les postes utilisateurs et les connexions à distance ?

Pour administrer efficacement les postes utilisateurs et les connexions à distance, plusieurs mesures clés doivent être mises en place pour garantir sécurité, performance et facilité de gestion. Voici les principales mesures d'ordre général à considérer :

- Règles de sécurité strictes : définissez des règles de sécurité claires pour les utilisateurs du VPN, incluant des directives sur les mots de passe, l'accès aux ressources, et l'utilisation des accès à distance. Ces règles doivent être communiquées à l'ensemble du personnel.

- Accès basé sur le rôle : limitez l'accès aux ressources de l'entreprise ou de l'organisation en fonction des rôles et des besoins des utilisateurs, en s'assurant que les employés n'ont accès qu'aux informations et aux systèmes nécessaires à leur travail.
- Gestion centralisée des accès : utilisez l'Active Directory (AD) pour centraliser et regrouper les identités afin de simplifier la mise en œuvre de règles d'accès, notamment avec le Mode filtrant du Client VPN Windows Enterprise.
- Mise à jour et maintenance des postes utilisateurs : assurez-vous que tous les postes utilisateurs qui se connectent à vos réseaux disposent d'un système d'exploitation à jour et que la protection par logiciel antivirus et pare-feu est activée.
- Surveillance et audit : suivez les traces d'audit récoltées par le CMC pour détecter toute activité anormale ou malveillante sur le réseau.
- Formation et sensibilisation des utilisateurs : formez les utilisateurs aux bonnes pratiques de sécurité, à la reconnaissance des tentatives de phishing et à la gestion sécurisée des informations.
- Plan de réponse aux incidents : établissez un plan de réponse aux incidents de sécurité pour réagir rapidement en cas de détection d'une activité malveillante ou d'une violation de données.

Par ailleurs, les mesures suivantes sont à prendre en compte du point de vue des clients VPN :

- Authentification forte : utilisez une authentification multi-facteurs (MFA) pour renforcer la sécurité des connexions VPN. Cela peut se traduire par l'association du couple identifiant / mot de passe avec un certificat ou le stockage d'un certificat sur une clé de sécurité matérielle.
- Séparation des réseaux : isolez le trafic VPN dans un réseau séparé ou dans un VLAN dédié pour améliorer la sécurité et simplifier la gestion du réseau.
- Chiffrement des données : outre les données transitant par les Clients VPN TheGreenBow, il convient également de chiffrer et de protéger par mot de passe les fichiers de configuration.

En combinant ces différentes mesures, une entreprise ou une organisation peut s'assurer que son parc de clients VPN est sécurisé, performant et géré efficacement, tout en offrant un accès à distance sécurisé à ses effectifs.

2.4 Qu'est-ce qu'un tunnel, une connexion, une configuration ?

2.4.1 Introduction

Pour vous aider à établir des connexions sécurisées à vos systèmes d'informations, les Clients VPN TheGreenBow utilisent des configurations

comportant des connexions et des tunnels. Afin de mieux comprendre leur fonctionnement, nous vous proposons ci-dessus un bref aperçu des notions qui y sont associées.

2.4.2 Qu'est-ce qu'un tunnel

Chez TheGreenBow, un tunnel sert à définir le niveau protocolaire d'un échange de données, à savoir :

- Le type de protocole utilisé
  - IPsec (IKEv2),
  - OpenVPN (SSL/TLS).
- Le mode d'authentification (intégrité)
  - clé partagée,
  - certificat,
  - couple identifiant/mot de passe (EAP).
- Les paramètres cryptographiques
  - algorithme de chiffrement,
  - algorithme d'intégrité (fonction de hachage),
  - longueur de clé.
- L'emplacement du certificat lorsqu'il est utilisé :
  - magasin de l'OS,
  - token ou carte à puce.

2.4.3 Qu'est-ce qu'une connexion

Une connexion quant à elle regroupe les fonctionnalités du Client VPN, notamment en matière d'automatisation :

- ouverture du tunnel :
  - avant l'ouverture de la session Windows,
  - au démarrage du Client VPN,
  - lorsqu'une clé USB est insérée,
  - sur détection de trafic ;
- maintien de la sécurité de la connexion lors d'un changement d'interface ;
- détection d'un réseau de confiance ;
- détection de portail captif ;
- exécution de scripts :
  - avant ou après l'ouverture du tunnel,
  - avant ou après la fermeture du tunnel.

⚠ Un tunnel peut être utilisé dans plusieurs connexions, mais une connexion ne peut contenir qu'un seul tunnel (voir schéma ci-dessous).

ℹ Le **Panneau TrustedConnect** ne permet d'établir qu'une seule connexion à la fois. Le **Panneau des Connexions** quant à lui permet d'ouvrir plusieurs connexions en même temps. Ce dernier est donc à privilégier quand vous souhaitez établir plusieurs connexions à différents réseaux en même temps.

2.4.4 Qu'est-ce qu'une configuration

Une configuration contient un ensemble de connexions et de tunnels qui permet de répondre aux exigences d'une politique de sécurité définie pour un groupe d'utilisateurs donné. Pour l'utilisateur du Client VPN, il s'agit essentiellement de la liste de connexions qui lui est présentée. Toutefois, le Client VPN peut être configuré de telle sorte que l'utilisateur ne voit qu'une seule connexion et son état.

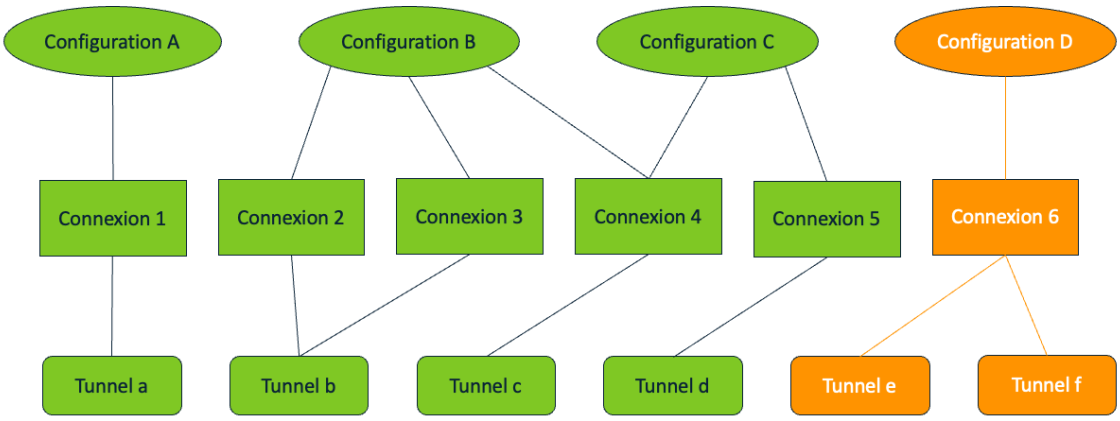
ℹ Lorsqu'un utilisateur ouvre un tunnel, il établit une connexion qui exploite le tunnel associé à la connexion. Les notions de tunnel et de connexion sont synonymes de son point de vue.

La fonctionnalité de Mode filtrant est associée au niveau de la configuration et n'est disponible que si celle-ci contient effectivement une connexion TrustedConnect.

ℹ Une configuration doit contenir au moins une connexion nécessairement constituée d'un seul tunnel.

2.4.5 Configurations possibles

Le schéma ci-dessous représente différentes combinaisons possibles pour constituer une ou plusieurs configurations, ainsi qu'une combinaison impossible (en orange).



La configuration A représente la configuration minimale.

La configuration B illustre une configuration comportant trois connexions dont deux (2 et 3) qui exploitent un même tunnel (b).

La configuration C illustre une configuration qui partage une connexion (4) avec une autre configuration (B).

La configuration D illustre une configuration impossible : une connexion (6) ne peut pas exploiter deux tunnels différents (e et f).

2.5 Qu'est-ce que la santé/conformité du terminal ?

La santé ou la conformité du terminal se rapporte à la mesure dans laquelle un terminal (ou *endpoint* en anglais, soit un ordinateur, un smartphone, une tablette, etc.) répond à une série de critères de sécurité définis par une organisation avant qu'il ne soit autorisé à accéder à ses ressources réseau ou à ses données. Ces critères sont établis pour protéger l'infrastructure informatique de l'entreprise ou de l'organisation contre les vulnérabilités, les logiciels malveillants (ou *malwares* en anglais), et autres risques de sécurité qui pourraient être introduits par des terminaux non conformes ou compromis.

La santé ou la conformité d'un terminal peut comprendre les aspects suivants :

- Mises à jour logicielles : les dernières mises à jour du système d'exploitation et des applications doivent être installées sur le terminal pour s'assurer que toutes les failles de sécurité connues sont corrigées.
- Solutions de sécurité : le terminal doit être équipé de solutions de sécurité à jour, telles que des logiciels antivirus et anti-malware, et des pare-feu personnels.
- Configuration de sécurité : les paramètres de sécurité du terminal doivent être configurés selon les directives de l'organisation pour minimiser la surface d'attaque. Cela peut inclure la désactivation de

services inutiles, la configuration de politiques de mot de passe robustes, et l'activation du chiffrement des données.
- Absence de logiciels malveillants : le terminal ne doit pas être infecté par des logiciels malveillants, des logiciels espions ou tout autre code malveillant qui pourrait compromettre la sécurité des données de l'entreprise.
- Conformité aux politiques de l'entreprise : le terminal doit respecter toutes les politiques de sécurité et d'utilisation acceptable définies par l'entreprise ou l'organisation, y compris les restrictions sur les types d'applications qui peuvent être installées.

Pour évaluer et garantir la conformité des terminaux, les organisations peuvent recourir à des solutions de gestion des appareils mobiles (ou MDM, *Mobile Device Management* an anglais), de gestion unifiée des terminaux (ou UEM, *Unified Endpoint Management* en anglais), ou d'autres outils de sécurité réseau qui permettent d'effectuer des vérifications de conformité en temps réel. Si un terminal n'est pas conforme, l'accès au réseau de l'entreprise peut lui être refusé, ou il peut être placé dans un réseau isolé où il a accès à des ressources limitées jusqu'à ce que les problèmes de conformité soient résolus.

Lorsqu'ils sont associés au Secure Connection Agent (SCA), les Clients VPN TheGreenBow pour Windows peuvent contribuer à assurer la conformité des terminaux. Actuellement, la présence d'un logiciel antivirus à jour et d'un pare-feu est vérifiée avant d'autoriser la demande d'ouverture d'une connexion.

La gestion de la santé et de la conformité des terminaux est une composante essentielle d'une stratégie de sécurité informatique globale, aidant à prévenir les violations de données et à protéger les actifs numériques de l'organisation contre les menaces internes et externes.

2.6 IPsec/IKEv2 ou OpenVPN, quel protocole choisir ?

Lors de la création d'un tunnel dans le CMC, l'un des choix fondamentaux à faire concerne le type de protocole de tunnelisation. Le choix entre IPsec/IKEv2 et OpenVPN dépendra des besoins spécifiques de l'entreprise ou de l'organisation en matière de sécurité, de performance, de compatibilité avec les terminaux et de facilité de configuration.

En effet, si les deux protocoles offrent un niveau de sécurité très élevé, OpenVPN peut être légèrement moins rapide qu'IKEv2, en particulier sur les connexions avec une latence élevée ou une faible bande passante.

En revanche, le protocole IPsec/IKEv2 est à privilégier pour tout usage critique, notamment pour établir des connections VPN avec des passerelles configurées selon le référentiel IPsec DR.

☞ Reportez-vous au « Guide de configuration » *Client VPN et IPsec DR* pour plus de précisions à ce sujet.

2.7 Quel mode d'authentification choisir pour le client ?

2.7.1 Introduction

Le choix entre clé partagée, certificat et EAP dépend des besoins spécifiques en matière de sécurité, de la taille de l'organisation, des ressources disponibles pour la gestion de la sécurité et de la complexité de l'environnement réseau.

Les certificats offrent une sécurité robuste pour les environnements d'entreprise, la clé partagée est plus simple à mettre en œuvre pour les petits réseaux, et EAP offre une flexibilité pour s'adapter à diverses exigences d'authentification dans des environnements complexes.

☞ Reportez-vous au « Guide de référence » du CMC pour plus de précisions sur les recommandations de sécurité.

2.7.2 Clé partagée

La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Elle apporte toutefois moins de souplesse dans la gestion de la sécurité que l'utilisation de certificats. Par exemple elle ne permet la gestion de l'interdiction d'accès à un poste en particulier.

2.7.3 Certificat

L'utilisation de l'option **Certificat** apporte une plus grande sécurité dans la gestion des connexions VPN, car elle s'appuie sur les autorités de contrôle (CA) pour la gestion de la validité des certificats (authentification mutuelle, vérification des durées de vie, révocation, etc.).

Ce mode est recommandé.

2.7.4 EAP

Le mode EAP (protocole d'authentification extensible ou *Extensible Authentication Protocol* en anglais) permet d'authentifier l'utilisateur grâce à un couple identifiant/mot de passe. Lorsque le mode **EAP** est sélectionné, une fenêtre demande à l'utilisateur de saisir son identifiant et son mot de passe à chaque ouverture du tunnel.

Il est alors possible de choisir entre le fait que l'identifiant et le mot de passe EAP soient demandés à chaque ouverture de tunnel (en cochant la case **Popup EAP**), ou qu'ils soient mémorisés dans la configuration VPN en les configurant dans les champs **Identifiant** et **Mot de passe**.

L'enregistrement de l'identifiant et du mot de passe dans la configuration VPN n'est pas recommandé.

2.7.5 Authentification multiple

Outre l'authentification par certificat plus EAP, le CMC permet désormais de configurer une authentification comportant plusieurs certificats pour les Clients VPN Windows Enterprise de version 7.5, conformément à la RFC 4739.

Les combinaisons possibles sont les suivantes :

- clé partagée,
- certificat,
- EAP,
- certificat + EAP,
- certificats multiples.

Si vous configurez une première authentification de type certificat, vous pouvez ajouter d'autres authentifications. Si vous configurez une seconde authentification de type certificat, vous pouvez ajouter des authentifications supplémentaires, mais uniquement de type certificat.

Dans ce cas, vous pouvez ordonner la liste des authentifications par certificat.

2.8 AES CBC, CTR ou GCM, quel mode choisir ?

2.8.1 Introduction

Lors de la création d'une configuration VPN dans le CMC pour les Clients VPN TheGreenBow, vous serez amené à choisir un mode de chiffrement si vous ne souhaitez pas laisser le Client VPN s'adapter automatiquement aux paramètres de la passerelle.

Ci-dessous, vous trouverez quelques éclairages destinés à vous aider dans le choix du mode de chiffrement.

La norme de chiffrement avancée (AES ou *Advanced Encryption Standard* en anglais) est un algorithme de chiffrement symétrique adopté par le National Institute of Standards and Technology (NIST) en 2001 après un processus de sélection rigoureux visant à remplacer son prédécesseur DES devenu obsolète.

L'AES utilise une taille de clé variable (128, 192 ou 256 bits), ce qui en fait un algorithme de choix pour différentes applications de sécurité, notamment la protection des communications sur internet.

Le processus de chiffrement AES consiste à effectuer une série de transformations sur des blocs de données de taille fixe. Ces transformations impliquent des opérations mathématiques, telles que des substitutions et des permutations, qui sont effectuées de manière itérative pour produire des données chiffrées.

L'AES définit différents modes de chiffrement par bloc qui assurent la confidentialité (dont CBC et CTR), mais ceux-ci ne protègent pas contre les modifications accidentelles ou les falsifications malveillantes et doivent donc être associés à une signature numérique. C'est pourquoi il existe également des modes de chiffrement combinés (dont GCM), alliant confidentialité et intégrité des données.

Le choix du mode de chiffrement dépend de plusieurs facteurs, notamment le niveau de sécurité requis, la bande passante disponible, l'interopérabilité entre le Client VPN et la passerelle, ou encore les exigences réglementaires ou normatives.

☞ Pour plus de précisions sur les modes de chiffrement par bloc, reportez-vous aux ressources du NIST disponibles à l'adresse suivante : https://csrc.nist.gov/Projects/block-cipher-techniques/BCM/current-modes.

☞ Pour vous aider dans le choix de l'algorithme, consultez le *Guide de sélection d'algorithmes cryptographiques* de l'ANSSI disponible à l'adresse suivante : https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf.

Ci-après, vous trouverez quelques précisions sur les trois modes de chiffrement par bloc disponibles pour les Clients VPN TheGreenBow.

2.8.2 CBC

Le mode de chiffrement avec chaînage de blocs (CBC ou *Cipher Block Chaining* en anglais) figure parmi les plus couramment utilisés avec l'AES. Dans ce mode, avant d'être chiffré, chaque bloc de texte clair est combiné par un OU exclusif (XOR) avec le bloc chiffré précédent. Le premier bloc du texte en clair est combiné avec un vecteur d'initialisation pour éviter que deux messages chiffrés avec la même clé ne produisent les mêmes blocs chiffrés.

Le mode CBC est sensible aux erreurs de transmission du fait que chaque bloc chiffré dépend du bloc précédent. Si un bit est ajouté ou perdu dans le flot de texte chiffré, tous les blocs qui suivent sont décalés et deviennent indéchiffrables. Il nécessite, par conséquent, des mécanismes de détection et de correction d'erreurs pour être utilisé de manière fiable sur des canaux bruités.

Autre inconvénient du chaînage de blocs, le chiffrement et le déchiffrement ne peuvent pas être facilement parallélisés, ce qui peut limiter les performances dans certaines applications.

2.8.3 CTR

Le mode de chiffrement basé sur compteur (CTR ou *Counter* en anglais) utilise un compteur unique pour imiter le fonctionnement d'un chiffrement par flot. Ce compteur doit être initialisé avec une valeur initiale, appelée nom occasionnel ou *nonce*, pour une protection supplémentaire contre les attaques. Il est souvent incrémenté pour chaque bloc chiffré.

Étant donné que chaque bloc de texte clair est chiffré indépendamment des autres, le CTR permet une parallélisation efficace du chiffrement et du déchiffrement.

Contrairement au mode CBC, le CTR n'est pas sensible aux erreurs de transmission dans les données chiffrées du fait que chaque bloc de texte clair est chiffré de manière indépendante.

Le mode CTR ne fournit pas d'authentification intégrée, ce qui signifie qu'il est vulnérable à certaines attaques. Il doit donc être associé à un mécanisme d'authentification externe pour garantir l'intégrité des données.

Il est souvent privilégié pour sa simplicité et ses performances élevées lorsque le chiffrement efficace des données est essentiel.

2.8.4 GCM

Le mode de chiffrement Galois/compteur (GCM ou *Galois/Counter Mode* en anglais) associe le chiffrement basé sur compteur à une balise d'authentification générée en appliquant une fonction de hachage à l'intégralité du texte chiffré. Cela permet à la fois de chiffrer les données et de vérifier leur intégrité pour assurer une protection complète contre la manipulation des données.

Le mode GCM utilise un polynôme d'authentification de Galois pour calculer les valeurs d'authentification des données, ce qui garantit la détection de toute altération des données lors du processus de déchiffrement.

Étant donné que le mode basé sur compteur (CTR) est utilisé pour le chiffrement, le mode GCM peut bénéficier de la parallélisation efficace des opérations, ce qui permet d'obtenir de bonnes performances, notamment dans les environnements haut débit.

Le mode GCM est considéré comme sécurisé lorsqu'il est utilisé correctement avec une clé et un vecteur d'initialisation appropriés. Il a été conçu pour résister à de nombreuses attaques cryptographiques et de ce fait il est largement utilisé dans de nombreuses applications critiques.

2.9 Connexion classique ou TrustedConnect, quelles différences ?

Le CMC propose deux types de connexion différents : **Classique** ou **TrustedConnect**. Ce dernier comporte des paramétrages spécifiques destinés au fonctionnement avec le **Panneau TrustedConnect**, uniquement disponible avec le Client VPN Windows Enterprise.

Le **Panneau TrustedConnect** ne s'appuie que sur les connexions prévues à cet effet, excluant donc les connexions classiques. Il permet d'ouvrir une connexion VPN de manière automatisée lorsque le poste est situé en dehors du réseau de confiance, et de garder la connexion ouverte même en cas de changement d'interface réseau, grâce aux deux fonctionnalités suivantes :

- **TND (Trusted Network Detection)** : permet de déterminer si le poste est à l'intérieur du réseau de confiance en se basant sur des suffixes DNS et l'identification de balises.
- **Always-On** : assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau, par exemple, entre Ethernet, Wi-Fi et 4G/5G.

Depuis la version 7.5 du Client VPN Windows Enterprise, le comportement du **Panneau TrustedConnect** s'adapte en fonction du niveau de conformité détecté par le Secure Connection Agent (SCA), qui détermine si un poste doit être autorisé à accéder au réseau de l'entreprise.

Le **Panneau des Connexions** dans le Client VPN Windows Enterprise, ou la liste des connexions dans les autres Clients VPN TheGreenBow, présente à l'utilisateur l'ensemble des connexions disponibles dans la configuration, qu'elles soient de type **Classique** ou **TrustedConnect**.

☞ Reportez-vous au « Guide de référence » du CMC et au « Guide de l'administrateur » du Client VPN Windows Enterprise pour plus de précisions sur le **Panneau TrustedConnect**.

2.10 Qu'est-ce que le mode IPsec DR ?

Le mode IPsec DR limite les réglages de configuration d'un tunnel IPsec/IKEv2 aux seules options conformes au référentiel IPsec DR de l'ANSSI.

☞ Reportez-vous au « Guide de configuration Client VPN et IPsec DR » pour plus de précisions sur le mode IPsec Diffusion Restreinte (IPsec DR) et savoir comment configurer les Clients VPN TheGreenBow en vue d'établir des connexions avec des passerelles configurées en mode IPsec DR.

2.11 Fonctionnement du Client VPN Quantum Safe

Le nouveau Client VPN Quantum Safe de TheGreenBow propose des algorithmes de cryptographie post-quantique (*post-quantum cryptography* ou PQC en anglais). À quoi servent-ils et comment sont-ils mis en œuvre ?

L'avènement des ordinateurs quantiques menace sérieusement la sécurité de nos communications et de nos données numériques, car ils pourront facilement décrypter les algorithmes de chiffrement comme le RSA. La PQC émerge alors comme une solution essentielle pour contrer cette menace.

Contrairement à la cryptographie traditionnelle basée sur la factorisation de grands nombres, les algorithmes post-quantiques s'appuient sur des problèmes mathématiques résistants aux attaques quantiques. Le NIST a lancé en 2016 un processus de standardisation, aboutissant aux premiers standards en 2024, notamment les algorithmes CRYSTALS-Kyber[1] pour l'échange de clés et CRYSTALS-Dilithium[2] pour l'authentification.

Les VPN post-quantiques assurent une protection efficace contre les attaques de type « *Harvest Now, Decrypt Later* » (HNDL), qui consistent à capturer dès à présent des communications chiffrées pour les déchiffrer ultérieurement. Cette protection est indispensable pour les secteurs manipulant des données sensibles à long terme (défense, santé, finance).

Actuellement, le nouveau Client VPN Quantum Safe de TheGreenBow propose des algorithmes post-quantiques pour les échanges de clés (voir section 2.12 Algorithmes d'échange de clés post-quantiques, quelles différences ?).

Face à l'immaturité actuelle de la PQC et à l'ampleur de la menace quantique, la « crypto-agilité » devient essentielle. Elle permet aux organisations de passer rapidement d'un système de chiffrement à un autre, grâce à une conception modulaire et des interfaces standardisées comme PKCS #11.

Les VPN post-quantiques de TheGreenBow constituent donc une solution incontournable pour sécuriser durablement les communications sensibles face à la révolution quantique.

[1] Normalisé sous le nom Federal Information Processing Standard (FIPS) 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).

[2] Normalisé sous le nom Federal Information Processing Standard (FIPS) 204: Module-Lattice-Based Digital Signature Standard (ML-DSA).

2.12 Algorithmes d'échange de clés post-quantiques, quelles différences ?

Le nouveau Client VPN Quantum Safe de TheGreenBow propose les trois algorithmes de chiffrement post-quantiques suivants pour les échanges de clés :

- CRYSTALS-Kyber KEM[1]
- FrodoKEM AES
- FrodoKEM SHAKE

En voici les principales différences.

Kyber KEM et FrodoKEM appartiennent à deux familles d'algorithmes différents. La première famille est fondée sur les réseaux euclidiens et plus précisément l'apprentissage modulaire avec erreurs (*module learning with errors* ou M-LWE en anglais) alors que la seconde est fondée sur l'apprentissage avec erreurs (*learning with errors* ou LWE en anglais) réalisé sur des matrices aléatoires classiques (sans structure mathématique supplémentaire).

En termes de performances, Kyber KEM est très efficace aussi bien en ce qui concerne la vitesse de calcul que la taille des clés, alors que FrodoKEM est plus conservatif en matière de sécurité. Du fait que ce dernier repose uniquement sur le LWE avec des matrices entièrement aléatoires, son analyse est plus robuste que celle de Kyber KEM face à d'éventuelles failles structurelles.

Enfin, FrodoKEM AES se distingue par l'utilisation d'AES pour la génération des nombres aléatoires nécessaires aux clés, alors que FrodoKEM SHAKE utilise la fonction de hachage SHAKE comme source d'aléa, offrant ainsi une alternative à AES pour ceux qui veulent éviter les dépendances aux blocs de chiffrement.

Les avantages et inconvénients de ces algorithmes sont résumés dans le tableau suivant :

Algorithme	Famille	Performances	Sécurité
CRYSTALS-Kyber KEM	M-LWE	Très efficace	Robuste, mais exploite une structure mathématique
FrodoKEM AES	LWE	Moins efficace	Plus conservatif (pas de structures)
FrodoKEM SHAKE	LWE	Moins efficace	Plus conservatif, sans dépendance à AES

[1] Renommé en ML-KEM par le NIST (voir note 1 à la page précédente).

3 Prise en main du CMC

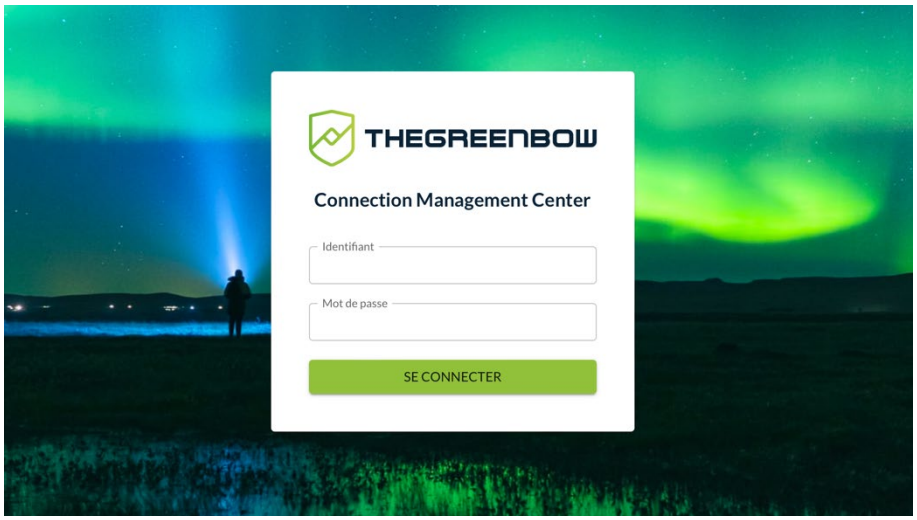
3.1 Introduction

Ce chapitre est destiné à faciliter la prise en main de l'application web Connection Management Center (CMC). Vous y trouverez des informations sur la navigation et les éléments généraux d'ergonomie.

3.2 Connexion au CMC

La connexion au CMC se fait par l'intermédiaire d'un navigateur internet à l'adresse configurée pour l'application web de type `cmc.domaine.lan`.

Lorsque vous accédez à l'URL du CMC, vous verrez un écran de connexion comme ci-dessous :



Les données d'accès par défaut sont les suivantes :

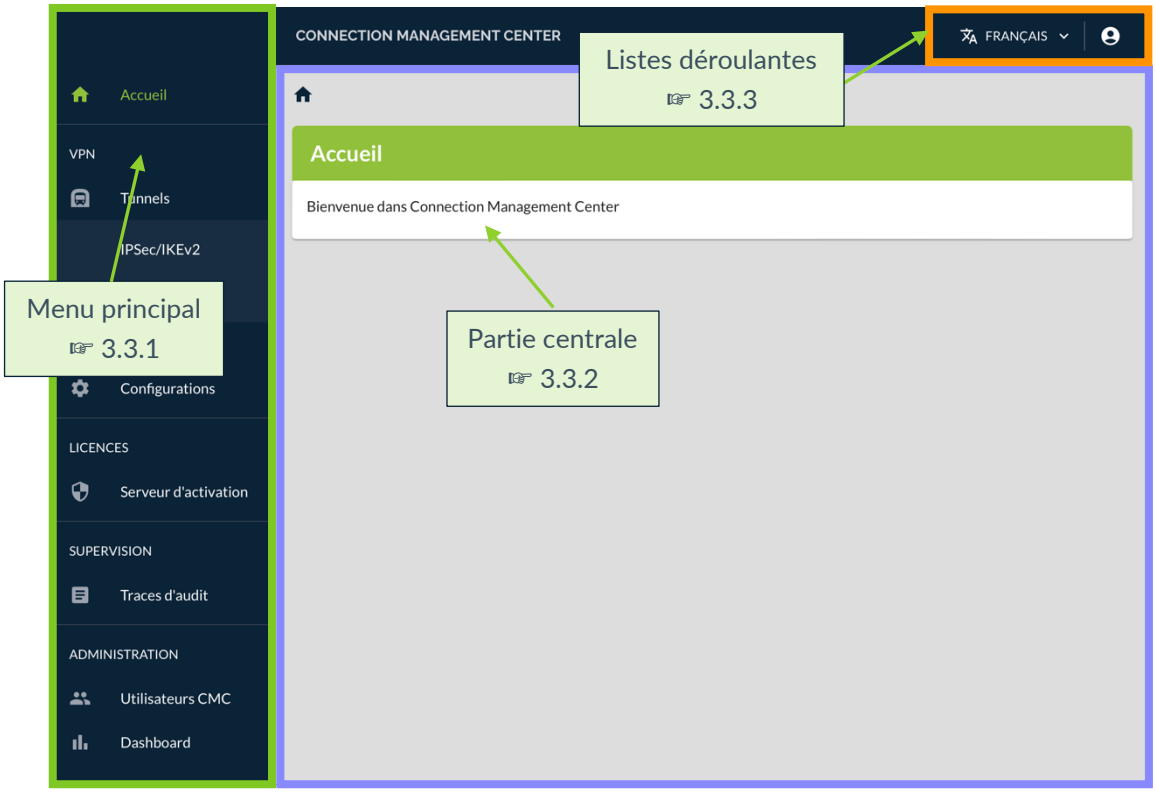
- Identifiant : `cmc_admin`
- Mot de passe : `cmc_admin_pwd`

Il est recommandé de modifier le mot de passe de l'utilisateur par défaut dès la première connexion.

3.3 Interface

L'interface du CMC se veut simple et facile à naviguer. Elle est constituée d'un menu principal à gauche (en vert sur la figure ci-dessous), d'une partie

centrale (en violet) présentant le contenu et de deux listes déroulantes (en orange) en haut à droite de la page.



3.3.1 Menu principal

Le menu principal contient les cinq rubriques principales suivantes (en vert dans le graphique ci-dessous) :

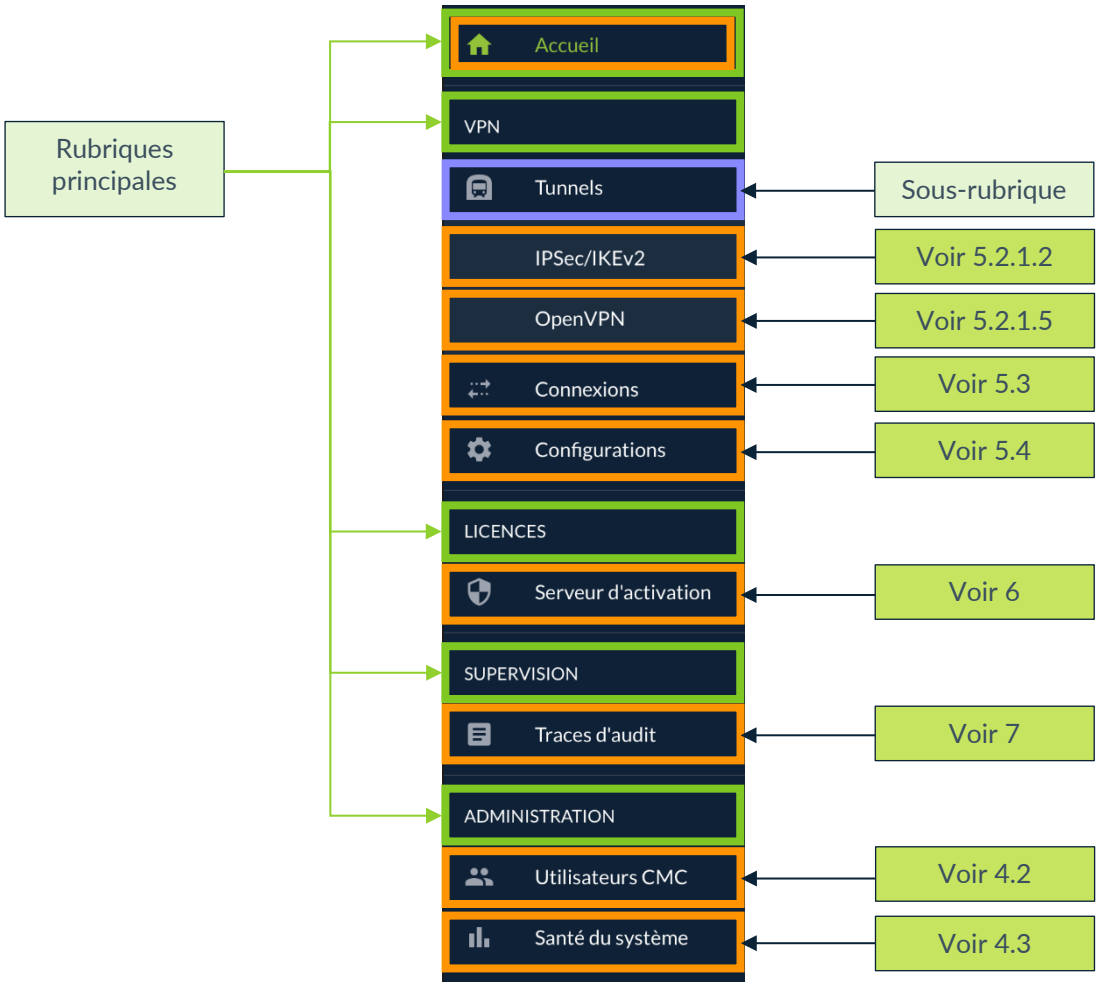
- Accueil
- VPN
- LICENCES
- SUPERVISION
- ADMINISTRATION

La rubrique **Accueil** donne directement accès à la page d'accueil de l'application web.

Les quatre autres rubriques contiennent une ou plusieurs pages (en orange).

La rubrique **VPN** contient en outre une sous-rubrique **Tunnels** (en violet).

La page actuellement affichée dans la partie centrale est mise en évidence par l'affichage en vert du nom de la page.



3.3.2 Partie centrale

La partie centrale de l'interface du CMC est l'endroit où s'affiche le contenu des pages sélectionnées à partir du menu principal.

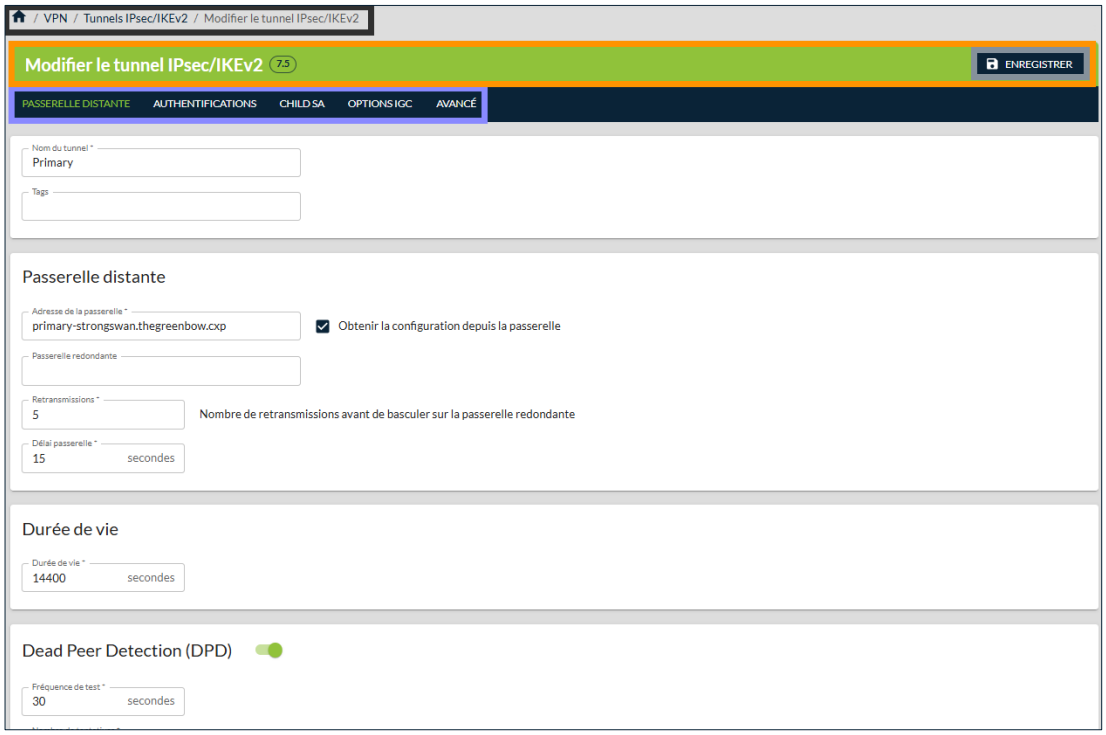
Certaines pages affichées dans la partie centrale peuvent contenir plusieurs onglets (en violet dans le graphique ci-dessous). C'est notamment le cas des pages de création ou de modification des tunnels.

Comme pour les pages sélectionnées dans le menu principal, l'onglet sélectionné dans une page est mis en évidence par l'affichage en vert du nom de l'onglet.

Un fil d'Ariane (en bleu nuit) dans la partie supérieure de la page permet de revenir en arrière dans les différents niveaux de navigation. Il suffit pour cela de cliquer sur le niveau souhaité.

⚠ Si vous quittez une page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

Des boutons d'action (en gris) sur certaines pages donnent accès à des pages de création ou de modification des éléments, ou permettent d'enregistrer les modifications. Ils figurent généralement dans la partie droite du bandeau de titre des pages (en orange).

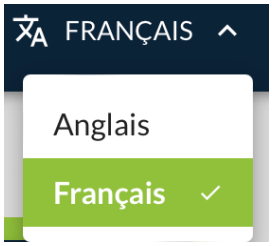


Certaines pages contiennent des listes d'objets structurées sous forme de tableaux qui comportent des fonctionnalités communes décrites ci-après (cf. 3.4 Comment exploiter les listes d'objets).

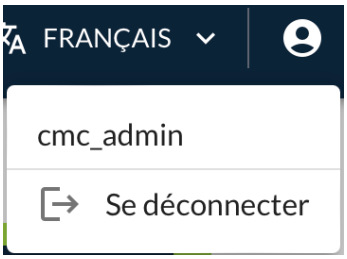
3.3.3 Listes déroulantes

En haut à droite de l'interface du CMC figurent deux listes déroulantes.

Celle de gauche sert à sélectionner la langue. Actuellement, seul le français et l'anglais sont disponibles.



Celle de droite affiche le nom de l'utilisateur actuellement connecté à l'interface et un bouton de déconnexion. Si vous disposez des droits d'administration des utilisateurs, vous pouvez cliquer sur le nom d'utilisateur pour afficher ses droits.



3.4 Comment exploiter les listes d'objets

3.4.1 Introduction

Les pages présentées sous forme de liste d'objets comportent des éléments communs qui permettent d'effectuer des actions sur les données de la liste, notamment pour les trier, filtrer, sélectionner, dupliquer, exporter ou supprimer.

Ces éléments peuvent varier d'une liste à une autre et leur présence dépend également des droits attribués à l'utilisateur. Leur utilisation se veut simple et intuitive. Il s'agit notamment des éléments suivants :

- le nombre de lignes dans la liste figure à la suite du nom de la page ;
- un ou plusieurs boutons d'action figurent à droite dans la barre de titre de la page, notamment pour ajouter une ligne à la liste ;
- une colonne de sélection tout à fait à gauche ;
- une colonne **Actions** tout à fait à droite comportant :
  - un bouton d'édition en forme de crayon qui ouvre la ligne correspondante en mode modification et
  - un menu d'action en forme de pictogramme avec trois points verticaux ;
- visibles au survol avec la souris, chaque en-tête de colonne autre que les deux mentionnées ci-dessus comporte :
  - un menu d'en-tête en forme de pictogramme avec trois points verticaux et,
  - le cas échéant, un pictogramme en forme de flèche vers le haut ou le bas indiquant l'ordre de tri sélectionné ;
- dans la partie inférieure droite de la liste :
  - un menu de sélection du nombre de lignes à afficher par page ;
  - les lignes affichées sur la page en cours et le nombre de lignes au total ;
  - des flèches de navigation permettant de faire défiler les pages de la liste lorsqu'elle en contient plusieurs.

3.4.2 Sélectionner une ou plusieurs lignes

Pour sélectionner une ou plusieurs lignes, procédez comme suit :

- dans la colonne de sélection, cochez la case de la ou des lignes que vous souhaitez sélectionner ;

OU :

- si vous souhaitez sélectionner toutes les lignes de la page actuelle, cochez la case dans l'en-tête de la colonne de sélection.

Le nombre de lignes sélectionnées et un bouton **Supprimer** s'affichent en bas de la liste.

3.4.3 Supprimer une ou plusieurs lignes

Vous disposez de deux moyens pour supprimer une ligne. Vous pouvez soit :

- développer le menu d'action de la ligne concernée, puis sélectionner l'option **Supprimer** ;
- ou cocher la case de la ligne à supprimer dans la colonne de sélection, puis cliquer sur le bouton **Supprimer** qui s'affiche en bas de la liste.

Si vous souhaitez supprimer plusieurs lignes en même temps, cochez les cases correspondant aux lignes à supprimer dans la colonne de sélection, puis cliquez sur le bouton **Supprimer** qui s'affiche en bas de la liste.

Dans tous les cas, un message de confirmation s'affiche avant que la ou les lignes ne soient définitivement supprimées.

Si un tunnel est utilisé dans un connexion et que vous tentez de le supprimer, un message s'affiche vous indiquant la ou les connexions dans lesquelles le tunnel est utilisé et que vous ne pouvez pas le supprimer. Vous devez d'abord le désassocier de la ou des connexions dans lesquelles il est utilisé avant de pouvoir le supprimer.

Il en va de même pour les connexions utilisées dans des configurations.

La suppression d'une ligne est définitive. Une fois confirmée, cette opération ne peut pas être annulée.

3.4.4 Trier la liste d'objets

Pour trier la liste selon le contenu d'une colonne, il suffit de cliquer sur le nom de la colonne choisie. Un pictogramme avec une flèche pointant vers le haut ↑ s'affiche à côté du nom de la colonne dans l'en-tête pour indiquer que la liste est triée dans l'ordre ascendant du contenu de cette colonne.

Cliquez une nouvelle fois sur le nom de la colonne ou sur le pictogramme en forme de flèche pour inverser l'ordre de tri. Le pictogramme évolue et la flèche pointe vers le bas. La liste est triée dans l'ordre descendant du contenu de cette colonne.

Cliquez une troisième fois pour annuler le tri. Le pictogramme disparaît.

Si vous avez trié la liste sur le contenu d'une colonne et que vous cliquez sur le nom de la colonne ou sur le pictogramme en forme de flèche d'une autre colonne, la liste sera triée dans l'ordre ascendant du contenu de cette nouvelle colonne. Le pictogramme en forme de flèche disparaît de l'en-tête de la colonne précédemment triée et s'affiche dans celui de la nouvelle colonne.

Vous pouvez également activer le tri ascendant ou descendant depuis le menu contextuel de chaque en-tête de colonne. Pour cela, cliquez sur le pictogramme avec les trois points verticaux qui s'affiche au survol de l'en-tête avec le pointeur de la souris, puis sélectionnez l'option **Tri ascendant** ou **Tri descendant**.

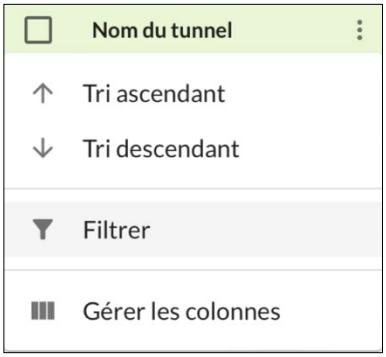
Pour annuler le tri, cliquez sur le pictogramme du menu contextuel, puis sélectionnez l'option **Annuler le tri**.

Il n'est pas possible de trier la liste d'objets sur plusieurs colonnes. En revanche, vous pouvez appliquer des filtres sur plusieurs colonnes (voir section 3.4.5 Filtrer la liste d'objets).

3.4.5 Filtrer la liste d'objets

Pour filtrer la liste d'objets, procédez comme suit :

1. Cliquez sur le pictogramme avec les trois points verticaux qui s'affiche au survol de l'en-tête d'une colonne avec le pointeur de la souris.



2. Dans le menu contextuel, sélectionnez l'option **Filtrer**. Une fenêtre pop-up s'affiche avec un premier filtre comportant le nom de la **Colonne** à partir de laquelle vous avez appelé la fonction, l'opérateur **Contient** et le champ **Valeur** vide.

3. Si vous souhaitez appliquer le filtre à une autre colonne, sélectionnez la colonne souhaitée dans la liste déroulante **Colonne**.
4. Si vous souhaitez utiliser un autre opérateur pour le filtre, sélectionnez l'opérateur souhaité dans la liste déroulante **Opérateur**. Vous pouvez choisir parmi les opérateurs suivants :
   - contient
   - est égal à
   - commence par
   - se termine par
   - est vide
   - n'est pas vide
   - fait partie de
5. Saisissez la valeur à filtrer. Le filtre s'applique immédiatement à la liste.
6. Vous pouvez modifier le filtre ou ajouter un filtre supplémentaire. Dans ce cas, sélectionnez l'opérateur logique (**Et**/**Ou**) à insérer entre les opérandes.
7. Cliquez en dehors de la fenêtre pop-up pour la fermer et poursuivre le travail sur la liste d'objets.
8. Un pictogramme en forme d'entonnoir s'affiche à droite du nom de la ou des colonnes filtrées. Vous pouvez cliquer sur le pictogramme pour rouvrir la fenêtre pop-up de filtrage.

Les valeurs filtrées ne sont pas sensibles à la casse. Vous pouvez appliquer un tri à une liste d'objets filtrée (voir section 3.4.4 Trier la liste d'objets).

Pour supprimer un filtre, procédez comme suit :

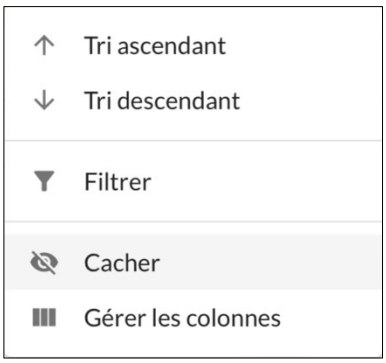
1. Cliquez sur le pictogramme en forme d'entonnoir dans l'en-tête d'une colonne filtrée ou ouvrez le menu contextuel en cliquant sur le pictogramme avec les trois points verticaux, puis sélectionnez l'option **Filtrer**. La fenêtre pop-up de filtrage s'affiche.
2. Cliquez sur la croix devant la ligne de filtre que vous souhaitez supprimer ou cliquez sur le bouton **TOUT SUPPRIMER** pour supprimer tous les filtres.

Si vous avez appliqué un tri à la liste d'objets, celui-ci ne sera pas supprimé lorsque vous supprimez un ou plusieurs filtres.

3.4.6 Cacher une colonne

Pour filtrer la liste d'objets, procédez comme suit :

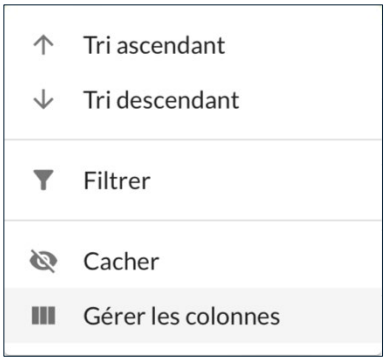
1. Cliquez sur le pictogramme avec les trois points verticaux ⋮ qui s'affiche au survol de l'en-tête d'une colonne avec le pointeur de la souris.



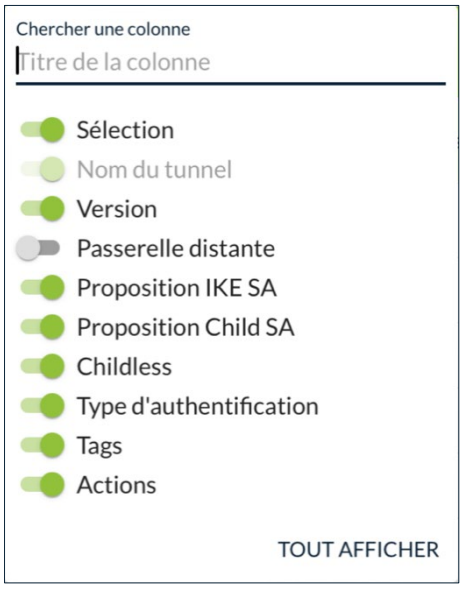
2. Dans le menu contextuel, sélectionnez l'option **Cacher**. La colonne est cachée.

Pour afficher une colonne cachée, procédez comme suit :

1. Cliquez sur le pictogramme avec les trois points verticaux ⋮ qui s'affiche au survol de l'en-tête d'une colonne avec le pointeur de la souris.



2. Sélectionnez l'option **Gérer les colonnes**. Une fenêtre pop-up s'affiche avec une liste des colonnes.



3. Actionnez le bouton bascule de la colonne masquée que vous souhaitez afficher de nouveau.

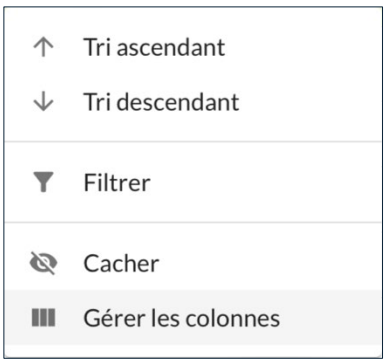
Certaines colonnes ne peuvent pas être masquées, p.ex. la colonne **Nom du tunnel** dans la liste des tunnels. L'option **Cacher** ne figure pas dans le menu contextuel de l'en-tête de ces colonnes et bouton bascule de la fenêtre pop-up de gestion des colonnes est grisée et ne peut pas être basculé.

3.4.7 Gérer les colonnes

L'option **Gérer les colonnes** du menu contextuel dans l'en-tête d'une colonne sert à afficher ou masquer les colonnes de la liste d'objets.

Pour afficher une colonne cachée, procédez comme suit :

1. Cliquez sur le pictogramme avec les trois points verticaux ⋮ qui s'affiche au survol de l'en-tête d'une colonne avec le pointeur de la souris.



2. Sélectionnez l'option **Gérer les colonnes**. Une fenêtre pop-up s'affiche avec une liste des colonnes.

3. Si vous souhaitez réduire le nombre de colonnes affichées dans la liste, saisissez une partie du titre de la colonne dans le champ prévu à cet effet.

4. Cachez ou masquez les colonnes de votre choix à l'aide des boutons bascule. Si vous souhaitez afficher toutes les colonnes, cliquez sur le bouton **TOUT AFFICHER**.

Certaines colonnes ne peuvent pas être masquées, p.ex. la colonne **Nom du tunnel** dans la liste des tunnels. L'option **Cacher** ne figure pas dans le menu contextuel de l'en-tête de ces colonnes et bouton bascule de la fenêtre pop-up de gestion des colonnes est grisée et ne peut pas être basculé.

4 Administration du CMC

4.1 Présentation

Le CMC peut être administré et exploité par une seule personne.

Cependant, en fonction de la taille de votre organisation, il pourrait s'avérer utile de partager les tâches d'administration avec d'autres membres de l'équipe. Par exemple, la Direction des systèmes d'information (DSI) s'occupe de l'administration des utilisateurs et le ou la Responsable de la sécurité des systèmes d'information (RSSI) se charge de définir les tunnels, les connexions et les configurations VPN.

La rubrique ADMINISTRATION du menu principal contient les deux pages suivantes :

- **Utilisateurs CMC**, voir 4.2
- **Santé du système**, voir 4.3

☞ Pour connaître les différents groupes d'utilisateurs et les droits associés, reportez-vous à la section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?

☞ Pour savoir comment créer un utilisateur, reportez-vous à la section 4.2.3 Créer un utilisateur.

4.2 Gestion des utilisateurs

4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?

Les groupes d'utilisateurs correspondent aux sections principales du menu de navigation. Lorsqu'ils se connectent au CMC, les utilisateurs ne verront que les menus pour lesquels ils le droit d'accès. La gestion des configurations VPN est en outre subdivisée en droits de consultation, d'édition et de suppression.

Sur les pages **Créer un utilisateur** et **Modifier l'utilisateur**, les groupes se présentent comme suit :

- Consulter les VPN
  - Éditer les VPN
  - Supprimer les VPN
- Licences
- Supervision
- Administration du compte

Il est impossible de créer un utilisateur sans le rattacher à au moins un groupe.

⚠ Les utilisateurs qui font partie du groupe **Administration du compte** disposent du droit d'administration du CMC et peuvent par conséquent modifier leur propres droits.

4.2.1.1 Gestion des configurations VPN

Les utilisateurs du groupe **Consulter les VPN** peuvent visualiser tous les détails des tunnels, connexions et configurations VPN, mais ne peuvent pas en créer de nouveaux ni modifier ou supprimer les éléments existants.

Ils peuvent aussi exporter les configurations au format JSON ou TGB, mais pas en importer.

Afin de pouvoir créer des tunnels, connexions et configurations ou modifier les éléments existants, l'utilisateur doit faire partie du groupe **Éditer les VPN**. Les utilisateurs de ce groupe peuvent aussi importer des configurations au format JSON.

Afin de pouvoir supprimer des tunnels, connexions et configurations, l'utilisateur doit faire partie du groupe **Supprimer les VPN**. Les utilisateurs de ce groupe qui ne font pas aussi partie du groupe **Éditer les VPN** ne peuvent pas modifier les éléments existants ni importer des configurations.

ℹ Les utilisateurs qui font partie du groupe **Éditer les VPN** ou **Supprimer les VPN** font obligatoirement partie du groupe **Consulter les VPN**.

4.2.1.2 Gestion des licences

Les utilisateurs du groupe **Licences** peuvent visualiser et exploiter les fonctions du service d'activation.

À ce titre, ils peuvent notamment :

- rechercher une licence et visualiser son activation ;
- réinitialiser des numéros de licence ;
- importer des numéros de licence ;
- procéder à une activation manuelle ;
- consulter les logs relatifs à l'activation d'un logiciel ;
- exporter les résultats d'une recherche de licences ou un log ;
- générer des rapports pour TheGreenBow.

☞ Pour savoir comment exploiter le service d'activation, reportez-vous au chapitre 6 Gestion des licences.

4.2.1.3 Supervision du CMC

Les utilisateurs du groupe **Supervision** peuvent visualiser les traces d'audit sur la page **Traces d'audit**.

☞ Pour savoir comment exploiter les fonctions de supervision, reportez-vous au chapitre 7 Supervision.

4.2.1.4 Administration du CMC

Les utilisateurs du groupe **Administration du compte** peuvent administrer les comptes utilisateurs, c'est-à-dire créer, modifier et supprimer des utilisateurs ainsi que leur attribuer ou retirer des droits. Ils ont également accès au tableau de bord **Santé du système** pour s'assurer du bon fonctionnement du CMC.

Lorsque les droits d'un utilisateur sont modifiés et que celui-ci est connecté au moment de la modification, les modifications ne prendront effet que lorsque l'utilisateur se sera déconnecté puis reconnecté.
Si vous souhaitez éjecter immédiatement un utilisateur du système, vous devez d'abord supprimer son compte avant de lui en recréer un nouveau, le cas échéant.

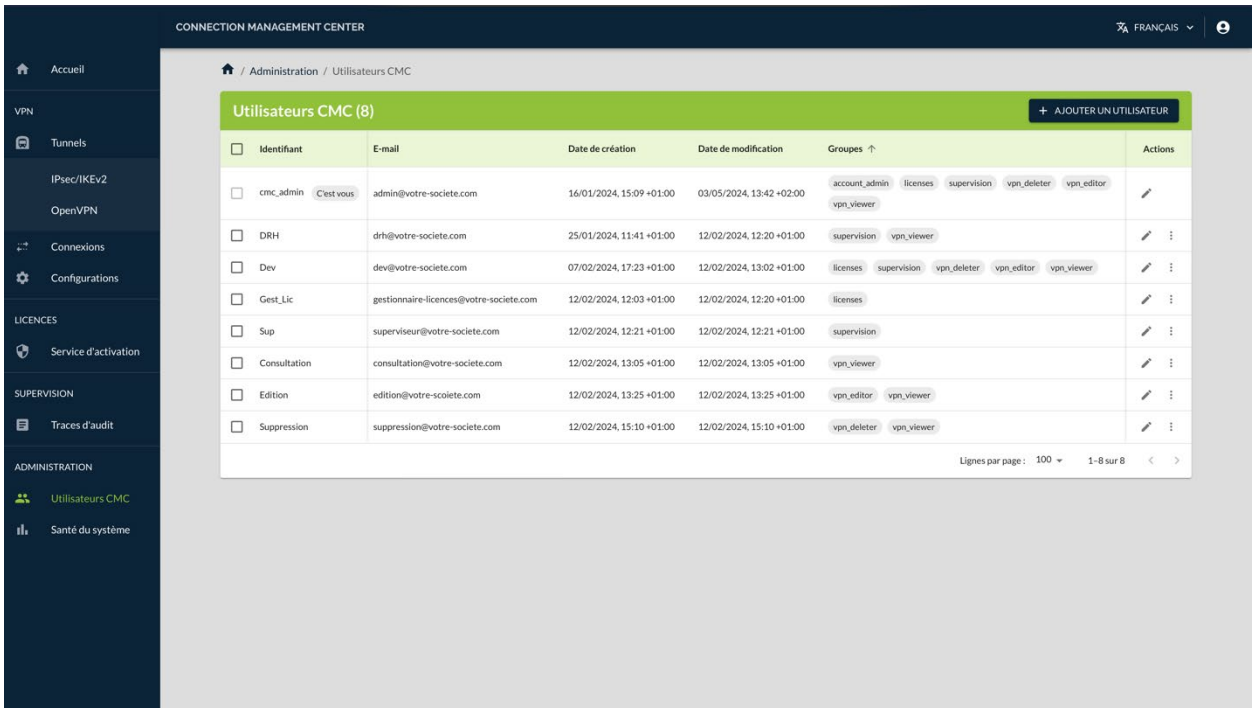
Les utilisateurs qui font partie du groupe **Administration du compte** disposent du droit d'administration du CMC et peuvent par conséquent modifier leur propres droits.

4.2.2 Travailler avec la liste des utilisateurs

Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à visualiser la liste des utilisateurs (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour afficher la liste des utilisateurs, dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Utilisateurs CMC**.

La liste des utilisateurs s'affiche :



Vous pouvez trier et filtrer les données de la liste, cacher ou afficher des colonnes, ou encore créer, modifier ou supprimer des utilisateurs.

☞ Pour savoir comment travailler avec les listes d'objets, reportez-vous à la section 3.4 Comment exploiter les listes d'objets.

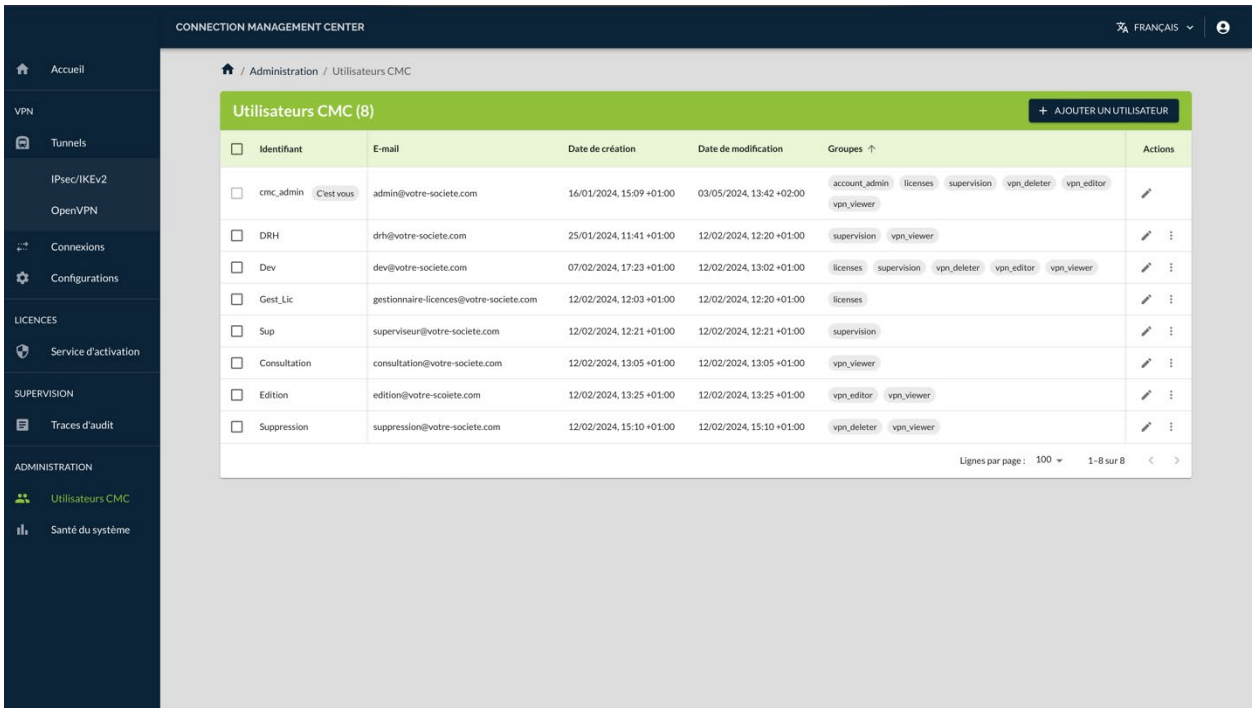
4.2.3 Créer un utilisateur

Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à créer des utilisateurs (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

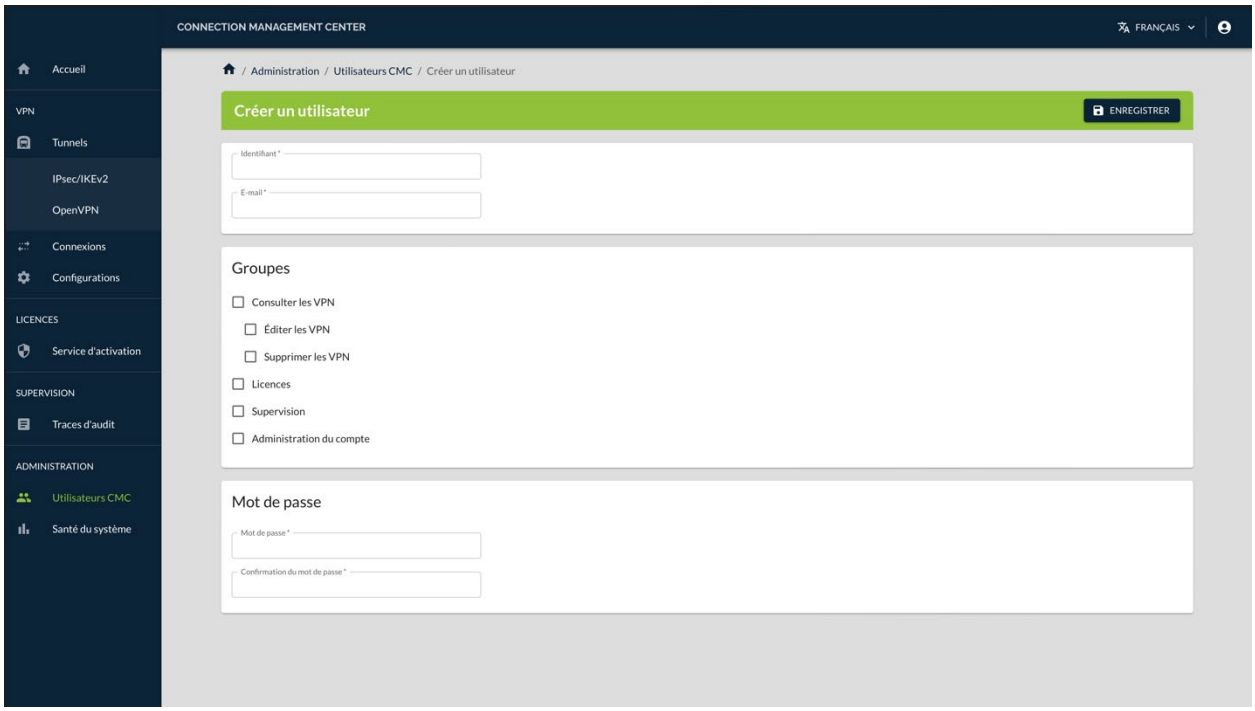
Pour créer un utilisateur, procédez de la manière suivante :

1. Dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Utilisateurs CMC**.

La liste des utilisateurs s'affiche :



2. En haut à droite, dans l'en-tête de la liste, cliquez sur le bouton **AJOUTER UN UTILISATEUR**. La page **Créer un utilisateur** s'affiche :

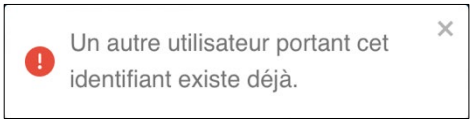


3. Renseignez un identifiant pour cet utilisateur.

Ce champ n'est pas sensible à la casse. Si vous avez saisi `Admin`, l'utilisateur pourra se connecter en saisissant `admin`. Par ailleurs, vous ne pouvez pas créer un utilisateur dont l'identifiant est `Admin` et un autre avec `admin`.

4. Saisissez son adresse e-mail.
5. Cochez les cases des groupes dont l'utilisateur doit faire partie. Les droits correspondant lui seront attribués (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).
6. Saisissez le mot de passe, puis confirmez-le.
7. Appuyez sur le bouton **ENREGISTRER** en haut à droite, dans l'en-tête de la page. Un message s'affiche dans la partie supérieure droite de la page pour confirmer le bon déroulement de l'opération :

Si vous avez attribué un identifiant existant à l'utilisateur que vous souhaitez créer, l'opération échoue et un message en ce sens s'affiche dans la partie supérieure droite de la page :



Dans ce cas, modifiez l'identifiant et cliquez à nouveau sur le bouton **ENREGISTRER**.

8. Lorsque la création de l'utilisateur a réussi, la liste des utilisateurs s'affiche avec l'utilisateur que vous venez de créer.

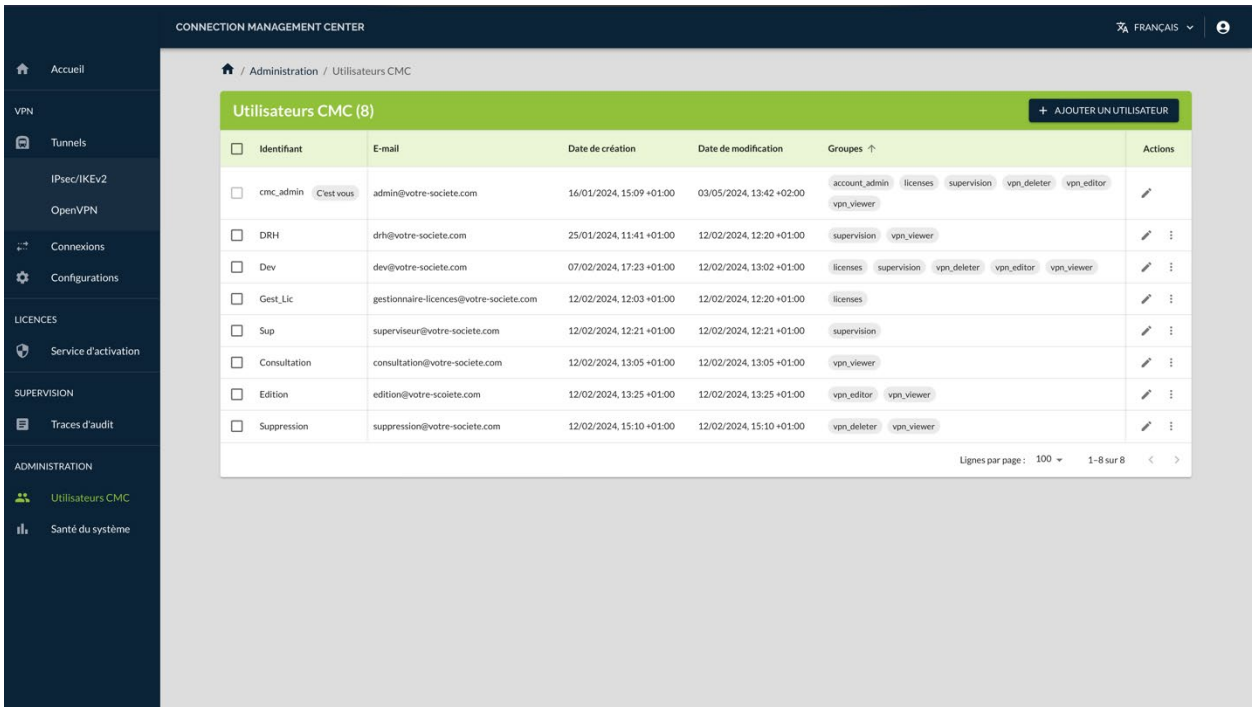
Le critère de tri par défaut est la **Date de création** dans l'ordre croissant. Avec ce critère, les nouveaux utilisateurs sont ajoutés à la fin de la liste. Si vous avez sélectionné un autre critère ou ordre de tri, les nouveaux utilisateurs figureront dans l'ordre correspondant. Reportez-vous à la section 3.4 Comment exploiter les listes d'objets pour plus de précision sur les critères et l'ordre de tri.

4.2.4 Modifier un utilisateur

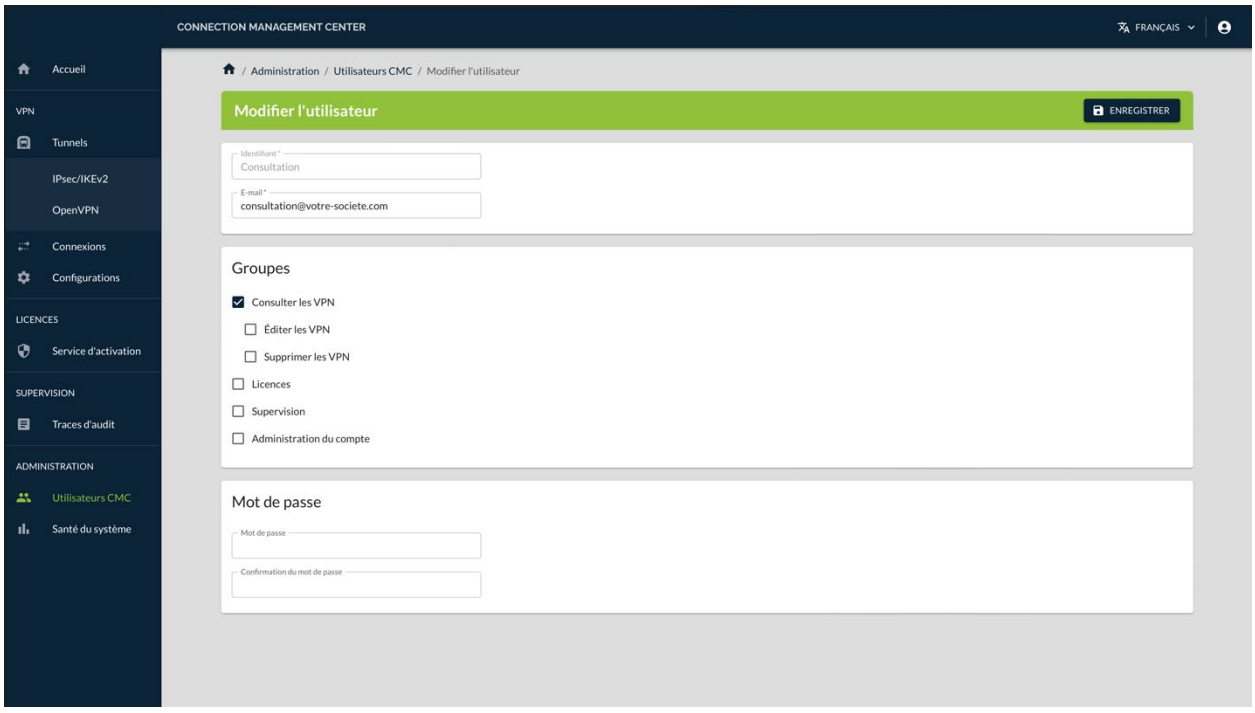
Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à modifier des utilisateurs (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour modifier un utilisateur, procédez de la manière suivante :

1. Dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Utilisateurs CMC**. La liste des utilisateurs s'affiche :



2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier** dans la ligne correspondant à l'utilisateur que vous souhaitez modifier. La page **Modifier l'utilisateur** s'affiche :



3. Apportez les modifications souhaitées, p. ex. ajoutez l'utilisateur à un groupe.
4. Cliquez sur le bouton **ENREGISTRER** en haut à droite, dans l'en-tête de la page. Un message s'affiche dans la partie supérieure droite de la page pour confirmer le bon déroulement de l'opération :

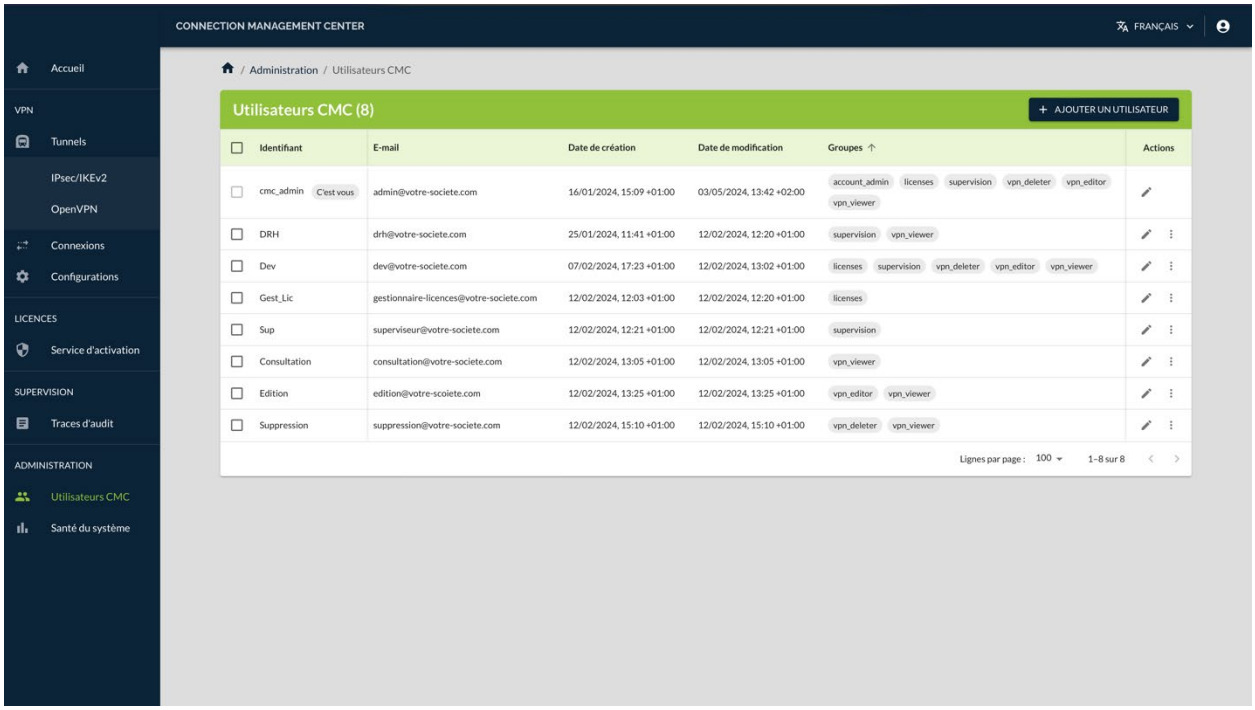
Vous pouvez modifier tous les éléments sauf l'identifiant.

5. Lorsque la modification de l'utilisateur a réussi, la liste des utilisateurs s'affiche.

4.2.5 Supprimer un utilisateur

Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à supprimer des utilisateurs (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour supprimer un utilisateur, dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Utilisateurs CMC**. La liste des utilisateurs s'affiche :



Vous pouvez supprimer un utilisateurs de deux manières :

- en cochant la ou les lignes à supprimer dans la colonne de sélection, puis en cliquant sur le bouton **Supprimer** qui s'affiche en bas de la liste ;
- en sélectionnant l'option **Supprimer** du menu d'action de la ligne à supprimer.

☞ Pour en savoir davantage sur la suppression des lignes d'une liste d'objets, reportez-vous à la section 3.4.3 Supprimer une ou plusieurs lignes.

La suppression d'un utilisateur est définitive. Une fois confirmée, cette opération ne peut pas être annulée.

L'utilisateur par défaut `cmc_admin` ne peut pas être supprimé.

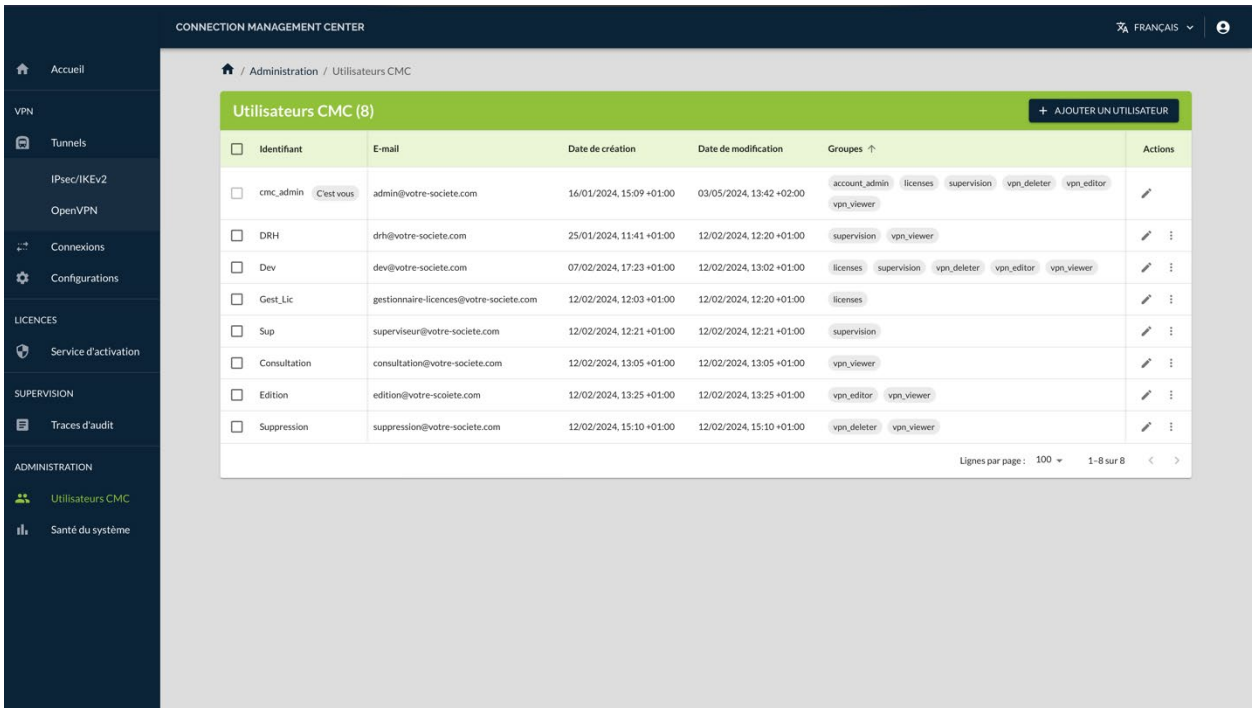
4.2.6 Affecter un utilisateur à un groupe d'utilisateurs

Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à affecter des utilisateurs à des groupes (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour affecter un utilisateur à un groupe ou modifier les groupes auxquels un utilisateur est affecté, procédez de la manière suivante :

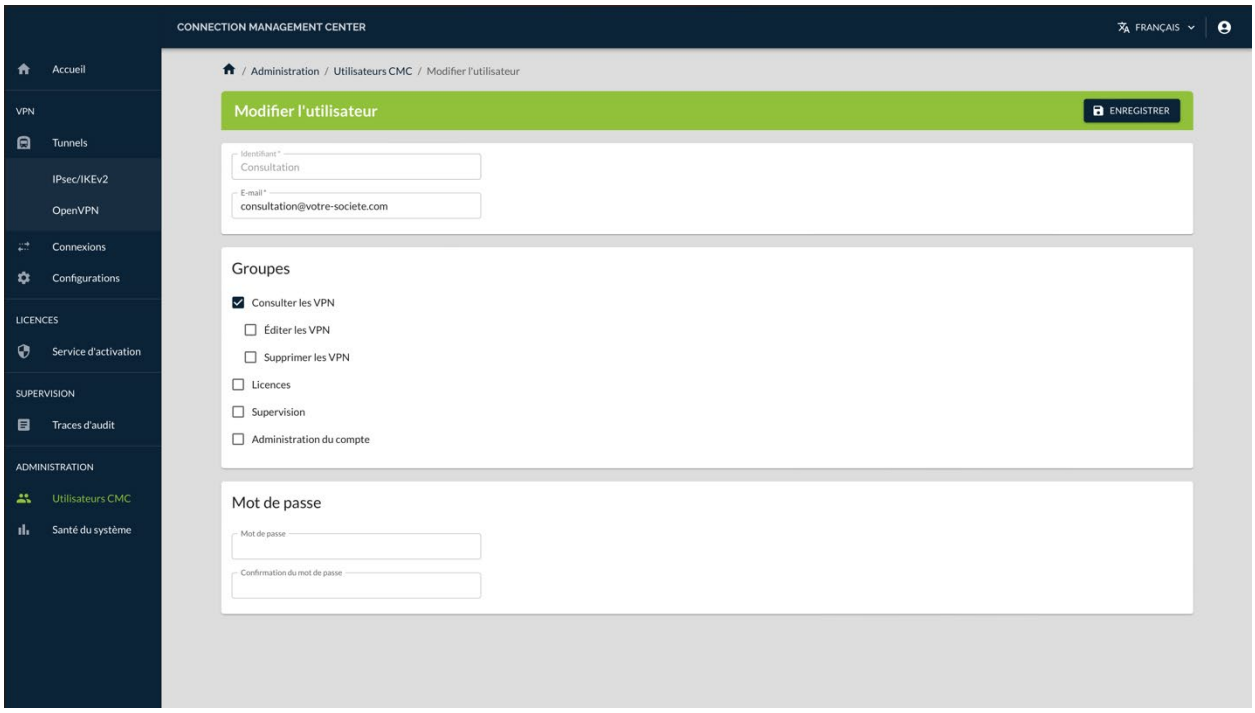
1. Dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Utilisateurs CMC**.

La liste des utilisateurs s'affiche :



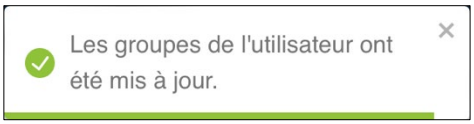
2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier** au niveau de la ligne correspondant à l'utilisateur que vous souhaitez modifier.

   La page **Modifier l'utilisateur** s'affiche :



3. Cochez la ou les cases des groupes auxquels vous souhaitez affecter l'utilisateur.

4. Cliquez sur le bouton **ENREGISTRER** en haut à droite, dans l'en-tête de la page. Un message s'affiche dans la partie supérieure droite de la page pour confirmer le bon déroulement de l'opération :



Si l'utilisateur est connecté au moment où les modifications sont effectuées, celles-ci ne seront prise en compte que lors de la prochaine session de l'utilisateur. En d'autres termes, l'utilisateur doit se déconnecter puis se reconnecter avant de bénéficier des nouveaux droits qui lui ont été attribués.

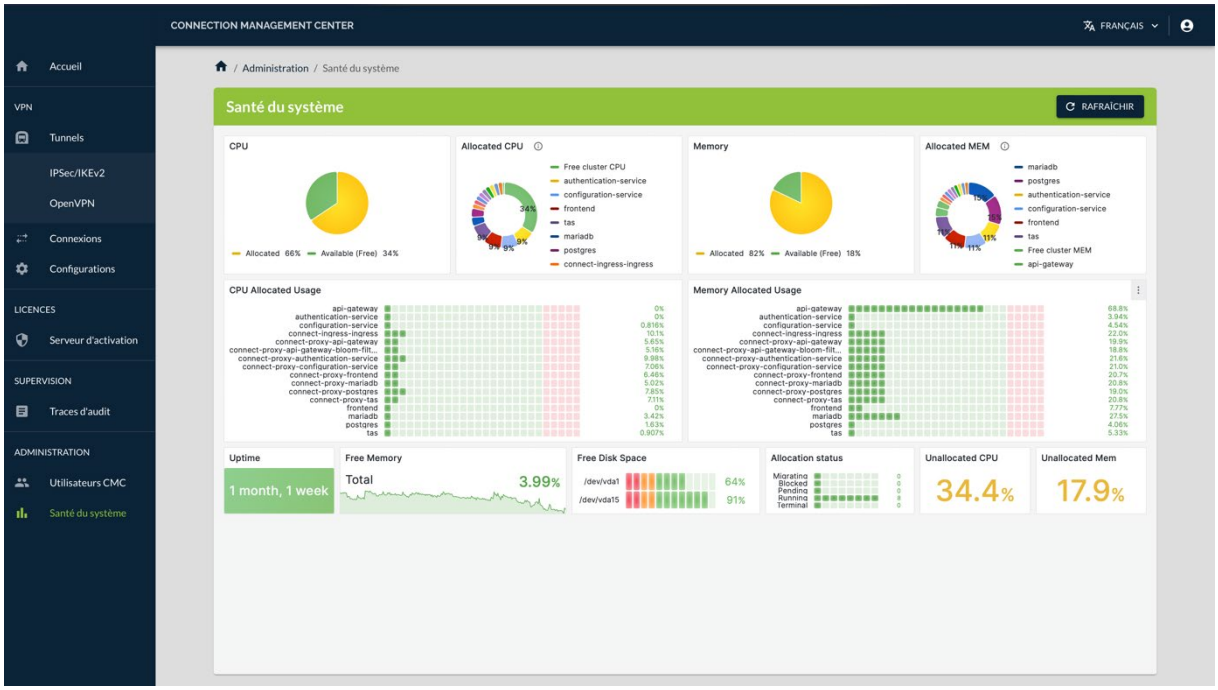
4.3 Santé du système

Seuls les utilisateurs qui disposent du droit d'administration du compte sont habilités à consulter la santé du système (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Le CMC met à disposition des administrateurs un certain nombre de tableaux de bord destinés à fournir une vue d'ensemble de la santé du système.

Pour accéder à cette vue, dans le menu principal, sous **ADMINISTRATION**, sélectionnez **Santé du système**.

La page **Santé du système** s'affiche avec l'ensemble des tableaux de bord :



Les tableaux de bord présentent différentes vues de l'allocation de la CPU à gauche et de l'allocation de mémoire à droite.

Dans la partie inférieure figurent les tableaux de bord suivants :

- Uptime : temps de fonctionnement depuis le dernier démarrage
- Free memory : taux de mémoire disponible
- Free disk space : taux de remplissage des disques durs
- Allocation status : état de l'allocation
- Unallocated CPU : taux de CPU non allouée
- Unallocated Mem : taux de mémoire non allouée

Toutes les informations sont uniquement disponibles en anglais.

Pour faciliter leur lecture, les informations présentées dans les différents tableaux de bord sont figées à l'instant où la page **Santé du système** a été ouverte. Si vous souhaitez actualiser les informations affichées, il suffit de cliquer sur le bouton **RAFRAÎCHIR** situé en haut à droite dans le bandeau de titre de la page.

5 Configuration VPN

5.1 Introduction

La procédure de création des configurations VPN est très similaire à celle des Clients VPN TheGreenBow. Si vous avez déjà utilisé nos produits Client VPN macOS ou Windows, vous allez rapidement vous retrouver.

☞ Pour comprendre les notions de tunnel, connexion et configuration telles qu'elles sont utilisées chez TheGreenBow, reportez-vous à la section 2.4 Qu'est-ce qu'un tunnel, une connexion, une configuration ?

De manière générale, un utilisateur commence par créer un ou plusieurs tunnels, puis il crée une ou plusieurs connexions exploitant ce ou ces tunnels, et enfin il crée une ou plusieurs configurations composées de connexions et de tunnels.

Une fois créées, les configurations pourront être exportées, puis déployées sur les postes de travail et terminaux mobiles équipés de Clients VPN.

En fonction des droits qui leur sont conférés par l'équipe d'administration du système, les utilisateurs du CMC pourront simplement consulter les éléments constitutifs de la configuration VPN, les modifier, voire les supprimer (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

5.2 Gérer les tunnels

5.2.1 Créer un tunnel

5.2.1.1 Introduction

Avant de créer un tunnel, vous devez déterminer le type de tunnel que vous souhaitez utiliser :

- IPsec/IKEv2,
- mode IPsec DR,
- v1.0 Quantum Safe,
- OpenVPN.

☞ Pour comprendre les différences entre les protocoles IPsec/IKEv2 et OpenVPN, reportez-vous à la section 2.6 IPsec/IKEv2 ou OpenVPN, quel protocole choisir ?

☞ Pour comprendre les spécificités du mode IPsec DR, reportez-vous à la section 2.10.

☞ Pour comprendre les spécificités du Client VPN Quantum Safe, reportez-vous à la section 2.11.

☞ Pour savoir comment créer un tunnel IPsec/IKEv2, reportez-vous à la section 5.2.1.2.

☞ Pour savoir comment créer un tunnel en mode IPsec DR, reportez-vous à la section 5.2.1.3.

☞ Pour savoir comment créer un tunnel doté d'une cryptographie résistante au quantique, reportez-vous à la section 5.2.1.4.

☞ Pour savoir comment créer un tunnel OpenVPN, reportez-vous à la section 5.2.1.5.

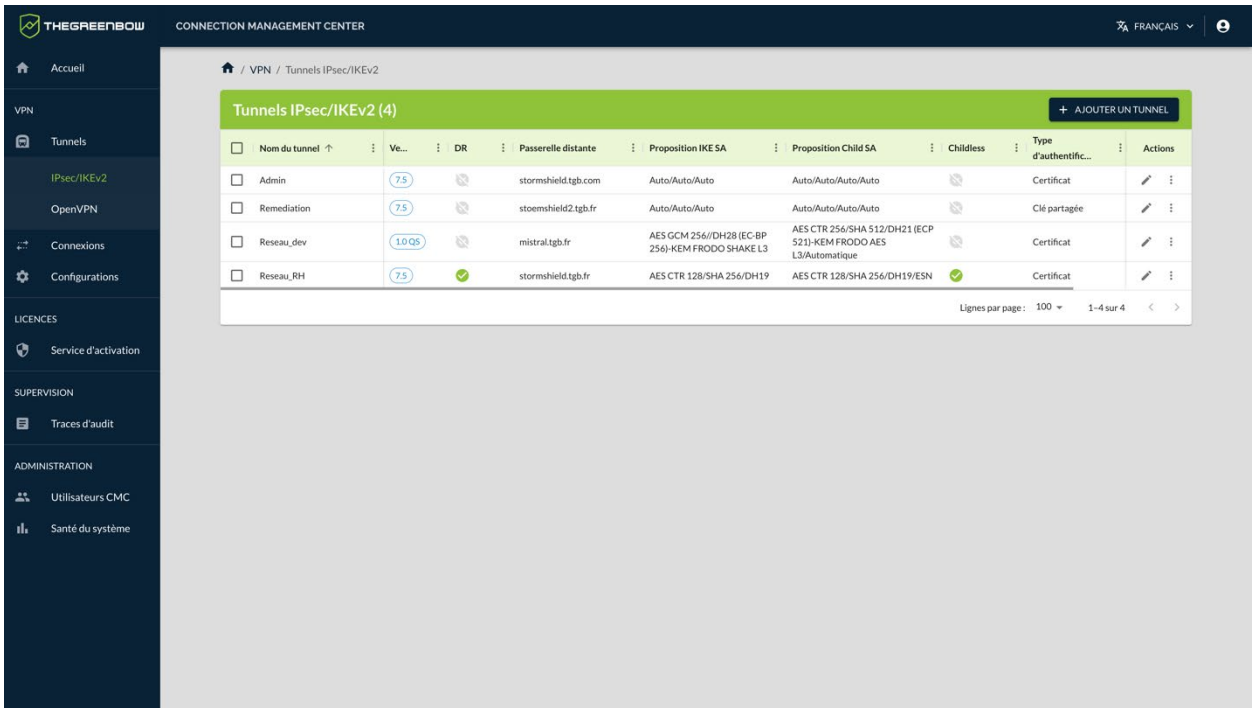
5.2.1.2 Créer un tunnel IPsec/IKEv2

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour créer un tunnel IPsec/IKEv2, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **IPsec/IKEv2**.

La liste des tunnels IPsec/IKEv2 s'affiche :



2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UN TUNNEL**. La boîte de dialogue **Créer un tunnel** s'affiche :

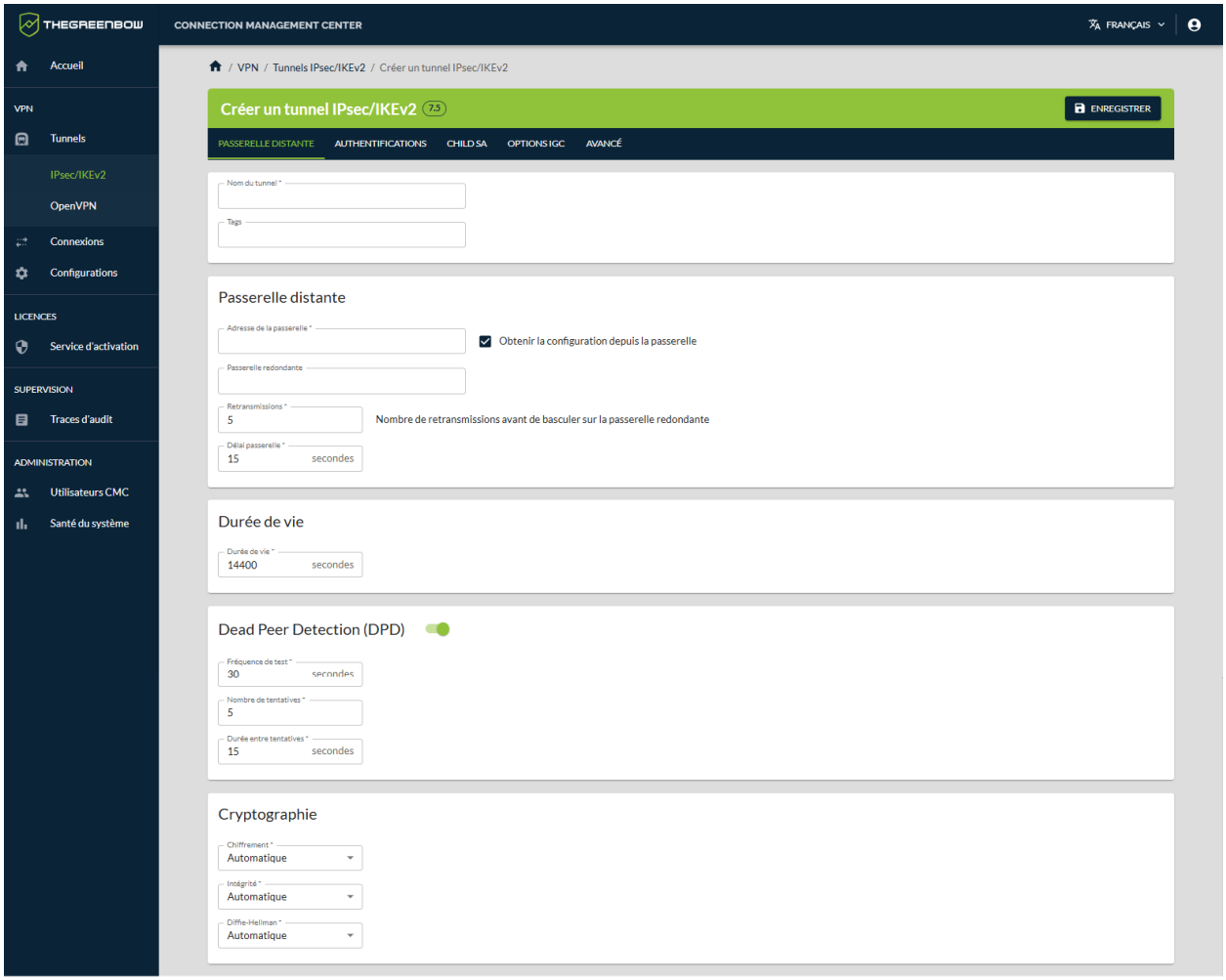
3. Dans la liste déroulante **Version du Client VPN**, sélectionnez la version du Client VPN pour lequel vous créez le tunnel[1][2][3].

[1] Si vous souhaitez utiliser les mêmes paramètres pour des terminaux équipés avec des Clients VPN TheGreenBow de versions différentes, vous devez dupliquer le tunnel autant de fois que vous avez de versions différentes de Clients VPN TheGreenBow.
[2] Si vous souhaitez créer un tunnel en mode IPsec DR, reportez-vous à la section 5.2.1.3.
[3] Si vous souhaitez créer un tunnel doté d'une cryptographie résistante au quantique, reportez-vous à la section 5.2.1.4.

Une fois la version sélectionnée, vous ne pourrez plus la modifier pour ce tunnel. En revanche, vous pourrez dupliquer le tunnel et choisir une version supérieure. Pour créer un tunnel identique ou similaire pour une version antérieure des Clients VPN, vous devez créer un nouveau tunnel.

4. Cliquez sur **CRÉER**.

   La page **Créer un tunnel IPsec/IKEv2** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :



Une vignette indiquant la version du Client VPN pour lequel vous créez un tunnel s'affiche à droite du titre de la page. Celle-ci se retrouve également dans la colonne **Version** de la liste des tunnels.

5. Dans le champ **Nom du tunnel**, saisissez le nom que vous souhaitez attribuer au tunnel.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

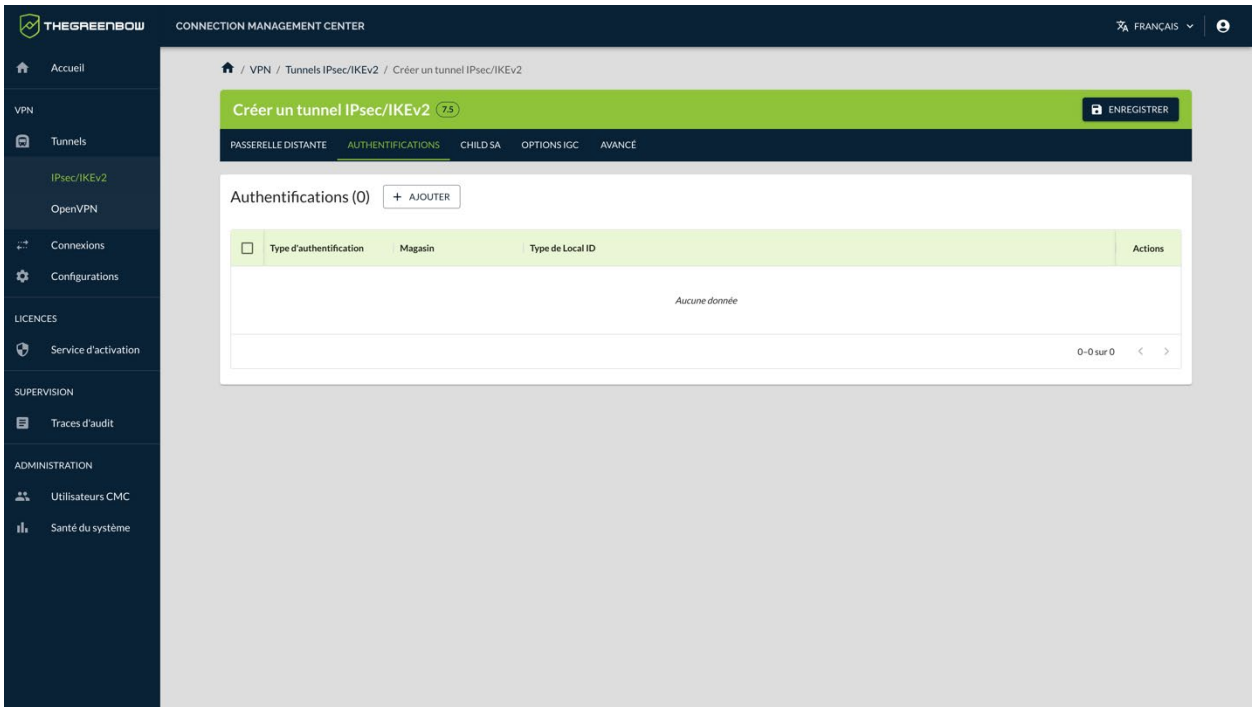
6. Saisissez l'adresse de la passerelle VPN distante dans le champ **Adresse de la passerelle**. La valeur saisie peut prendre la forme d'une adresse IP (IPv6 ou IPv4) ou d'une adresse DNS.
7. La case **Obtenir la configuration depuis la passerelle** est cochée par défaut. Cette option permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN : adresse du Client VPN, adresse réseau distant, masque réseau et adresses DNS. Décochez la case si vous préférez renseigner manuellement ces informations dans la configuration.
8. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.

Si vous cliquez sur le bouton **ENREGISTRER** avant d'avoir renseigné tous les champs obligatoires repérés par un astérisque, un message vous avertit qu'il manque des données, un triangle d'avertissement rouge s'affiche à côté du nom des tous les onglets dans lesquels il manque des informations et les champs concernés s'affichent en rouge avec un message correspondant.

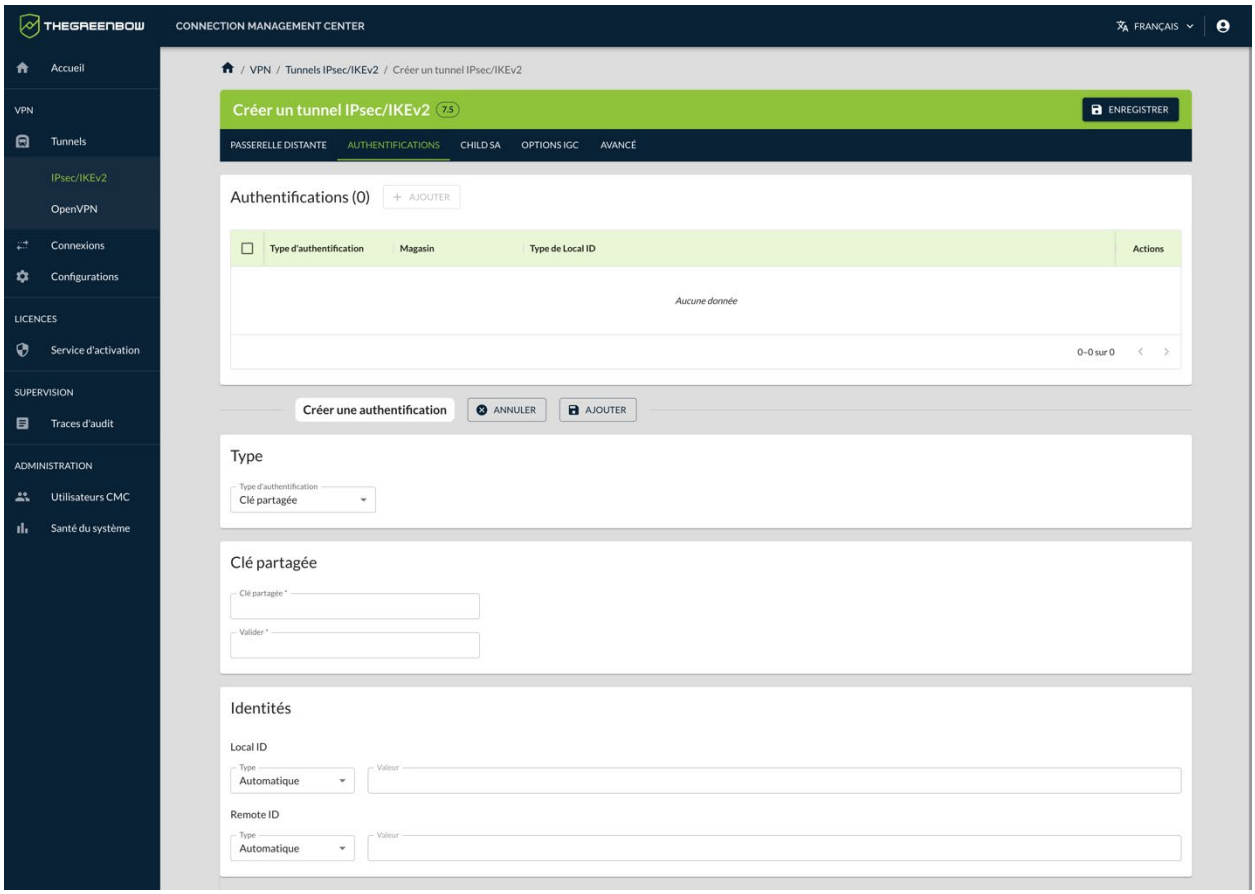
Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **PASSERELLE DISTANTE**.

9. Passez à l'onglet **AUTHENTIFICATIONS**.



10. Cliquez sur le bouton **+ AJOUTER**. Le volet **Créer une authentification** se développe sous la liste des authentifications du tunnel.



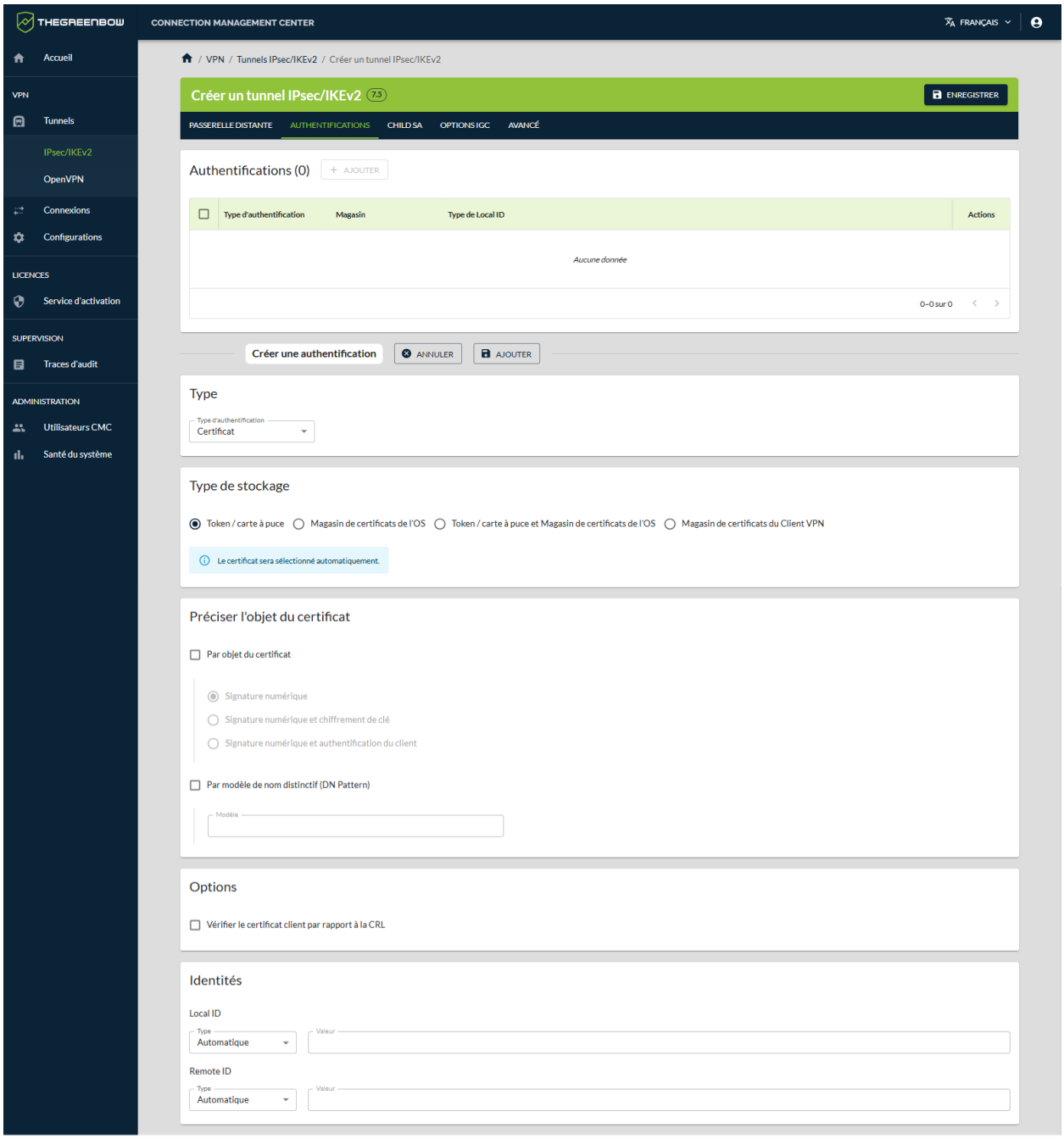
11. Dans la liste déroulante **Type d'authentification**, sélectionnez le type souhaité: **Clé partagée**, **Certificat** ou **EAP**. Les blocs et champs de saisie s'adaptent en fonction du type sélectionné.

☞ Pour comprendre la différence entre les trois modes d'authentification, reportez-vous à la section 2.7 Quel mode d'authentification choisir pour le client ?

Il est recommandé de privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats du système d'exploitation.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATIONS**.

Dans la suite de cet exemple de création d'un tunnel, nous allons poursuivre avec un certificat stocké sur support amovible.



12. Sous la rubrique **Type de stockage**, l'option **Token / carte à puce** est sélectionnée par défaut. Le cas échéant, choisissez un autre type de stockage. Le certificat sera sélectionné automatiquement.
13. Vous pouvez laisser tous les autres champs de l'onglet **AUTHENTIFICATIONS** définis à leur valeur par défaut ou les modifier selon vos besoins.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATIONS**.

14. Cliquez sur le bouton **Ajouter** à côté du bandeau **Créer une authentification**.

L'authentification est ajoutée à la liste des authentifications du tunnel et le volet **Créer une authentification** se referme.

15. Vous pouvez ajouter une ou plusieurs autres authentifications, en fonction du type d'authentification sélectionné.

Les combinaisons possibles sont les suivantes :
- clé partagée,
- certificat,
- EAP,
- certificat + EAP,
- certificats multiples.

16. À ce stade, vous pouvez enregistrer le tunnel. Nous vous invitons néanmoins à passer en revue les réglages des onglets **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

17. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page.

    Le tunnel est ajouté à la liste des **Tunnels IPsec/IKEv2** qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la création du tunnel IPsec/IKEv2. Vous pouvez poursuivre avec les étapes suivantes :

- Pour créer une connexion, reportez-vous à la section 5.3.1 Créer une connexion.
- Pour modifier le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.2.1 Modifier un tunnel IPsec/IKEv2.
- Pour dupliquer le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.3 Dupliquer un tunnel.
- Pour supprimer le tunnel que vous venez de créer, reportez-vous à la section 5.2.4 Supprimer un tunnel.
- Pour créer un tunnel en mode IPsec DR, reportez-vous à la section 5.2.1.3 Créer un tunnel IPsec/IKEv2 en mode DR.
- Pour créer un tunnel doté d'une cryptographie résistante au quantique, reportez-vous à la section 5.2.1.4 Créer un tunnel 1.0 QS.
- Pour créer un tunnel OpenVPN, reportez-vous à la section 5.2.1.5 Créer un tunnel OpenVPN.

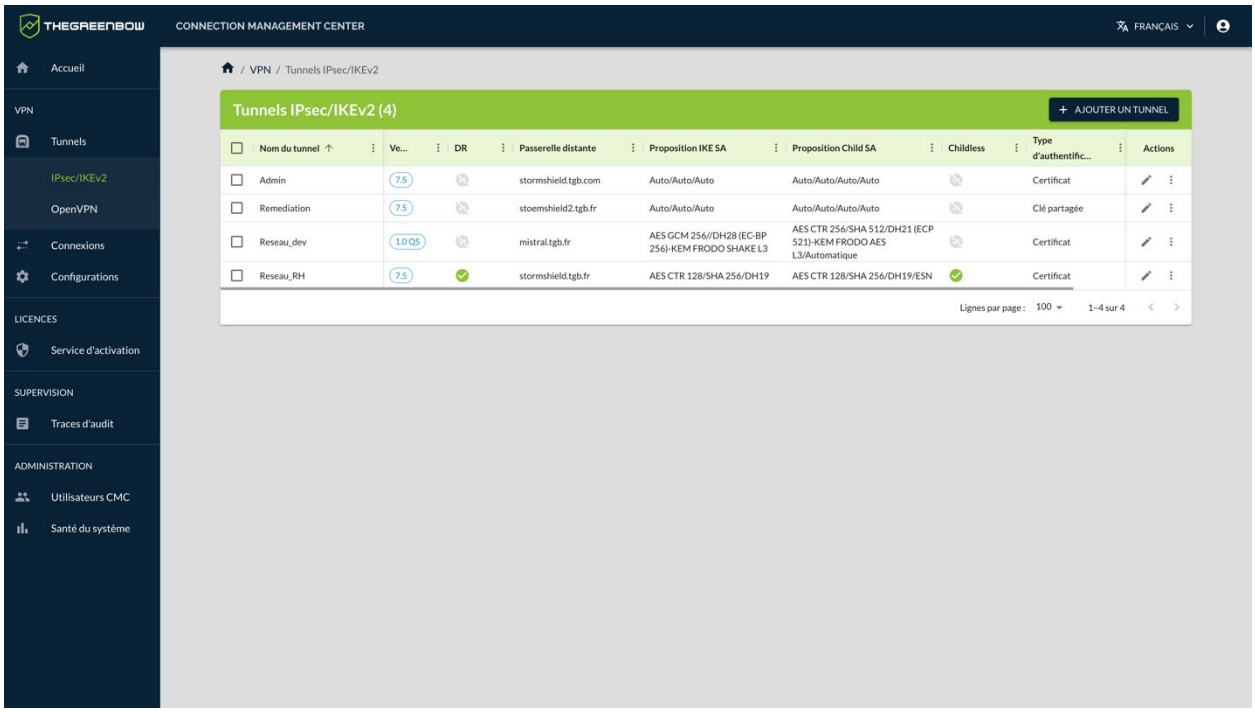
5.2.1.3 Créer un tunnel IPsec/IKEv2 en mode DR

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour créer un tunnel IPsec/IKEv2 en mode DR, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **IPsec/IKEv2**.

La liste des tunnels IPsec/IKEv2 s'affiche :

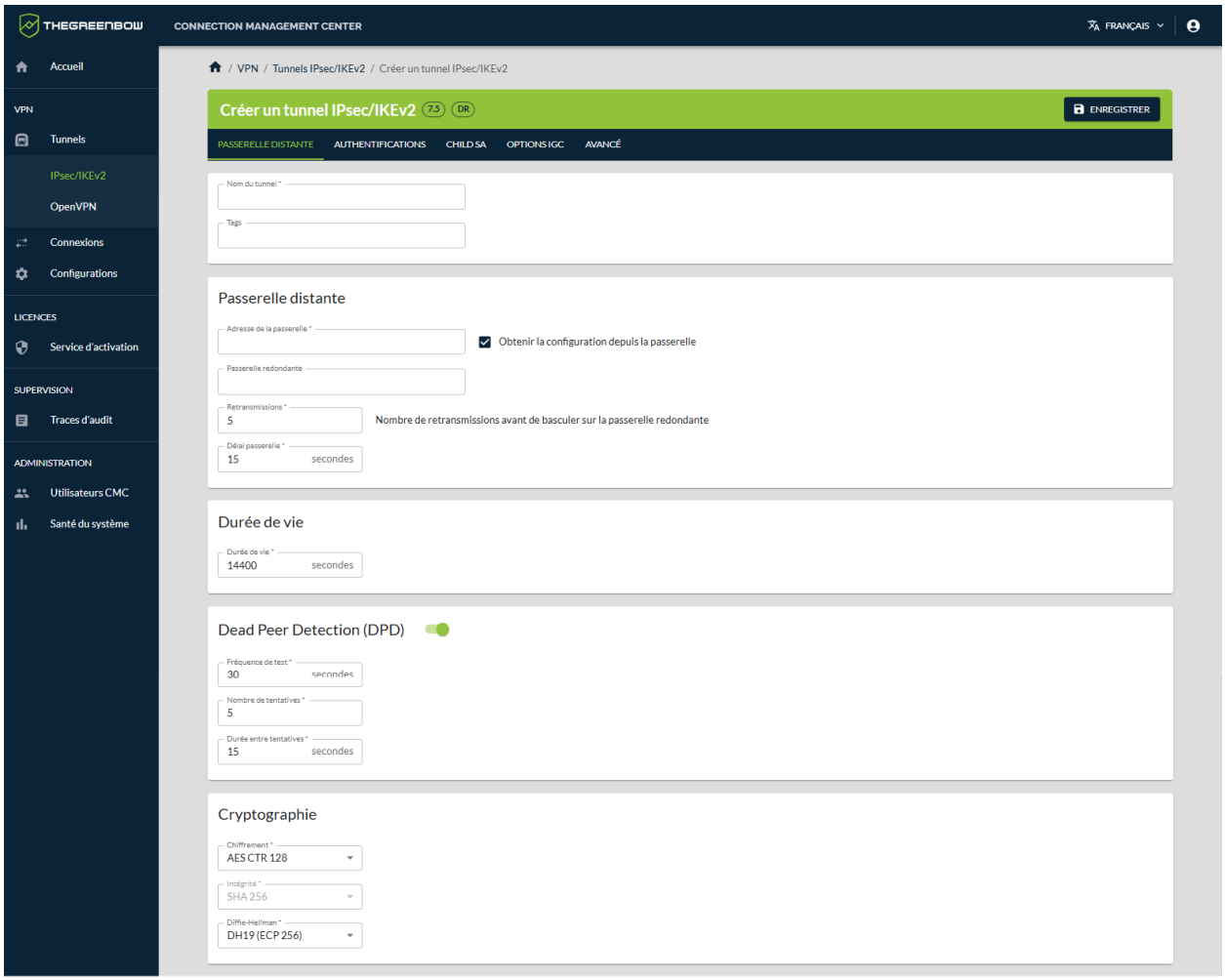


2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UN TUNNEL**. La boîte de dialogue **Créer un tunnel** s'affiche.
3. Dans la liste déroulante **Version du Client VPN**, sélectionnez la version 7.5 du Client VPN Windows Enterprise[1].
4. Cliquez sur le bouton bascule **Activer le mode DR**.

5. Cliquez sur **CRÉER**.

[1] Seul le Client VPN Windows Enterprise v7.5 prend en charge le mode IPsec DR.

La page **Créer un tunnel IPsec/IKEv2** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :



Une vignette 7.5 et une vignette DR s'affichent à droite du titre de la page. Celles-ci se retrouvent également dans la colonne **Version** de la liste des tunnels.

6. Dans le champ **Nom du tunnel**, saisissez le nom que vous souhaitez attribuer au tunnel.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

7. Saisissez l'adresse de la passerelle VPN distante dans le champ **Adresse de la passerelle**. La valeur saisie peut prendre la forme d'une adresse IP (IPv6 ou IPv4) ou d'une adresse DNS.
8. La case **Obtenir la configuration depuis la passerelle** est cochée par défaut. Cette option permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN :

adresse du Client VPN, adresse réseau distant, masque réseau et adresses DNS. Décochez la case si vous préférez renseigner manuellement ces informations dans la configuration.

9. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.

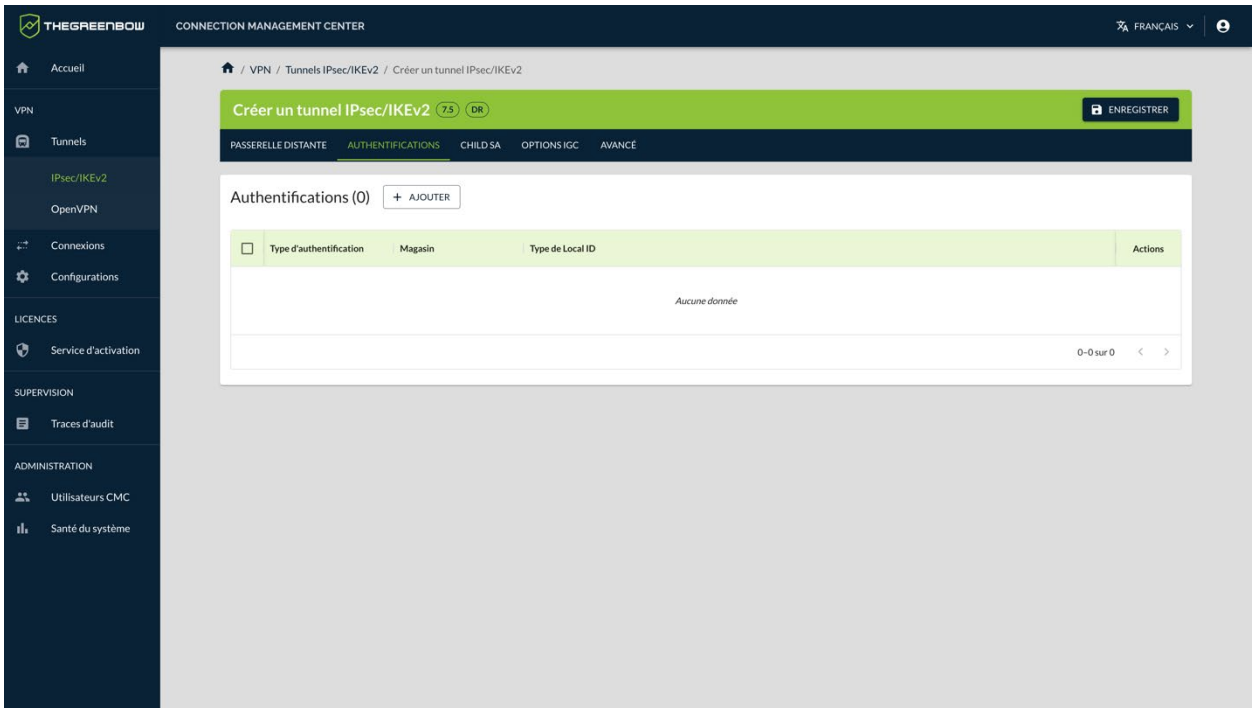
Les paramètres de cryptographie disponibles sont limités aux seules options disponibles pour le mode DR.

Si vous cliquez sur le bouton **ENREGISTRER** avant d'avoir renseigné tous les champs obligatoires repérés par un astérisque, un message vous avertit qu'il manque des données, un triangle d'avertissement rouge s'affiche à côté du nom des tous les onglets dans lesquels il manque des informations et les champs concernés s'affichent en rouge avec un message correspondant.

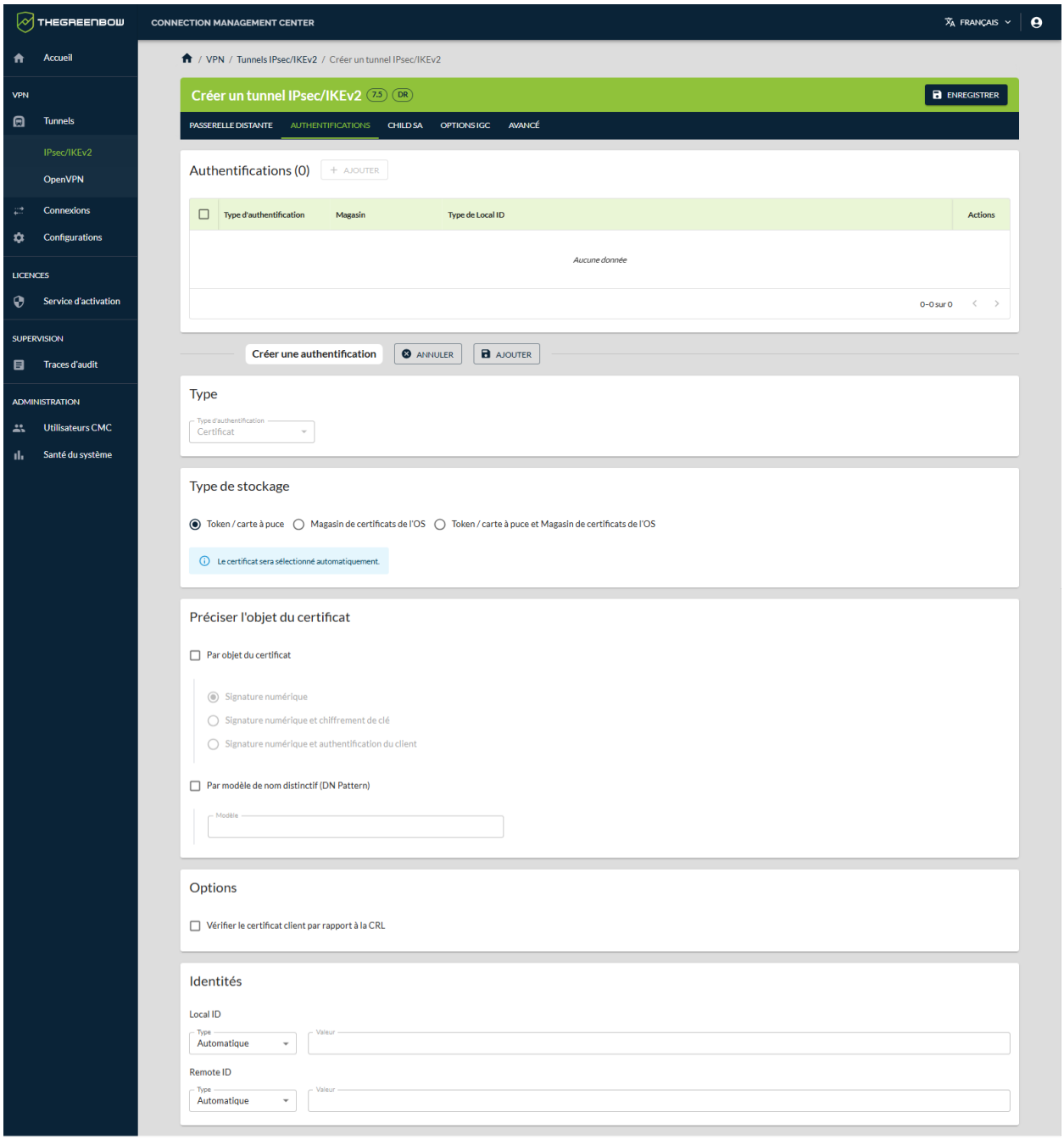
Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **PASSERELLE DISTANTE**.

10. Passez à l'onglet **AUTHENTIFICATIONS**.



11. Cliquez sur le bouton **+ AJOUTER**. Le volet **Créer une authentification** se développe sous la liste des authentifications du tunnel.



La liste déroulante **Type d'authentification** est grisée et l'option **Certificat** est sélectionnée, car c'est le seul type d'authentification autorisé en mode DR.

12. Sous la rubrique **Type de stockage**, sélectionnez l'emplacement à partir duquel le certificat doit être sélectionné. Le certificat sera sélectionné automatiquement.
13. Vous pouvez laisser tous les autres champs de l'onglet **AUTHENTIFICATIONS** définis à leur valeur par défaut ou les modifier selon vos besoins.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATIONS**.

14. Cliquez sur le bouton **Ajouter** à côté du bandeau **Créer une authentification**.

L'authentification est ajoutée à la liste des authentifications du tunnel et le volet **Créer une authentification** se referme.

Le mode DR n'admet pas d'authentification multiple.

15. À ce stade, vous pouvez enregistrer le tunnel. Nous vous invitons néanmoins à passer en revue les réglages des onglets **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

16. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est ajouté à la liste des **Tunnels IPsec/IKEv2** qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la création du tunnel IPsec/IKEv2 en mode DR. Vous pouvez poursuivre avec les étapes suivantes :

- Pour créer une connexion, reportez-vous à la section 5.3.1 Créer une connexion.
- Pour modifier le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.2.1 Modifier un tunnel IPsec/IKEv2.
- Pour dupliquer le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.3 Dupliquer un tunnel.
- Pour supprimer le tunnel que vous venez de créer, reportez-vous à la section 5.2.4 Supprimer un tunnel.
- Pour créer un tunnel doté d'une cryptographie résistante au quantique, reportez-vous à la section 5.2.1.4 Créer un tunnel 1.0 QS.
- Pour créer un tunnel OpenVPN, reportez-vous à la section 5.2.1.5 Créer un tunnel OpenVPN.

5.2.1.4 Créer un tunnel 1.0 QS

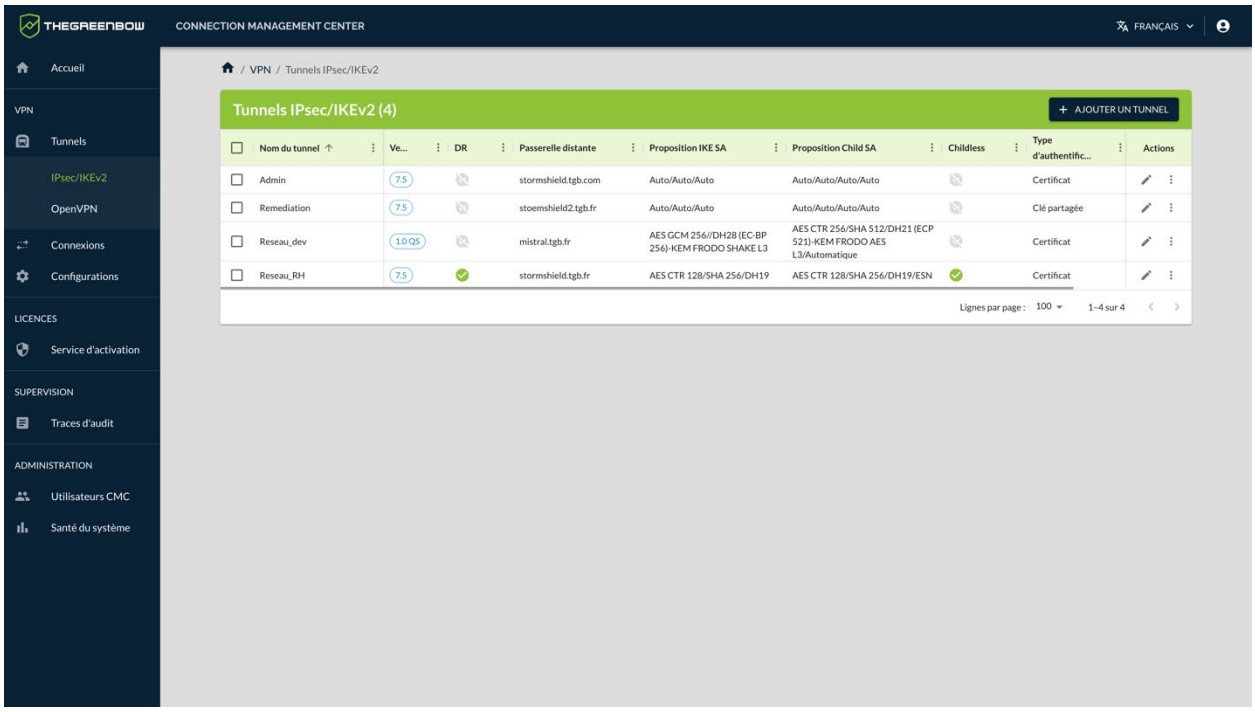
Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour créer un tunnel pour le Client VPN Quantum Safe v1.0, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **IPsec/IKEv2**.

Le Client VPN Quantum Safe v1.0 prend uniquement en charge les tunnels IPsec/IKEv2. Il n'est pas possible de créer un tunnel OpenVPN résistant au quantique pour le Client VPN Quantum Safe v1.0.

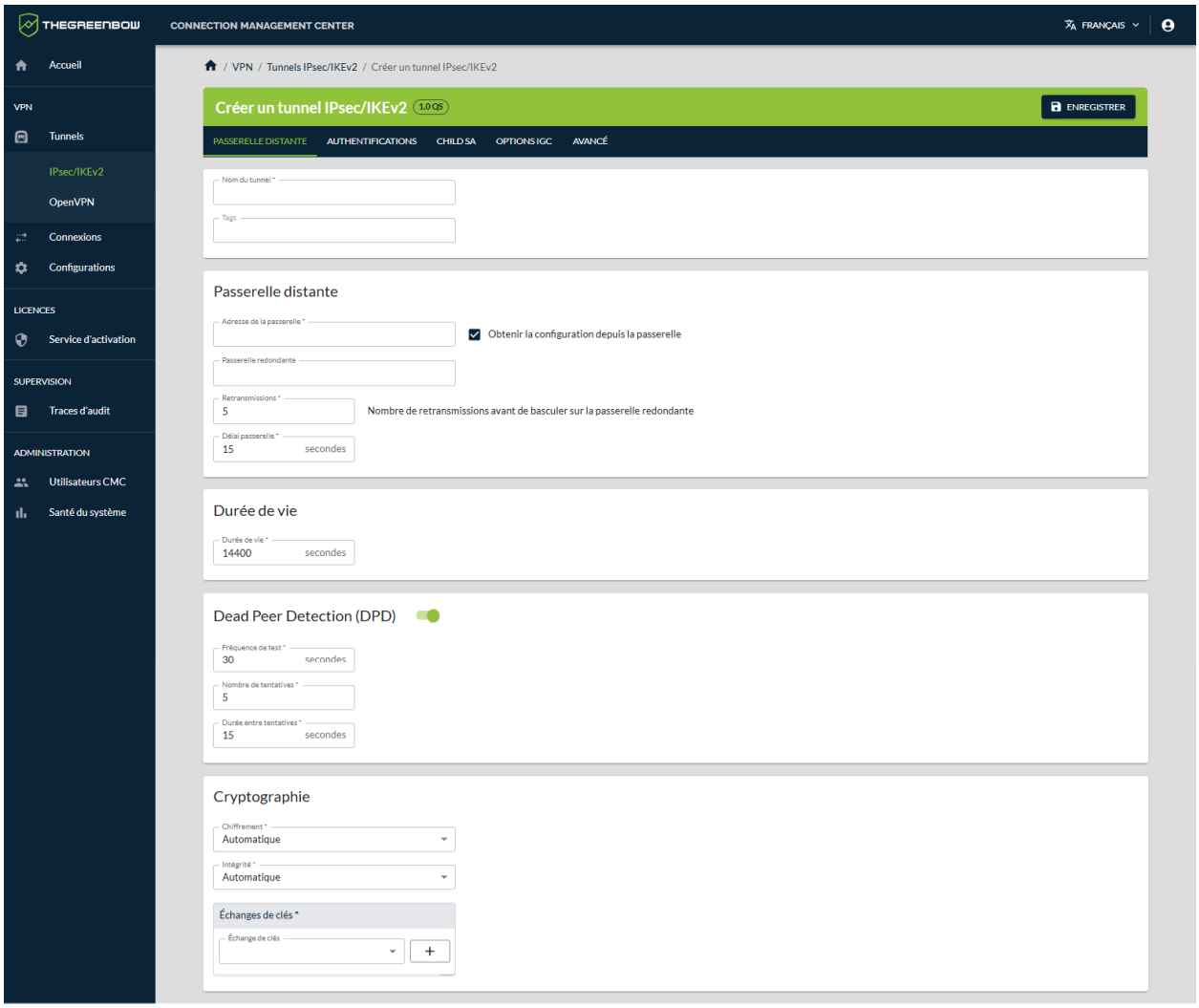
La liste des tunnels IPsec/IKEv2 s'affiche :



2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UN TUNNEL**. La boîte de dialogue **Créer un tunnel** s'affiche.
3. Dans la liste déroulante **Version du Client VPN**, sélectionnez la version **1.0 QS**.

4. Cliquez sur **CRÉER**.

   La page **Créer un tunnel IPsec/IKEv2** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :

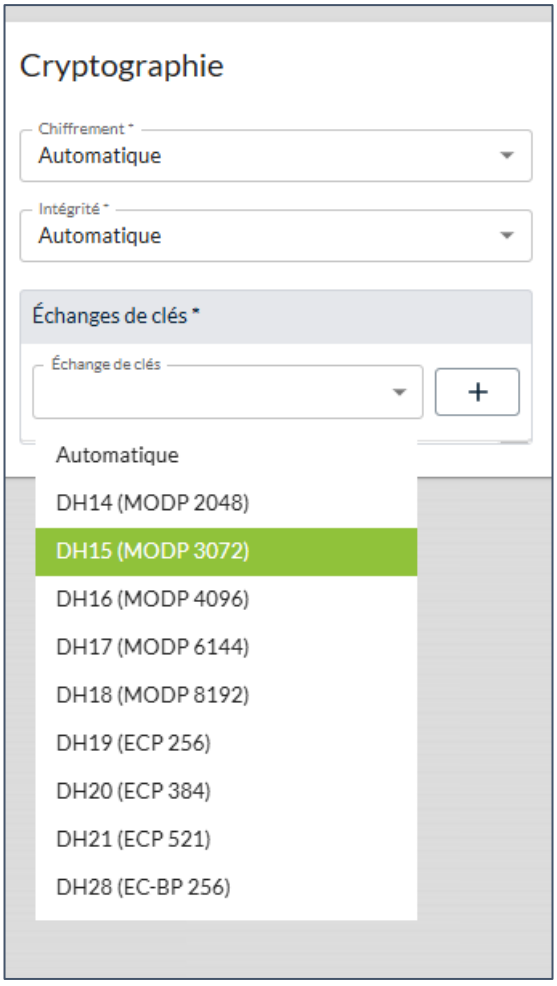


Une vignette **1.0 QS** s'affiche à droite du titre de la page. Celle-ci se retrouve également dans la colonne **Version** de la liste des tunnels.

5. Dans le champ **Nom du tunnel**, saisissez le nom que vous souhaitez attribuer au tunnel.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

6. Saisissez l'adresse de la passerelle VPN distante dans le champ **Adresse de la passerelle**. La valeur saisie peut prendre la forme d'une adresse IP (IPv6 ou IPv4) ou d'une adresse DNS.
7. La case **Obtenir la configuration depuis la passerelle** est cochée par défaut. Cette option permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN : adresse du Client VPN, adresse réseau distant, masque réseau et adresses DNS. Décochez la case si vous préférez renseigner manuellement ces informations dans la configuration.
8. Dans le bloc **Cryptographie**, renseignez un échange de clés. Pour cela, sélectionnez un groupe Diffie-Hellman de votre choix dans la liste déroulante **Échange de clés**.



Le premier échange de clés doit obligatoirement être basé sur une cryptographie classique. Vous pouvez vous satisfaire de cet échange ou ajouter un deuxième échange qui, lui, fait appel à l'un des nouveaux algorithmes post-quantiques CRYSTALS-Kyber KEM, FrodoKEM AES ou FrodoKEM SHAKE (voir section 2.12 Algorithmes d'échange de clés post-quantiques, quelles différences ?). Vous pouvez ajouter autant d'échanges de clés que vous le souhaitez. Dès lors que vous avez ajouté plus de deux échanges de clés, vous pouvez changer l'ordre dans la liste, sauf pour le premier qui doit toujours être un échange de clés Diffie-Hellman.

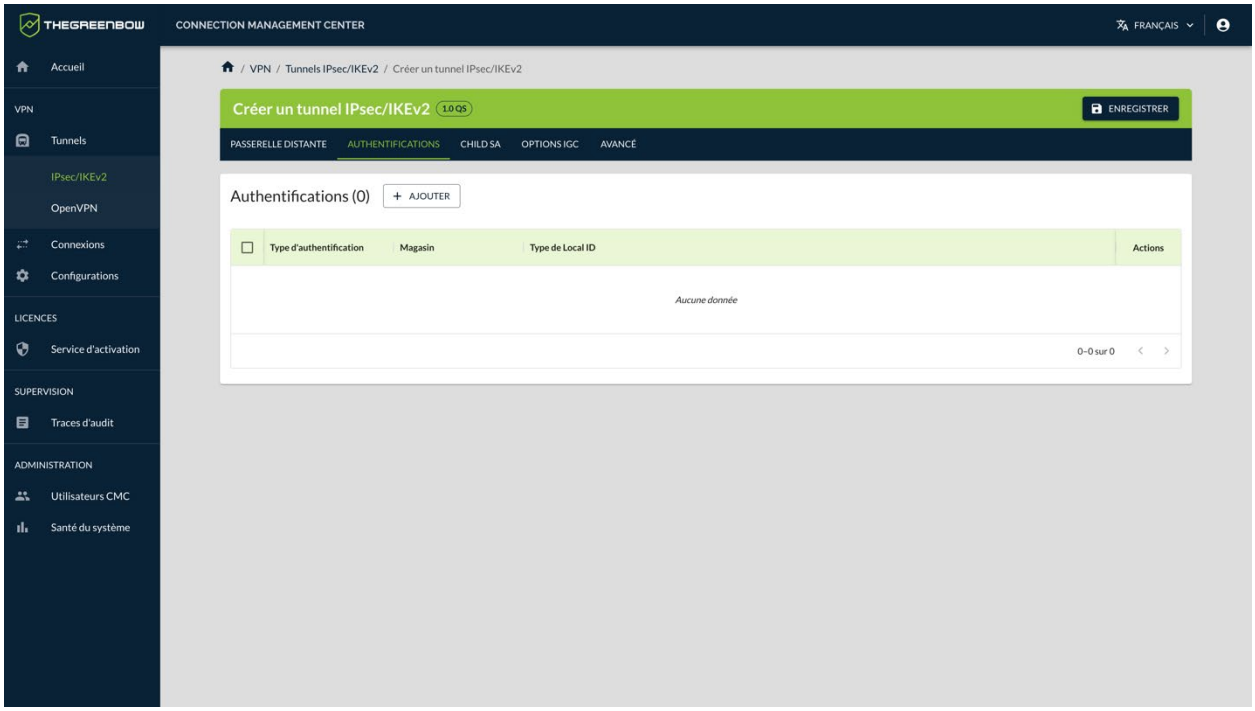
9. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.

Si vous cliquez sur le bouton **ENREGISTRER** avant d'avoir renseigné tous les champs obligatoires repérés par un astérisque, un message vous avertit qu'il manque des données, un triangle d'avertissement rouge s'affiche à côté du nom des tous les onglets dans lesquels il manque des informations et les champs concernés s'affichent en rouge avec un message correspondant.

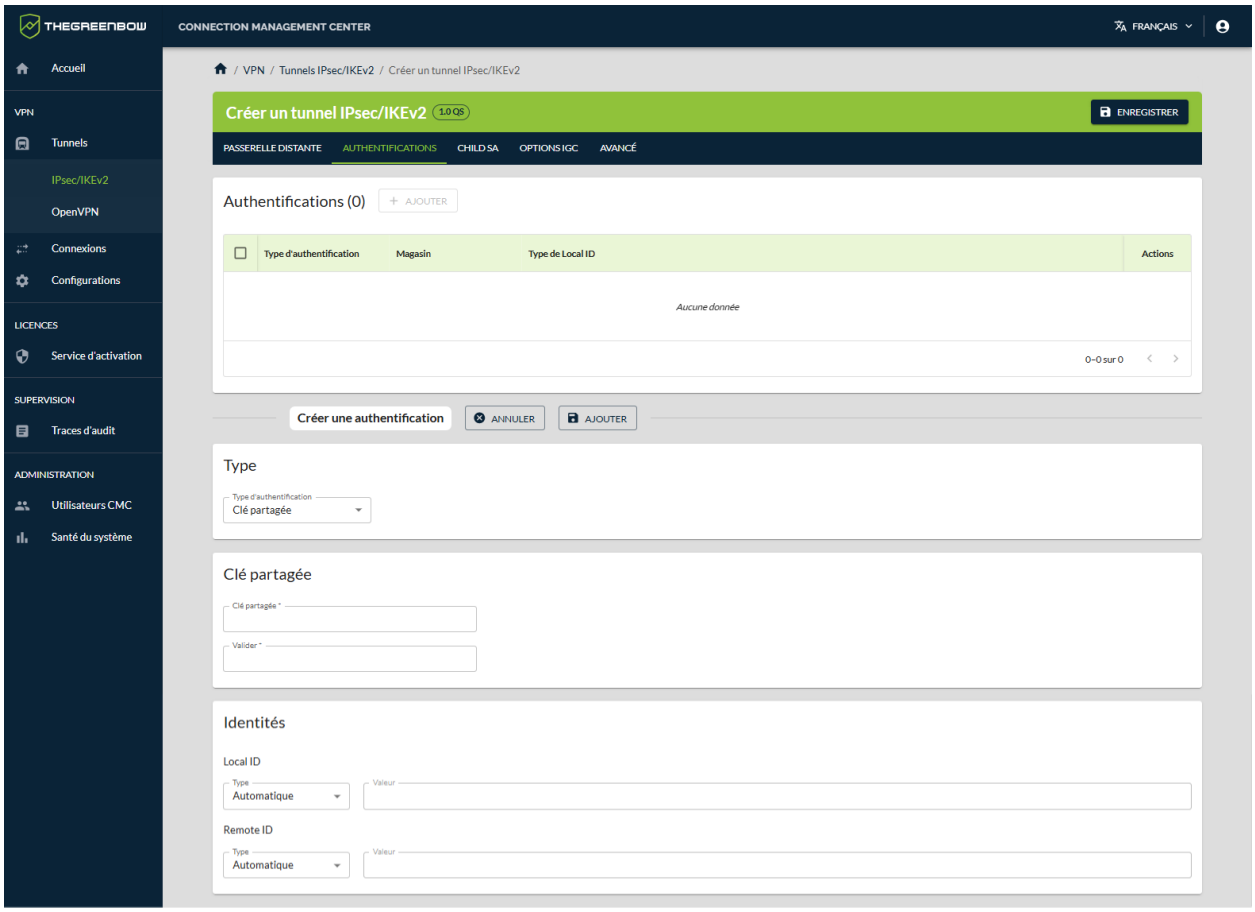
Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **PASSERELLE DISTANTE**.

10. Passez à l'onglet **AUTHENTIFICATIONS**.



11. Cliquez sur le bouton **+ AJOUTER**. Le volet **Créer une authentification** se développe sous la liste des authentifications du tunnel.



12. Dans la liste déroulante **Type d'authentification**, sélectionnez le type souhaité: **Clé partagée**, **Certificat** ou **EAP**. Les blocs et les champs de saisie s'adaptent en fonction du type sélectionné.

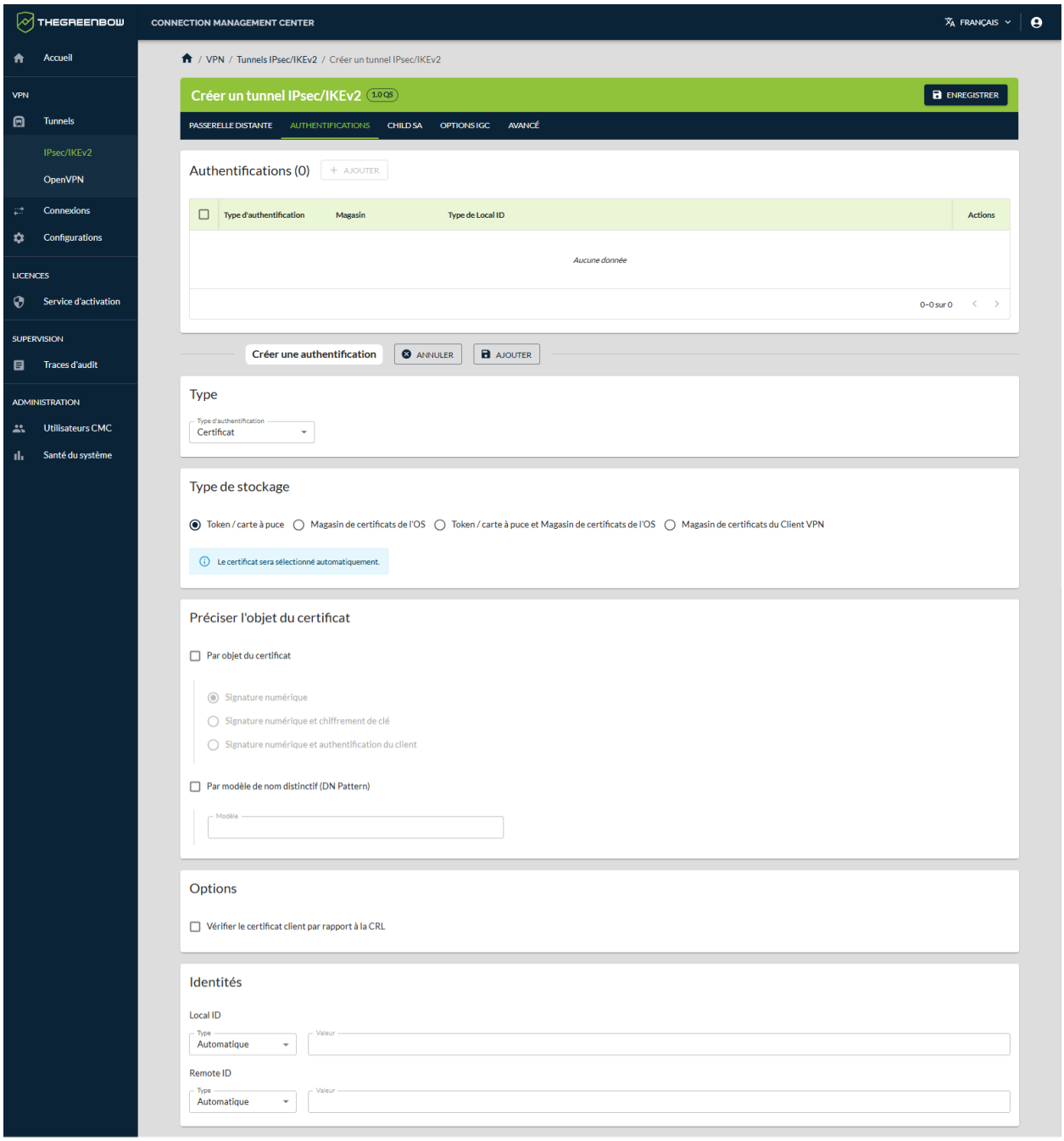
☞ Pour comprendre la différence entre les trois modes d'authentification, reportez-vous à la section 2.7 Quel mode d'authentification choisir pour le client ?

Il est recommandé de privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats du système d'exploitation.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATIONS**.

Dans la suite de cet exemple de création d'un tunnel, nous allons poursuivre avec un certificat stocké sur support amovible.

13. Sous la rubrique **Type de stockage**, sélectionnez l'option **Token / carte à puce**. Le cas échéant, choisissez un autre type de stockage.



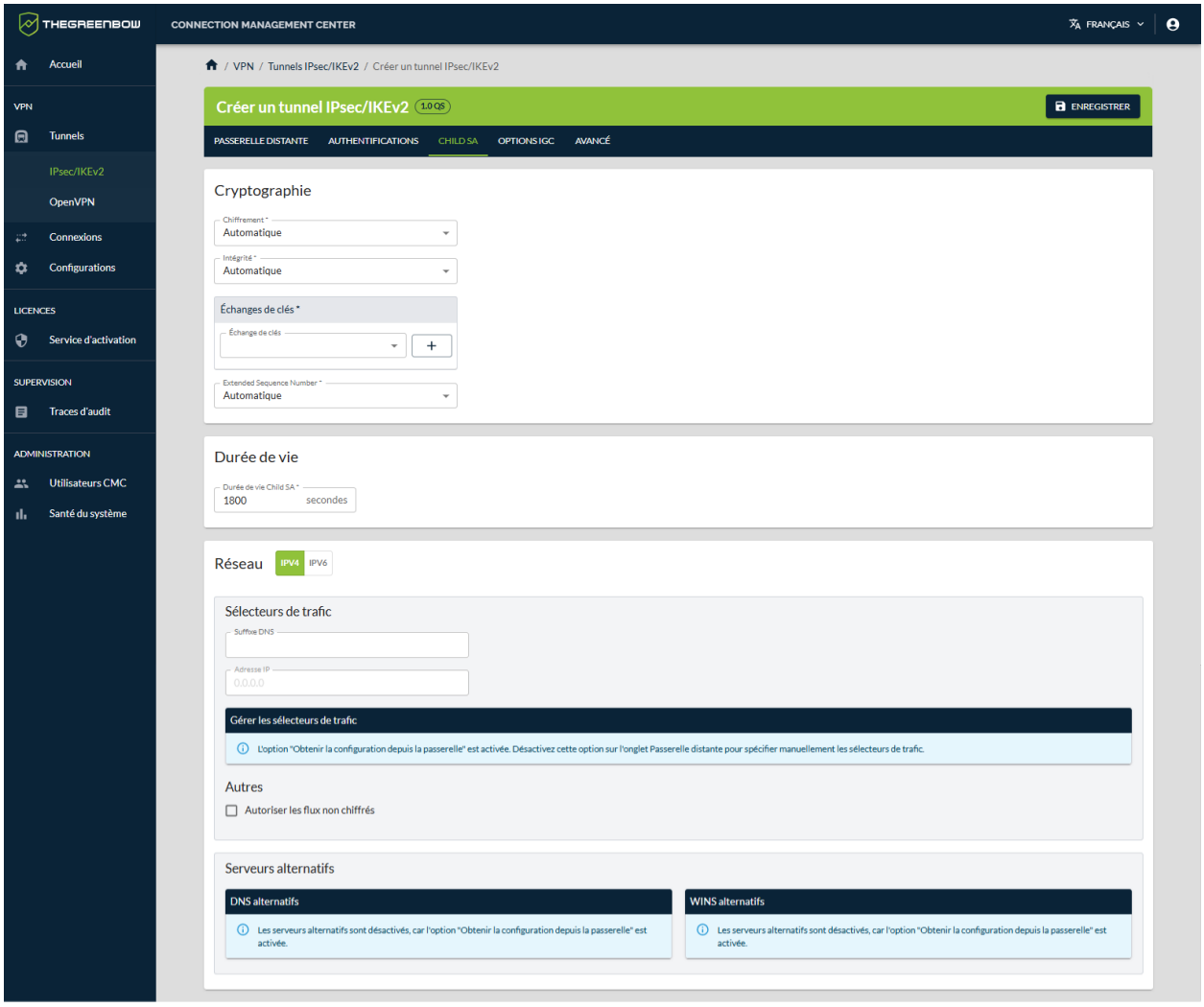
14. Vous pouvez laisser tous les autres champs de l'onglet **AUTHENTIFICATIONS** définis à leur valeur par défaut ou les modifier selon vos besoins.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATIONS**.

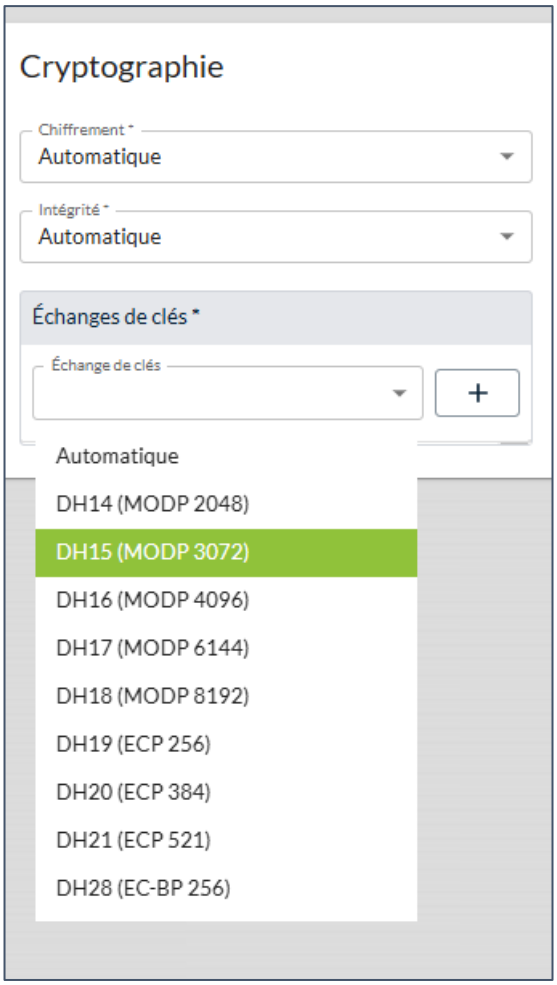
15. Cliquez sur le bouton **Ajouter** à côté du bandeau **Créer une authentification**.

L'authentification est ajoutée à la liste des authentifications du tunnel et le volet **Créer une authentification** se referme.

16. Passez à l'onglet **CHILD SA**.



17. Dans le bloc **Cryptographie**, renseignez un échange de clés. Pour cela, sélectionnez un groupe Diffie-Hellman de votre choix dans la liste déroulante **Échange de clés**.



Le premier échange de clés doit obligatoirement être basé sur une cryptographie classique. Vous pouvez vous satisfaire de cet échange ou ajouter un deuxième échange qui, lui, fait appel à l'un des nouveaux algorithmes post-quantiques CRYSTALS-Kyber KEM, FrodoKEM AES ou FrodoKEM SHAKE (voir section 2.12 Algorithmes d'échange de clés post-quantiques, quelles différences ?). Vous pouvez ajouter autant d'échanges de clés que vous le souhaitez. Dès lors que vous avez ajouté plus de deux échanges de clés, vous pouvez changer l'ordre dans la liste, sauf pour le premier qui doit toujours être un échange de clés Diffie-Hellman.

18. À ce stade, vous pouvez enregistrer le tunnel. Nous vous invitons néanmoins à passer en revue les réglages des onglets **OPTIONS IGC** et **AVANCÉ**.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

19. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page.

Le tunnel est ajouté à la liste des **Tunnels IPsec/IKEv2** qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la création du tunnel IPsec/IKEv2 pour Client VPN Quantum Safe v1.0. Vous pouvez poursuivre avec les étapes suivantes :

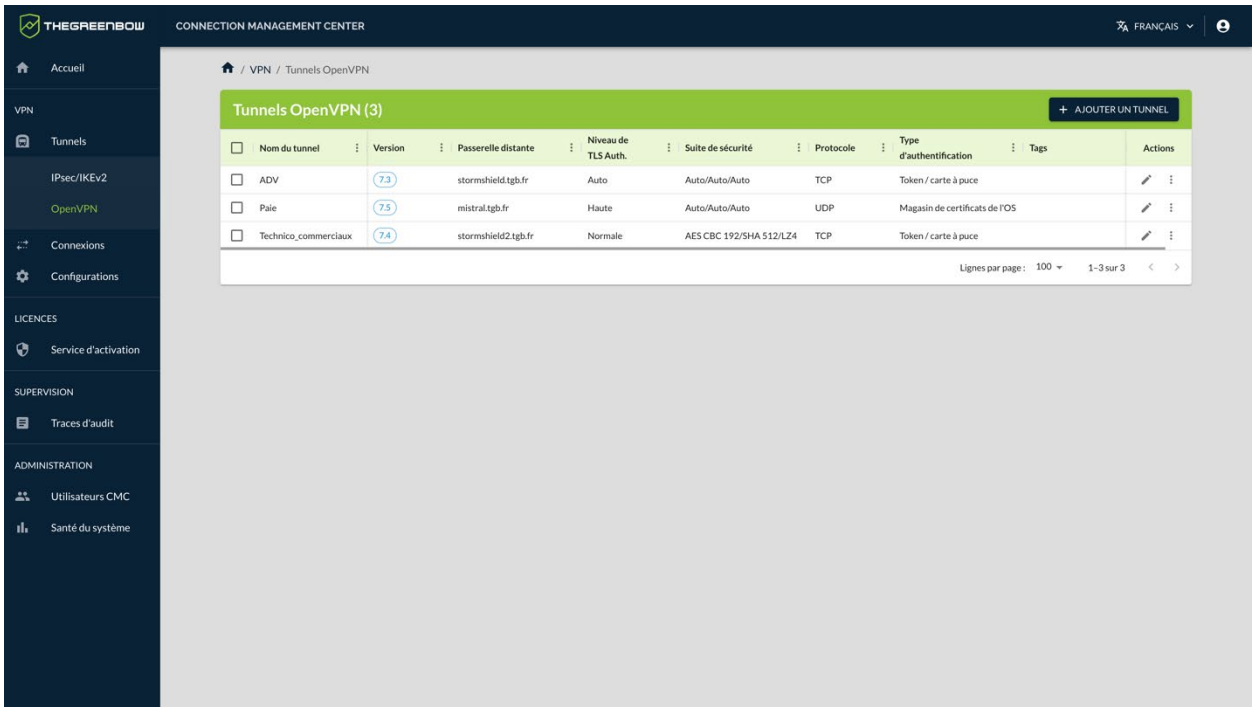
- Pour créer une connexion, reportez-vous à la section 5.3.1 Créer une connexion.
- Pour modifier le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.2.1 Modifier un tunnel IPsec/IKEv2.
- Pour dupliquer le tunnel IPsec/IKEv2 que vous venez de créer, reportez-vous à la section 5.2.3 Dupliquer un tunnel.
- Pour supprimer le tunnel que vous venez de créer, reportez-vous à la section 5.2.4 Supprimer un tunnel.
- Pour créer un tunnel en mode IPsec DR, reportez-vous à la section 5.2.1.3 Créer un tunnel IPsec/IKEv2 en mode DR.
- Pour créer un tunnel OpenVPN, reportez-vous à la section 5.2.1.5 Créer un tunnel OpenVPN.

5.2.1.5 Créer un tunnel OpenVPN

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour créer un tunnel OpenVPN, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **OpenVPN**. La liste des tunnels OpenVPN s'affiche :



2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UN TUNNEL**. La boîte de dialogue **Créer un tunnel** s'affiche :

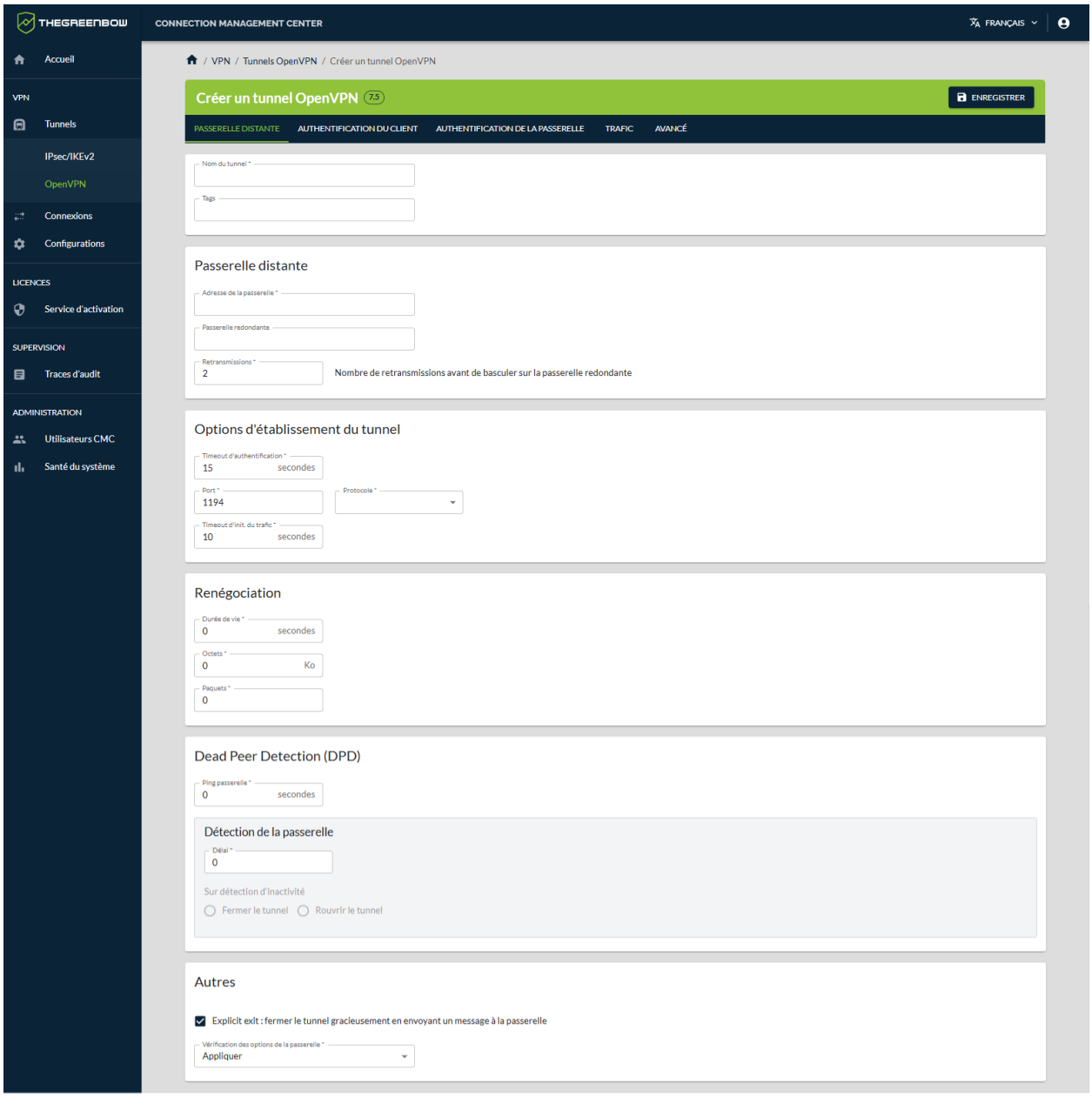
3. Dans la liste déroulante **Version du Client VPN**, sélectionnez la version du Client VPN pour lequel vous créez le tunnel[1][2][3].

Une fois la version sélectionnée, vous ne pourrez plus la modifier pour ce tunnel. En revanche, vous pourrez dupliquer le tunnel et choisir une version supérieure. Pour créer un tunnel identique pour une version antérieure du client VPN, vous devez créer un nouveau tunnel.

4. Cliquez sur **CRÉER**.

[1] Si vous souhaitez utiliser les mêmes paramètres pour des terminaux équipés avec des Clients VPN TheGreenBow de versions différentes, vous devez dupliquer le tunnel autant de fois que vous avez de versions différentes de Clients VPN TheGreenBow.
[2] Si vous souhaitez créer un tunnel en mode IPsec DR, reportez-vous à la section 5.2.1.3.
[3] Si vous souhaitez créer un tunnel doté d'une cryptographie résistante au quantique, reportez-vous à la section 5.2.1.4.

La page **Créer un tunnel OpenVPN** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :



5. Dans le champ **Nom du tunnel**, saisissez le nom que vous souhaitez attribuer au tunnel.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

6. Dans le bloc **Passerelle distante**, saisissez l'adresse de la passerelle VPN distante dans le champ **Adresse de la passerelle**. La valeur saisie peut prendre la forme d'une adresse IP (IPv6 ou IPv4) ou d'une adresse DNS.

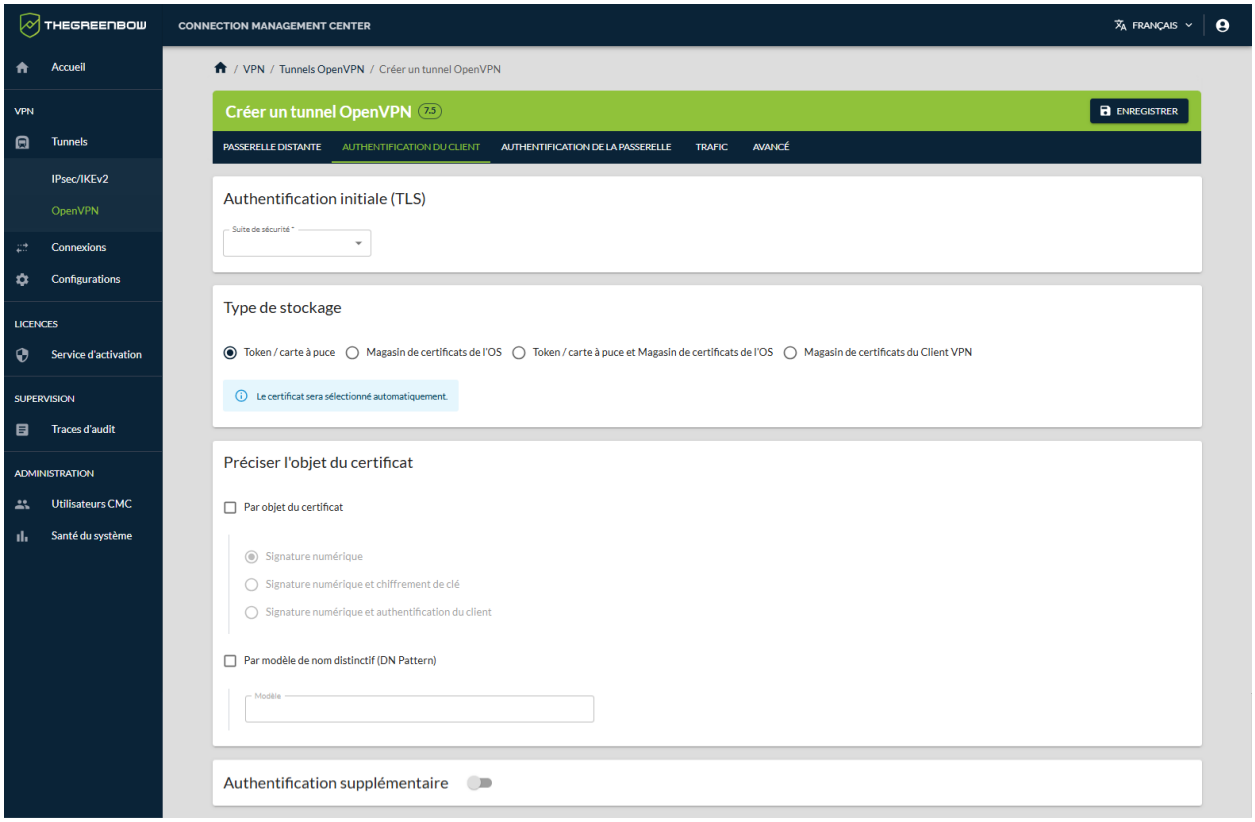
7. Dans le bloc **Options d'établissement du tunnel**, sélectionnez **TCP** ou **UDP** dans la liste déroulante **Protocole**.
8. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.

Si vous cliquez sur le bouton **ENREGISTRER** avant d'avoir renseigné tous les champs obligatoires repérés par un astérisque, un message vous avertit qu'il manque des données, un triangle d'avertissement rouge s'affiche à côté du nom des tous les onglets dans lesquels il manque des informations et les champs concernés s'affichent en rouge avec un message correspondant.

Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **PASSERELLE DISTANTE**.

9. Passez à l'onglet **AUTHENTIFICATION DU CLIENT**.

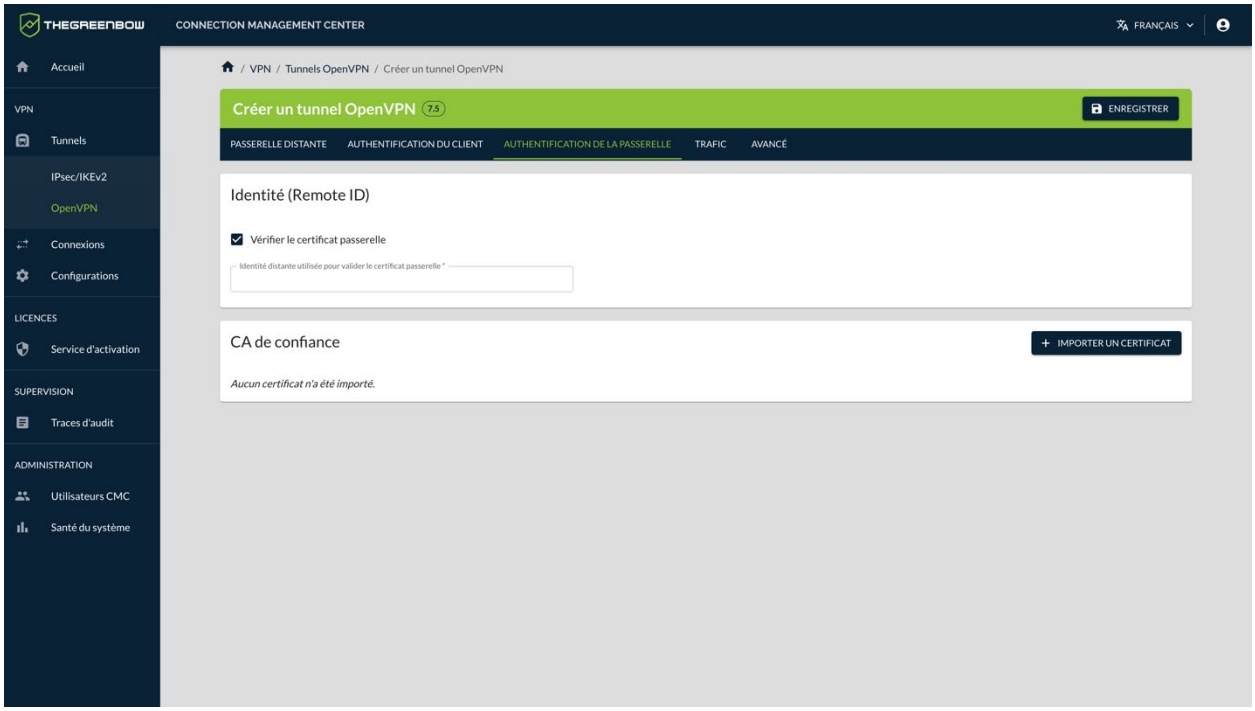


10. Dans le bloc **Authentification initiale (TLS)**, sélectionnez le niveau de sécurité de la phase d'authentification dans l'échange SSL dans la liste déroulante **Suite de sécurité**.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **AUTHENTIFICATION DU CLIENT**.

Dans la suite de cet exemple de création d'un tunnel, nous allons poursuivre avec une authentification initiale automatique.

11. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.
12. Passez à l'onglet **AUTHENTIFICATION DE LA PASSERELLE**.



13. Dans le bloc **Identité (Remote ID)**, la case **Vérifier le certificat passerelle** est cochée par défaut. Si vous souhaitez conserver ce réglage, vous devez renseigner l'identité distante utilisée pour valider le certificat passerelle dans la zone prévue à cet effet. Il s'agit ici du sujet du certificat de la passerelle. Sinon, décochez la case. Dans ce cas, la PKI n'est pas vérifiée.
14. Vous pouvez laisser tous les autres champs définis à leur valeur par défaut ou les modifier selon vos besoins.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **AUTHENTIFICATION DE LA PASSERELLE**, **TRAFIC** et **AVANCÉ**.

15. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est ajouté à la liste des **Tunnels OpenVPN** qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la création du tunnel OpenVPN. Vous pouvez poursuivre avec les étapes suivantes :

- Pour créer une connexion, reportez-vous à la section 5.3.1 Créer une connexion.
- Pour modifier le tunnel OpenVPN que vous venez de créer, reportez-vous à la section 5.2.2.2 Modifier un tunnel OpenVPN.
- Pour dupliquer le tunnel OpenVPN que vous venez de créer, reportez-vous à la section 5.2.3 Dupliquer un tunnel.
- Pour créer un tunnel IPsec/IKEv2, reportez-vous à la section 5.2.1.2 Créer un tunnel IPsec/IKEv2.

5.2.2 Modifier un tunnel

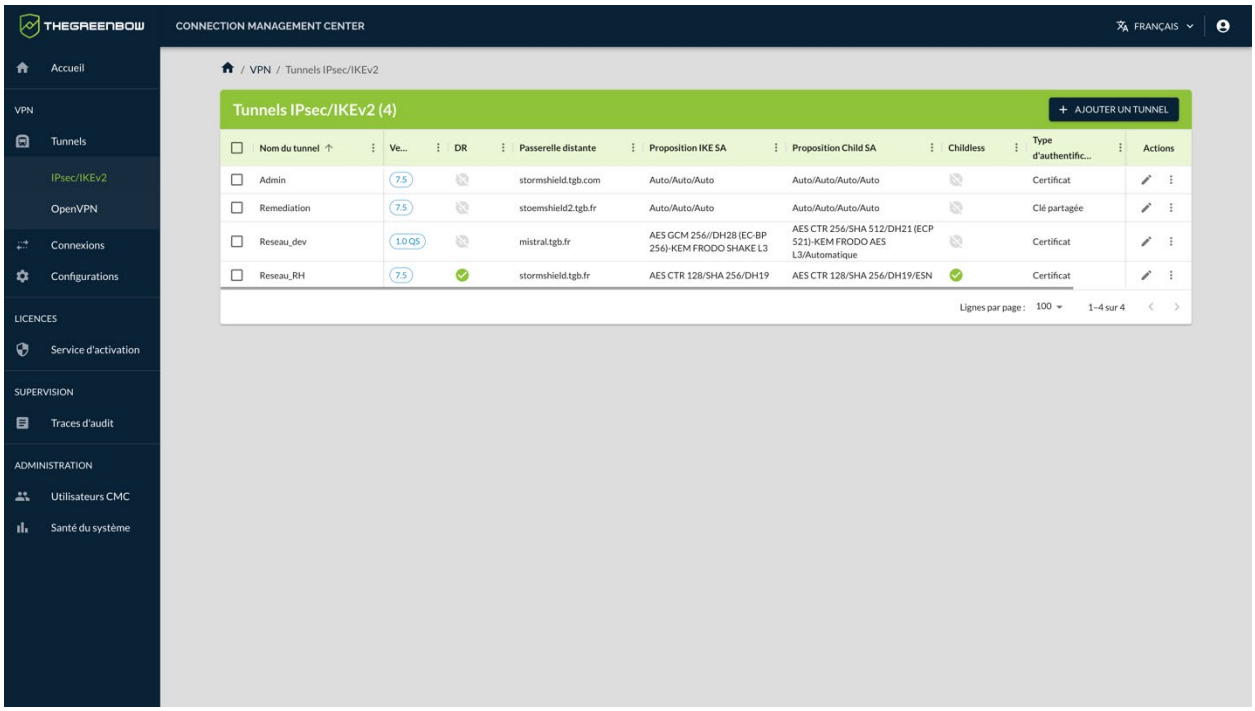
5.2.2.1 Modifier un tunnel IPsec/IKEv2

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à modifier les tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

La procédure de modification d'un tunnel est identique quel que soit le type de tunnel IPsec/IKEv2, qu'il soit standard, configuré en mode DR ou pour le Client VPN Quantum Safe. Seules les options disponibles diffèrent.

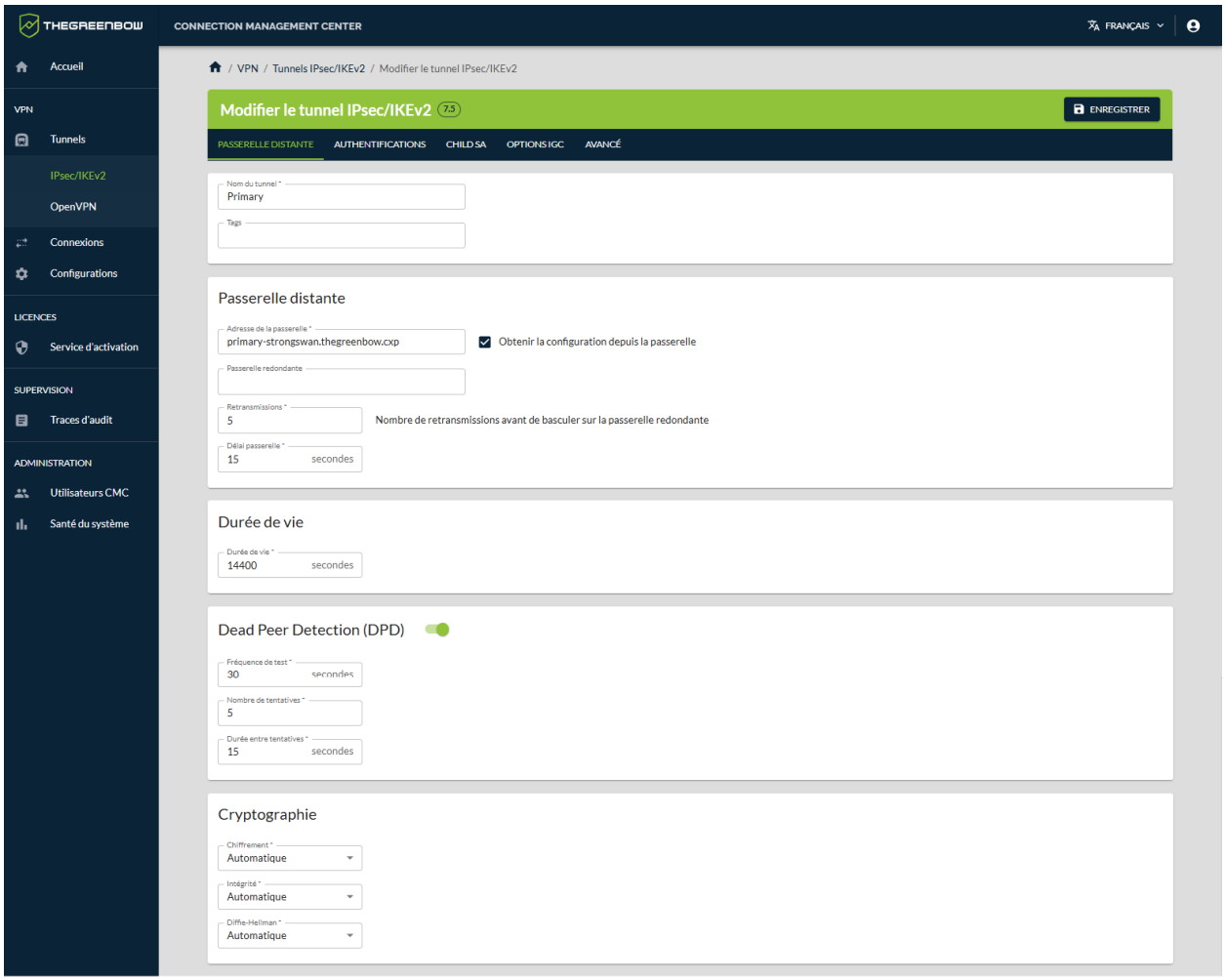
Pour modifier un tunnel IPsec/IKEv2, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **IPsec/IKEv2**. La liste des tunnels IPsec/IKEv2 s'affiche :



2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier**.

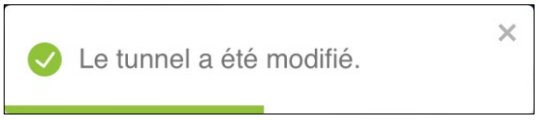
La page **Modifier le tunnel IPsec/IKEv2** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :



3. Effectuez les modifications souhaitées.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **PASSERELLE DISTANTE**, **AUTHENTIFICATIONS**, **CHILD SA**, **OPTIONS IGC** et **AVANCÉ**.

4. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est modifié et un message de confirmation s'affiche :



5. La page **Modifier le tunnel IPsec/IKEv2** reste affichée. Vous pouvez poursuivre vos travaux en sélectionnant l'option de votre choix dans le menu principal.

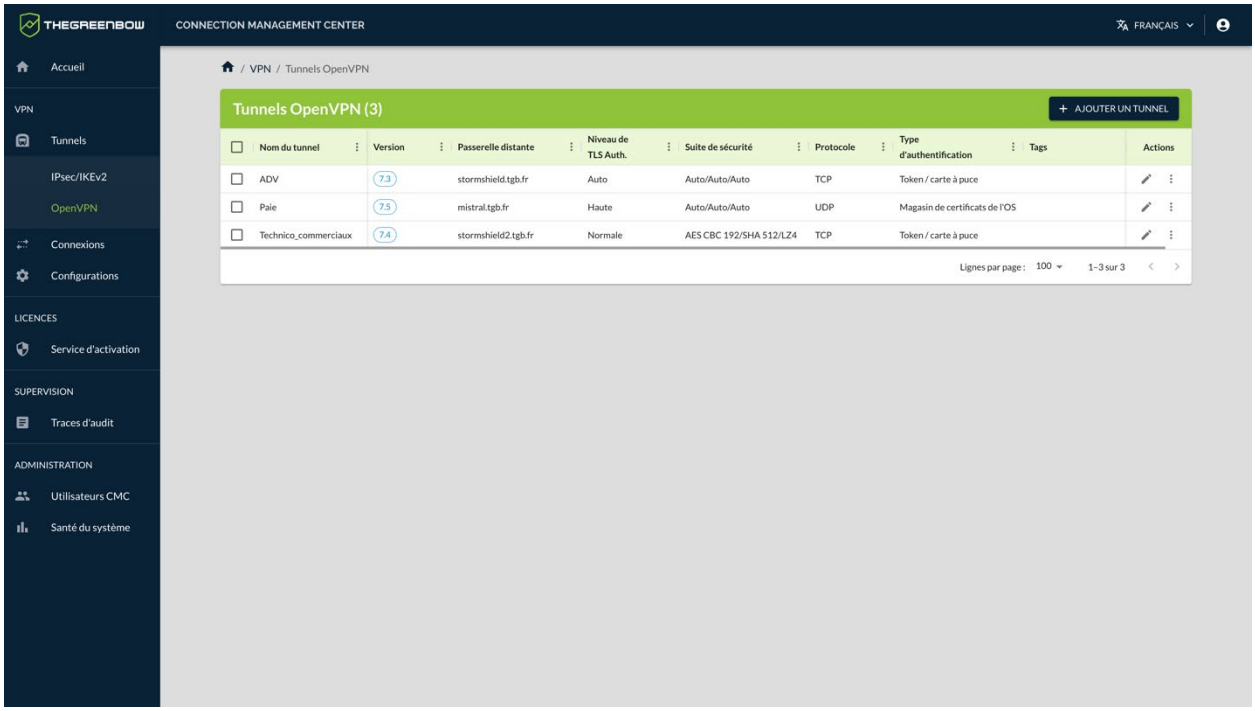
Vous avez terminé la modification du tunnel IPsec/IKEv2.

5.2.2.2 Modifier un tunnel OpenVPN

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à modifier les tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

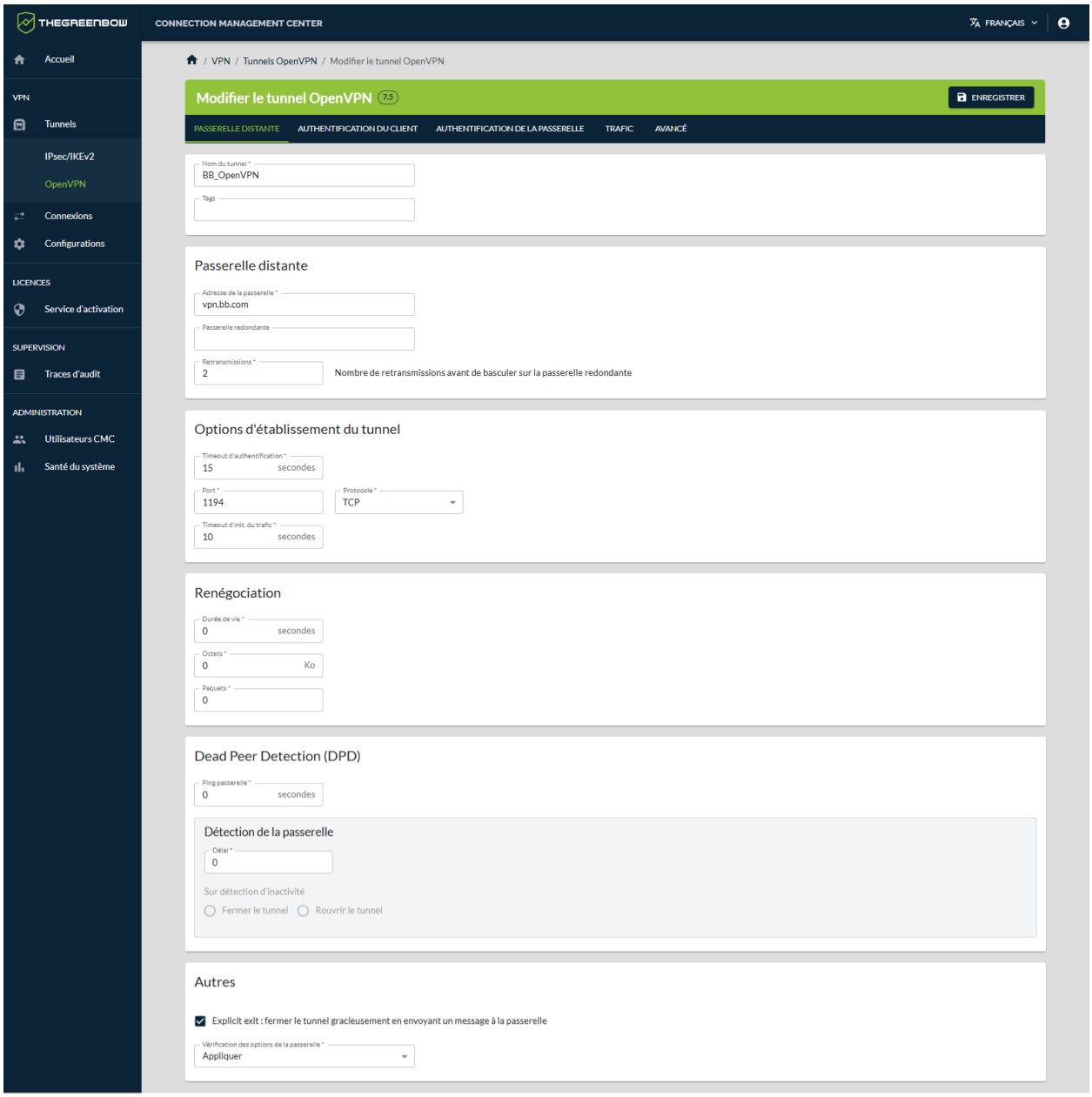
Pour modifier un tunnel OpenVPN, procédez comme suit :

1. Dans le menu principal, sous **VPN** > **Tunnels**, sélectionnez **OpenVPN**. La liste des tunnels OpenVPN s'affiche :



2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier**.

La page **Modifier le tunnel OpenVPN** s'ouvre sur le premier onglet **PASSERELLE DISTANTE** :



3. Effectuez les modifications souhaitées.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs des onglets **PASSERELLE DISTANTE**, **AUTHENTIFICATION DU CLIENT**, **AUTHENTIFICATION DE LA PASSERELLE**, **TRAFIC** et **AVANCÉ**.

4. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est modifié et un message de confirmation s'affiche :

5. La page **Modifier le tunnel OpenVPN** reste affichée. Vous pouvez poursuivre vos travaux en sélectionnant l'option de votre choix dans le menu principal.

Vous avez terminé la modification du tunnel OpenVPN.

5.2.3 Dupliquer un tunnel

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à dupliquer les tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

La procédure de duplication d'un tunnel est identique quel que soit le type de tunnel. Pour dupliquer un tunnel, procédez comme suit :

1. Accéder à la liste des tunnels IPsec/IKEv2 ou OpenVPN.
2. Dans la colonne **Actions**, cliquez sur le pictogramme avec les trois points verticaux ⋮ pour ouvrir le menu d'action.
3. Sélectionnez l'option **Dupliquer**. La boîte de dialogue **Créer un tunnel** s'affiche :

4. Dans la liste déroulant **Version du Client VPN**, sélectionnez la version souhaitée.

Vous pouvez uniquement choisir une version supérieure. Certaines options n'étant pas disponibles pour les versions antérieures des Clients VPN, si vous souhaitez créer un tunnel identique ou similaire, vous devez créer un nouveau tunnel.

En fonction du type de tunnel dupliqué, la fenêtre de création d'un tunnel IPsec/IKEv2 ou OpenVPN s'affiche avec l'ensemble des paramètres définis dans le tunnel dupliqué.

5. Modifiez le nom du tunnel ainsi que tous les autres paramètres que vous souhaitez changer.

⚠ Il ne peut y avoir deux tunnels avec le même nom indépendamment du type de protocole IPsec/IKEv2 ou OpenVPN. Si vous tentez d'enregistrer le tunnel sous le même nom, un message d'erreur s'affiche en haut à droite. Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs sur les différents onglets des pages **Créer un tunnel IPsec/IKEv2** et **Créer un tunnel OpenVPN**.

6. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est ajouté à la liste des tunnels correspondante qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la duplication du tunnel.

5.2.4 Supprimer un tunnel

🔒 Seuls les utilisateurs qui disposent du droit de suppression des VPN sont habilités à supprimer des tunnels (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Quel que soit le type de tunnel, la procédure de suppression d'un tunnel s'apparente à la suppression d'une ligne de données.

☞ Pour une description détaillée de la procédure de suppression d'une ligne de données, reportez-vous à la section 3.4.3 Supprimer une ou plusieurs lignes.

⚠ La suppression d'une ligne est définitive. Une fois confirmée, cette opération ne peut pas être annulée.

5.3 Gérer les connexions

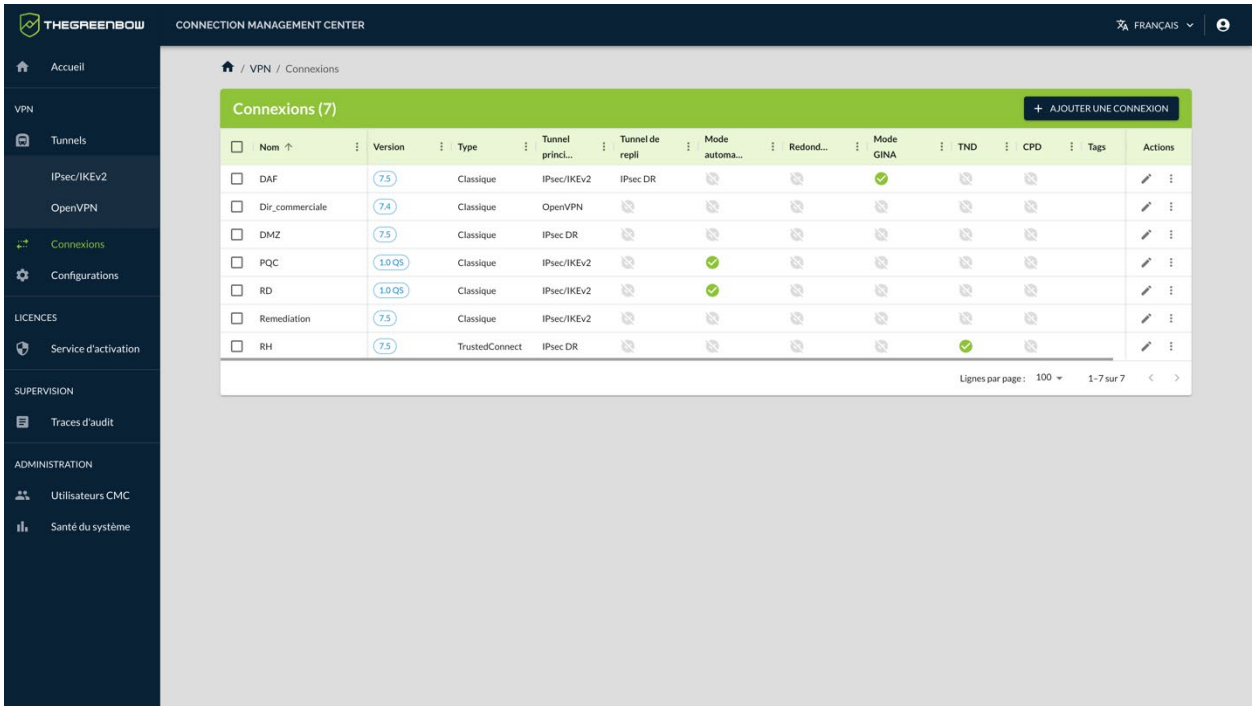
5.3.1 Créer une connexion

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des connexions (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Une connexion est nécessairement associée à un tunnel. Assurez-vous d'avoir créé un tunnel avant de procéder à la création d'une connexion.

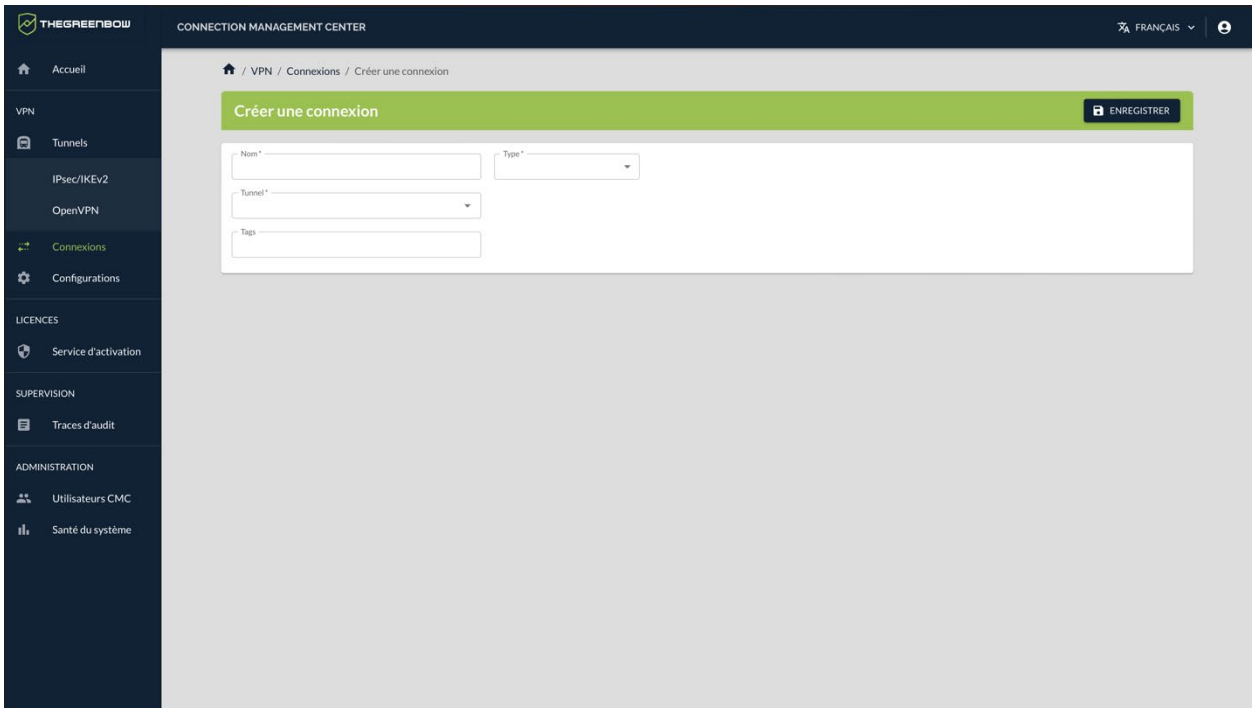
Pour créer une connexion, procédez comme suit :

1. Dans le menu principal, sous **VPN**, sélectionnez **Connexions**.
   La liste des connexions s'affiche :



2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UNE CONNEXION**.

La page **Créer une connexion** s'affiche :

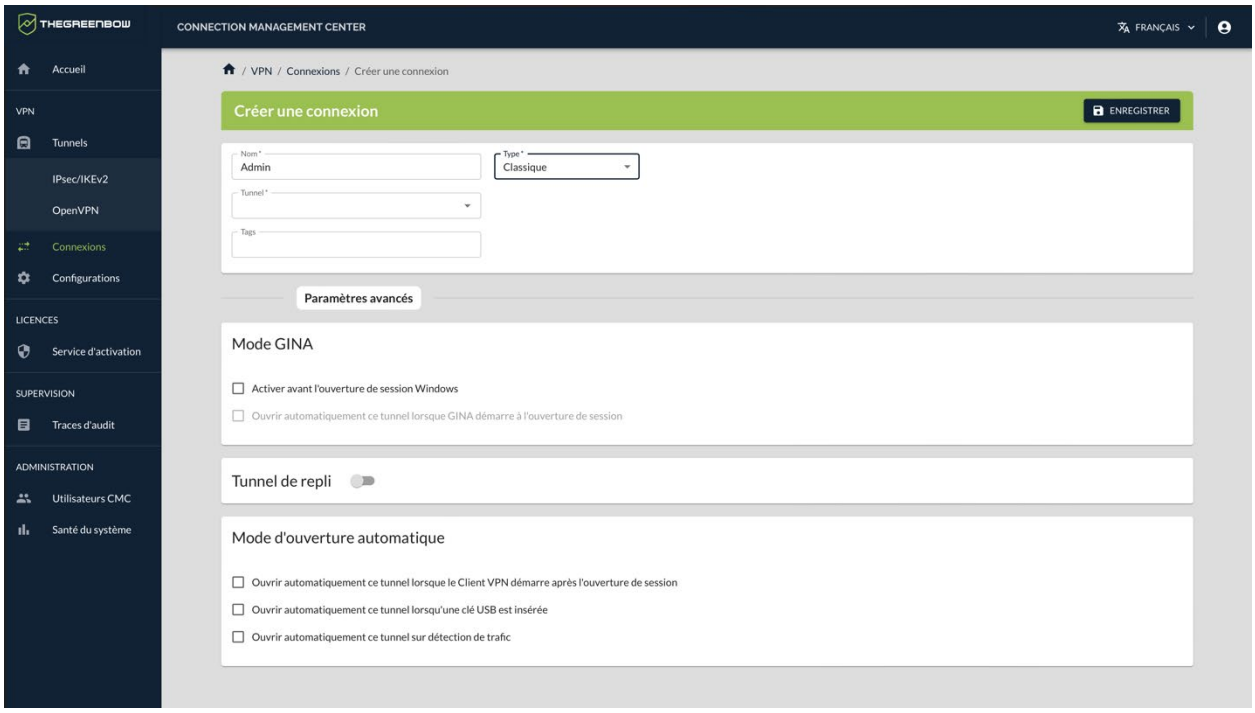


3. Dans le champ **Nom**, saisissez le nom que vous souhaitez attribuer à la connexion.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

4. Dans la liste déroulante **Type**, sélectionnez le type de connexion que vous souhaitez créer.

La section **Paramètres avancés** s'affiche :



☞ Pour comprendre la différence entre une connexion **Classique** et une connexion **TrustedConnect**, reportez-vous à la section 2.9 Connexion classique ou TrustedConnect, quelles différences ?

5. Dans la liste déroulante **Tunnel**, sélectionnez le tunnel que vous souhaitez utiliser avec cette connexion. Les autres champs et options sont facultatifs.

Seuls les tunnels compatibles avec le type de connexion sélectionné s'affichent dans la liste déroulante **Tunnel**. Si vous ne trouvez pas le tunnel souhaité, changez le type de connexion.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de la page **Créer une connexion**.

6. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La connexion est ajoutée à la liste des **Connexions** qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la création de la connexion. Vous pouvez poursuivre avec les étapes suivantes :

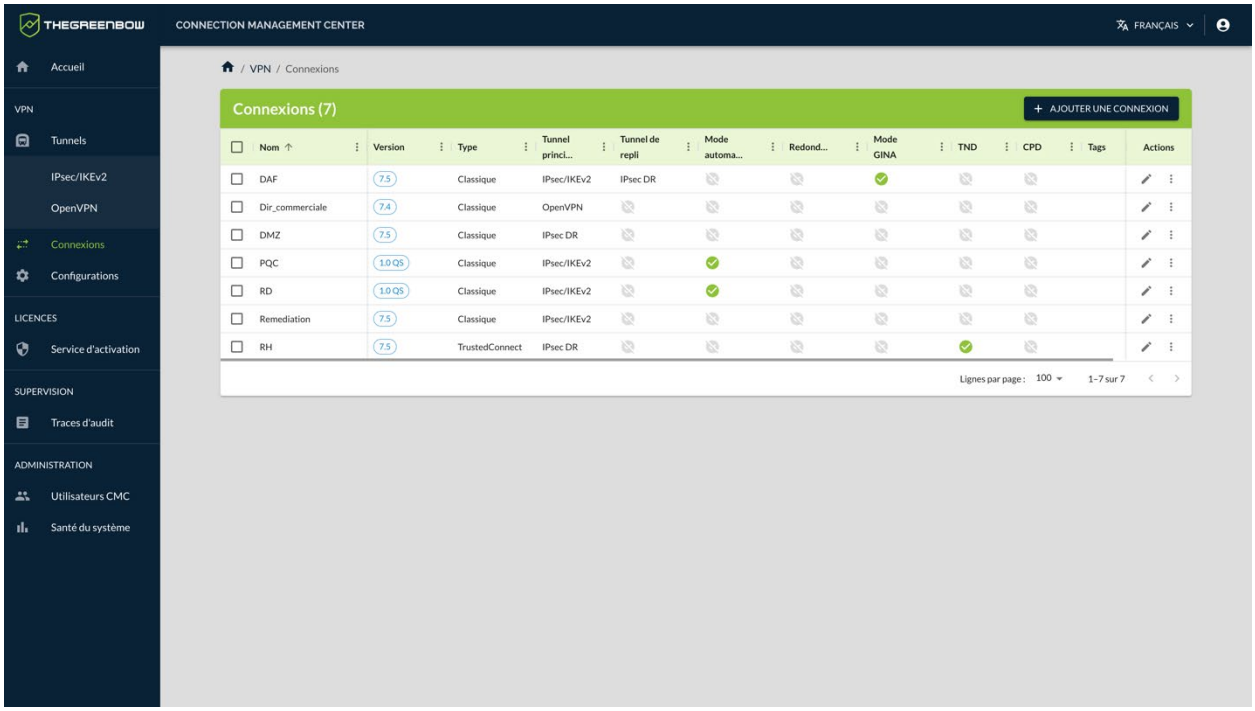
- Pour créer une configuration, reportez-vous à la section 5.4.1 Créer une configuration.
- Pour modifier la connexion que vous venez de créer, reportez-vous à la section 5.3.2 Modifier une connexion.

5.3.2 Modifier une connexion

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à modifier les connexions (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

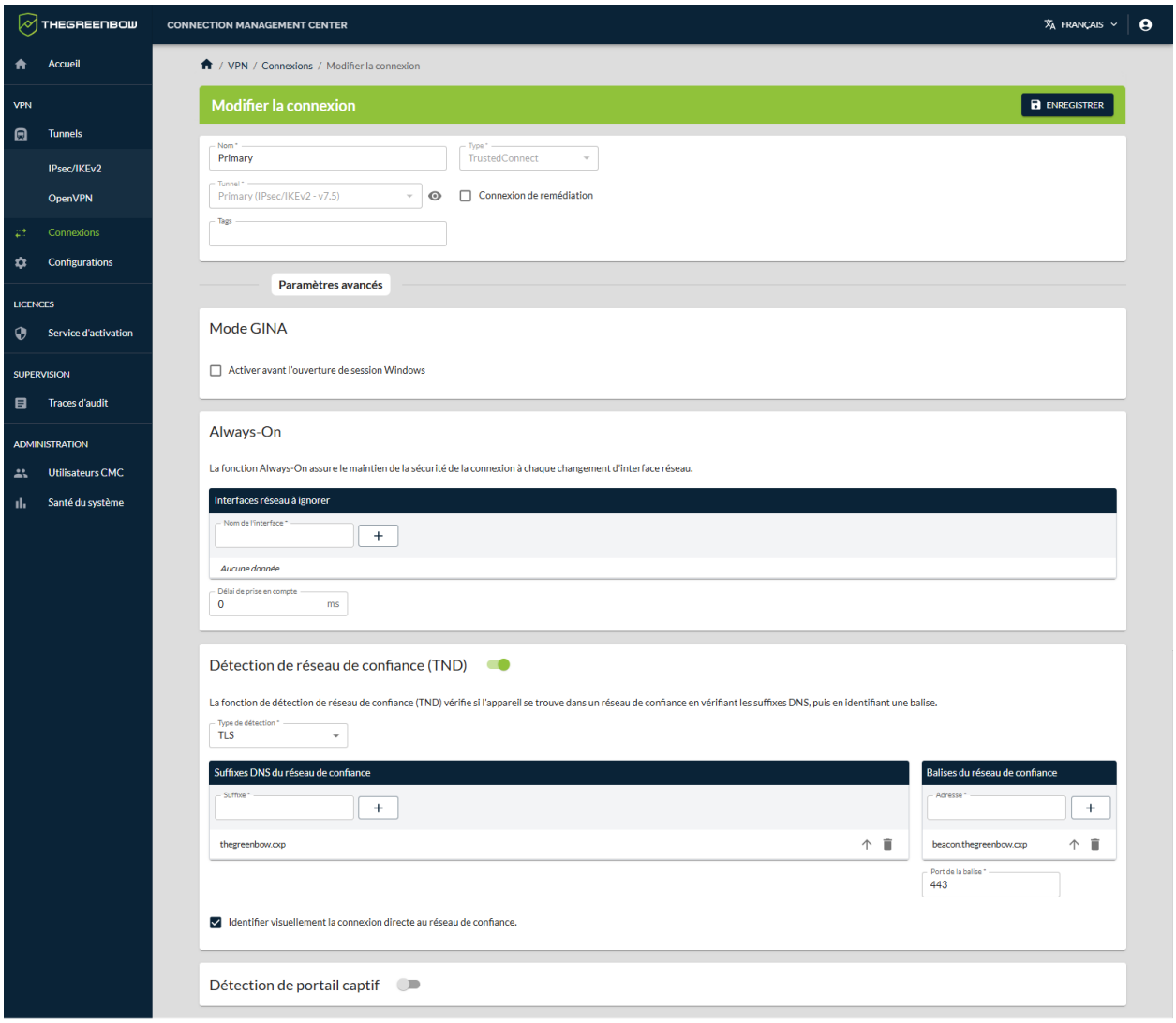
Pour modifier une connexion, procédez comme suit :

1. Dans le menu principal, sous **VPN**, sélectionnez **Connexions**. La liste des connexions s'affiche :



2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier**.

La page **Modifier la connexion** s'affiche :



3. Effectuez les modifications souhaitées.

Le type de connexion et le tunnel associé à la connexion sont grisés et ne peuvent pas être modifiés.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de la page **Modifier la connexion**.

4. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La connexion est modifiée et un message de confirmation s'affiche :

5. La page **Modifier la connexion** reste affichée. Vous pouvez poursuivre vos travaux en sélectionnant l'option de votre choix dans le menu principal.

5.3.3 Dupliquer une connexion

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à dupliquer des connexions (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour dupliquer une connexion, procédez comme suit :

1. Accéder à la liste des connexions.
2. Dans la colonne **Actions**, cliquez sur le pictogramme avec les trois points verticaux ⋮ pour ouvrir le menu d'action.
3. Sélectionnez l'option **Dupliquer**. La fenêtre de création d'une connexion s'affiche avec l'ensemble des paramètres définis dans la connexion dupliquée.
4. Modifiez le nom de la connexion ainsi que tous les autres paramètres que vous souhaitez changer.

Il ne peut y avoir deux connexions avec le même nom. Si vous tentez d'enregistrer la connexion sous le même nom, un message d'erreur s'affiche en haut à droite de la page. Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de la page **Créer une connexion**.

5. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La connexion est ajoutée à la liste des connexions qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la duplication de la connexion.

5.3.4 Supprimer une connexion

Seuls les utilisateurs qui disposent du droit de suppression des VPN sont habilités à supprimer des connexions (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

La procédure de suppression d'une connexion s'apparente à la suppression d'une ligne de données.

☞ Pour une description détaillée de la procédure de suppression d'une ligne de données, reportez-vous à la section 3.4.3 Supprimer une ou plusieurs lignes.

⚠ La suppression d'une ligne est définitive. Une fois confirmée, cette opération ne peut pas être annulée. Néanmoins, la suppression d'une connexion n'entraîne pas la suppression du tunnel qui lui est associé.

5.4 Gérer les configurations

5.4.1 Créer une configuration

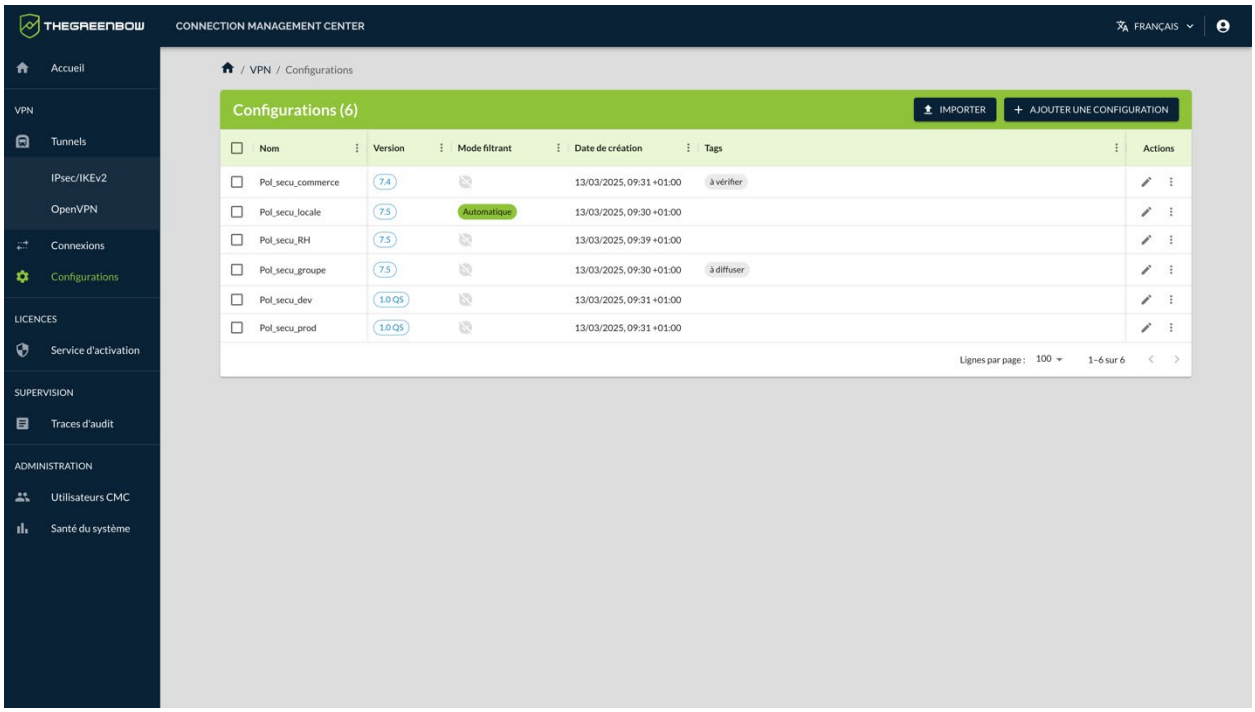
Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à créer des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Une configuration est nécessairement associée à au moins une connexion. Assurez-vous d'avoir créé une connexion avant de procéder à la création d'une configuration.

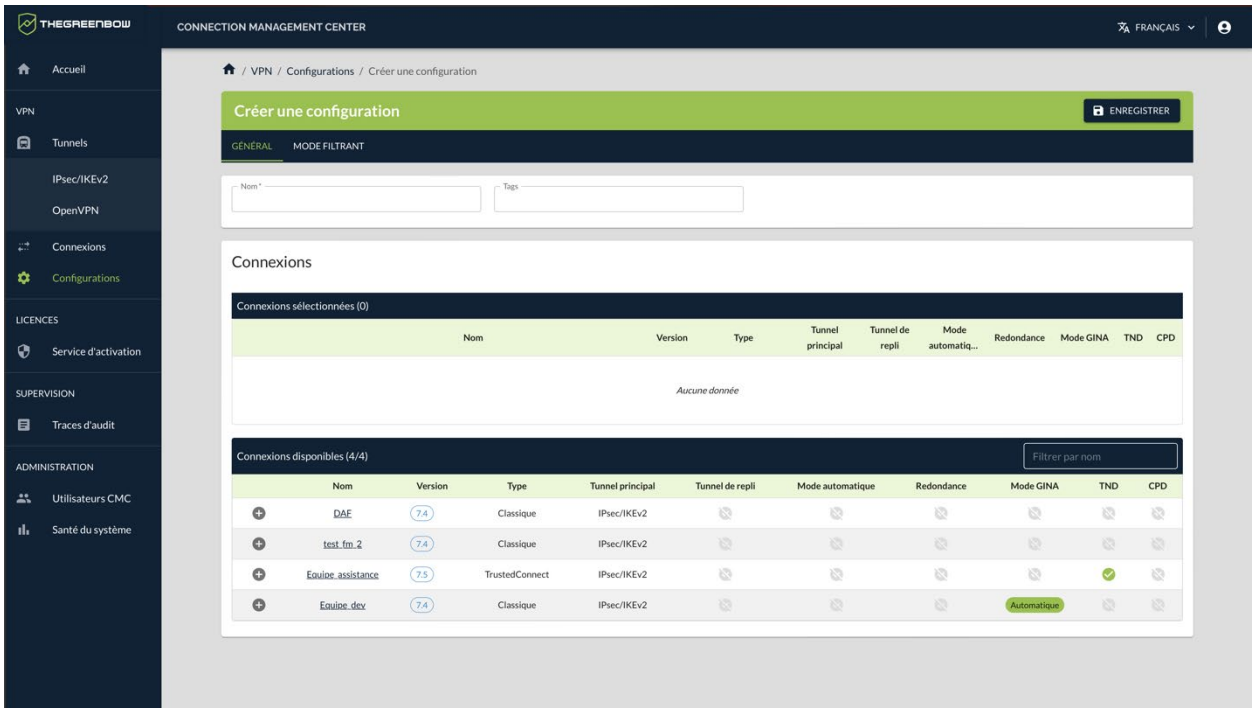
Pour créer une connexion, procédez comme suit :

1. Dans le menu principal, sous **VPN**, sélectionnez **Configurations**.

La liste des configurations s'affiche :



2. Dans la partie droite du bandeau de titre de la page, cliquez sur le bouton **+ AJOUTER UNE CONFIGURATION**. La page **Créer une configuration** s'ouvre sur le premier onglet **GÉNÉRAL** :



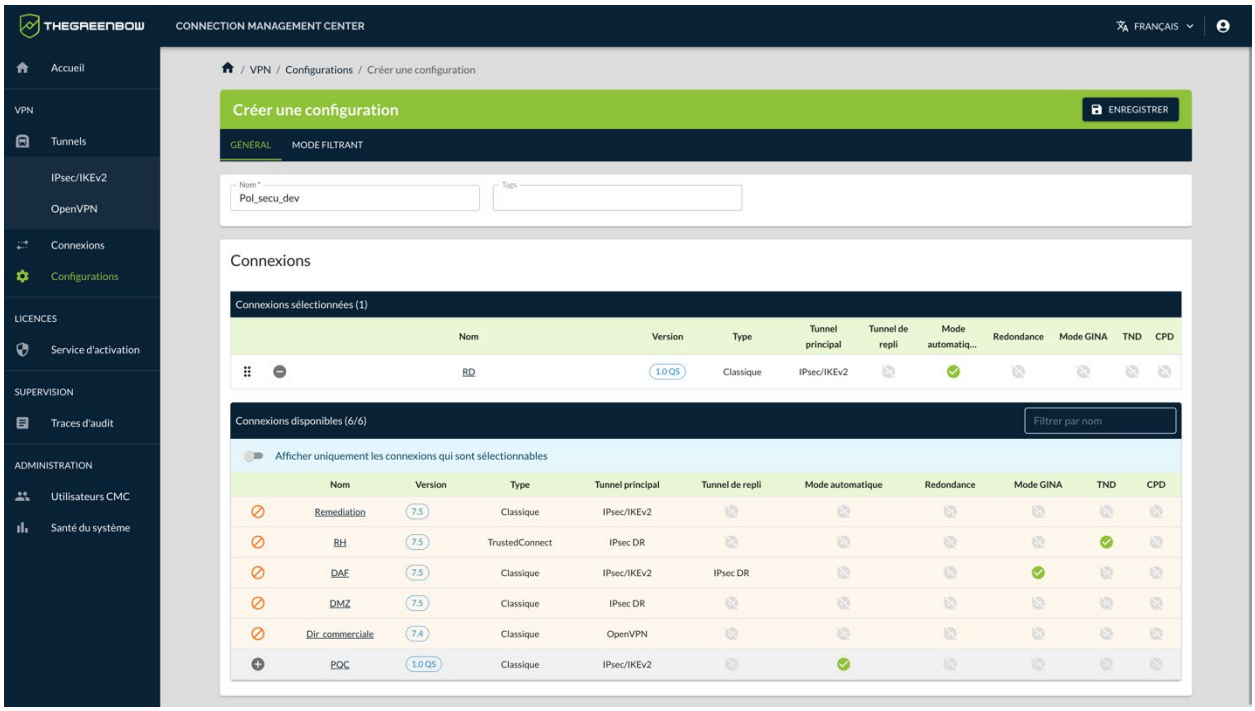
3. Dans le champ **Nom**, saisissez le nom que vous souhaitez attribuer à la configuration.

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

4. Dans la liste des **Connexions disponibles**, cliquez sur le pictogramme ⊕ de la ou des connexions que vous souhaitez ajouter à la configuration.

Vous pouvez filtrer la liste des **Connexions disponibles** par nom en saisissant tout ou partie du nom de la ou des connexions que vous souhaitez ajouter dans le champ prévu à cet effet dans la partie droite du bandeau de titre de la liste des **Connexions disponibles**.

La connexion sélectionnée est insérée dans la liste des **Connexions utilisées**.



Dans la liste des **Connexions disponibles**, un pictogramme accès interdit ⊘ s'affiche devant les connexions qui ne sont pas compatibles avec la connexion que vous venez d'ajouter à la configuration. Les lignes correspondantes apparaissent sur un fond orange pale. De plus, un bouton bascule **Afficher uniquement les connexions qui sont sélectionnables** s'affiche pour vous permettre de masquer les connexions qui ne sont pas compatibles.

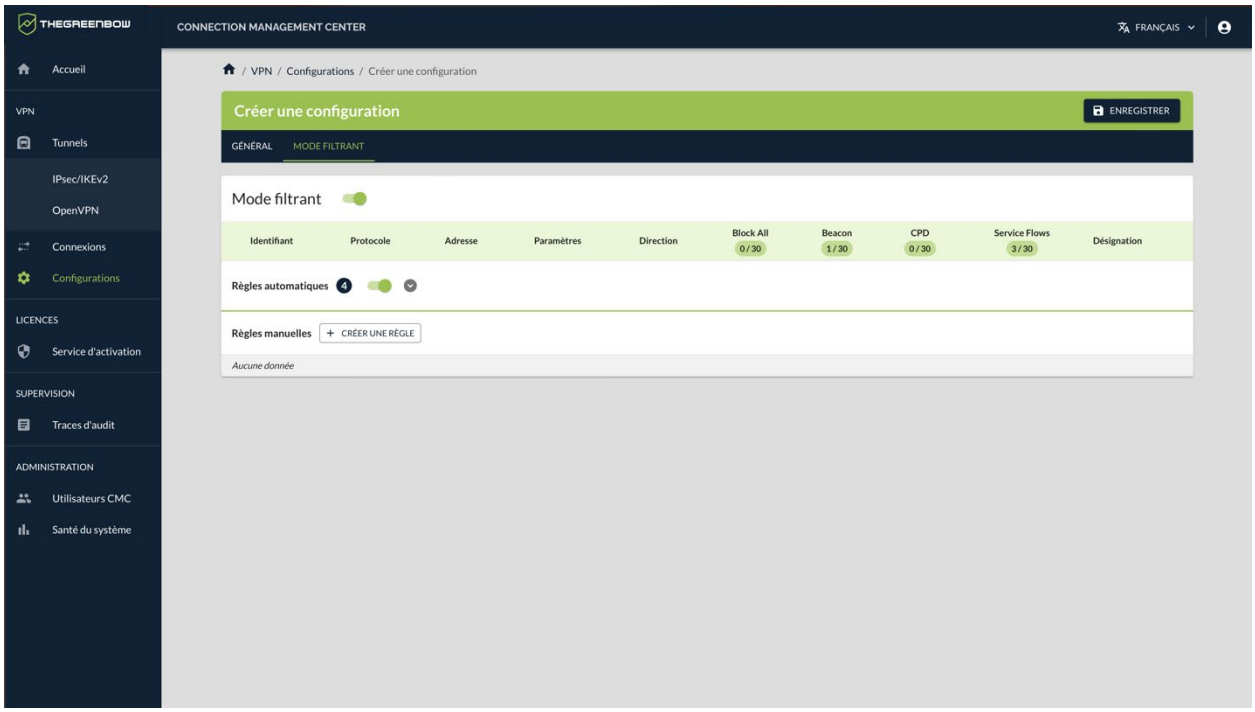
5. Vous pouvez ajouter autant de connexions compatibles que vous le souhaitez. Le pictogramme ⠿ au début de la ligne d'une connexion

sélectionnée vous permet de déplacer la connexion dans la liste des **Connexions utilisées** pour les arranger dans l'ordre de votre choix[1].

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **GÉNÉRAL**.

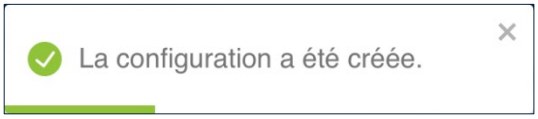
6. Si vous avez sélectionné au moins une connexion TrustedConnect, vous pouvez cliquer sur l'onglet **MODE FILTRANT** pour activer ce mode.

☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée de cette fonctionnalité.



☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de l'onglet **MODE FILTRANT**.

7. Lorsque vous avez terminé d'ajouter les connexions, cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La configuration est ajoutée à la liste des **Configurations** qui s'affiche à l'écran en même temps qu'un message de confirmation :



[1] Pour TrustedConnect, la première connexion de la liste est celle qui sera utilisée par défaut. Quand un tunnel de repli a été configuré, celui-ci doit se trouver en deuxième position.

Vous avez terminé la création de la configuration. Vous pouvez poursuivre avec les étapes suivantes :

- Pour exporter la configuration que vous venez de créer, reportez-vous à la section 5.4.5 Exporter une configuration.
- Pour modifier la configuration que vous venez de créer, reportez-vous à la section 5.4.2 Modifier une configuration.

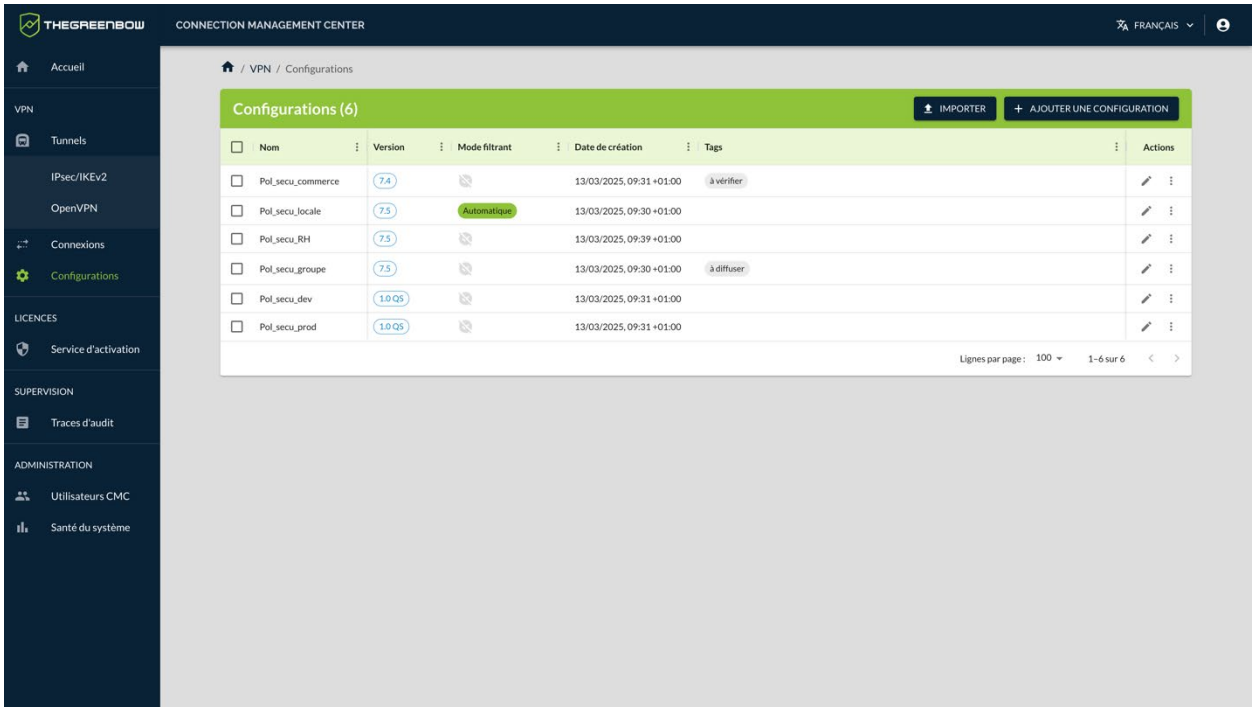
5.4.2 Modifier une configuration

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à modifier des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour modifier une configuration, procédez comme suit :

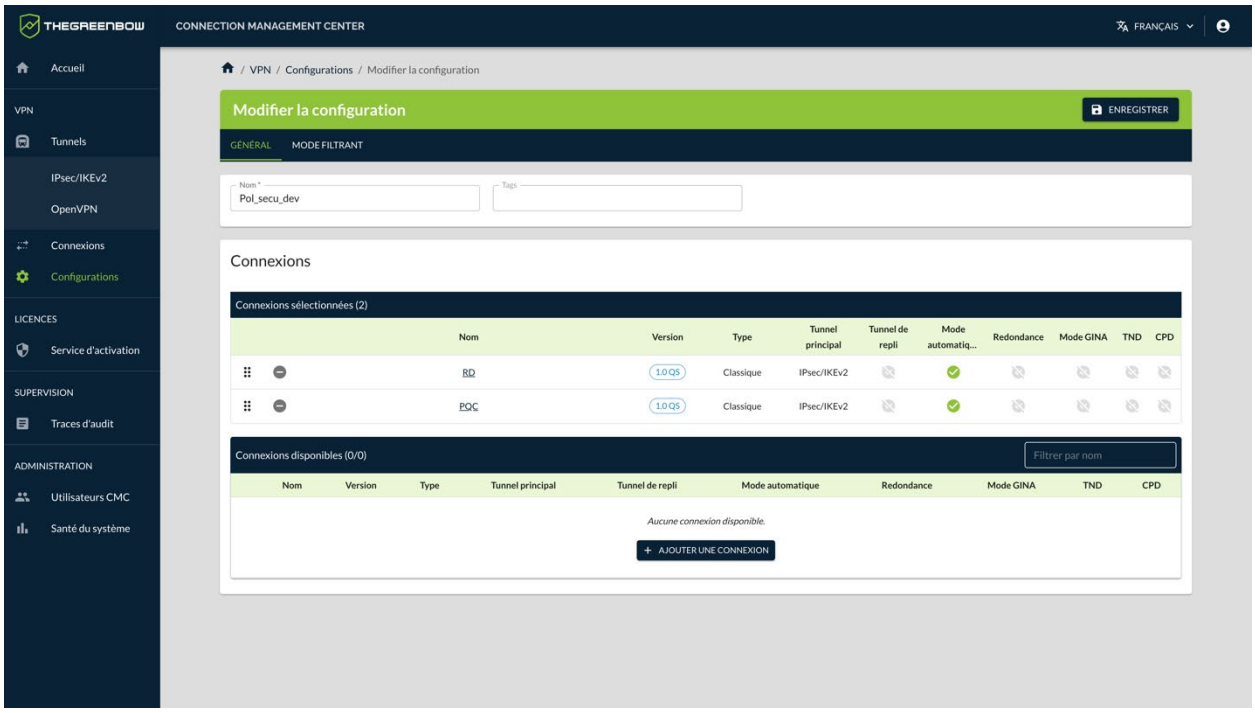
1. Dans le menu principal, sous **VPN**, sélectionnez **Configurations**.

   La liste des configurations s'affiche :



2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier**.

La page **Modifier la configuration** s'affiche :

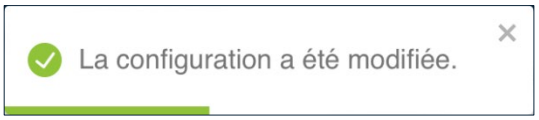


Seules les connexions de même type, et donc compatibles avec le type de connexion configurée, sont affichées dans la liste des connexions disponibles.

3. Effectuez les modifications souhaitées.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de la page **Modifier la configuration**.

4. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La configuration est modifiée et un message de confirmation s'affiche :



5. La page **Modifier la configuration** reste affichée. Vous pouvez poursuivre vos travaux en sélectionnant l'option de votre choix dans le menu principal.

Vous avez terminé la modification de la configuration.

5.4.3 Dupliquer une configuration

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à dupliquer des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour dupliquer une configuration, procédez comme suit :

1. Accéder à la liste des configurations.
2. Dans la colonne **Actions**, cliquez sur le pictogramme avec les trois points verticaux ⋮ pour ouvrir le menu d'action.
3. Sélectionnez l'option **Dupliquer**. La fenêtre de création d'une configuration s'affiche avec l'ensemble des paramètres définis dans la configuration dupliquée.
4. Modifiez le nom de la connexion ainsi que tous les autres paramètres que vous souhaitez changer.

Il ne peut y avoir deux configurations avec le même nom. Si vous tentez d'enregistrer la configuration sous le même nom, un message d'erreur s'affiche en haut à droite. Si vous quittez la page sans enregistrer vos modifications au préalable, celles-ci seront perdues.

☞ Reportez-vous au « Guide de référence » du CMC pour une description détaillée de tous les champs de la page **Créer une configuration**.

5. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. La configuration est ajoutée à la liste des configurations qui s'affiche à l'écran en même temps qu'un message de confirmation :

Vous avez terminé la duplication de la configuration.

5.4.4 Importer une configuration

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à importer des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Vous pouvez importer une configuration VPN en vue de la modifier ou de réutiliser les connexions et les tunnels qu'elle contient dans d'autres configurations.

⚠ Seules les configurations au format JSON exportées depuis un CMC peuvent être importées. Vous ne pouvez pas importer de configuration VPN au format `*.tgb` exportée depuis un client VPN.

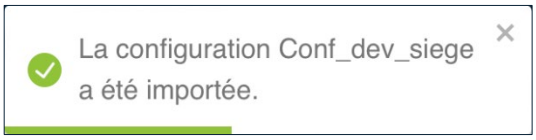
Pour importer une configuration, procédez comme suit :

1. Accédez à la liste des configurations, puis cliquez sur le bouton **IMPORTER** dans la partie droite du bandeau de titre de la page. Une boîte de dialogue **Importer une configuration** s'affiche à l'écran :

2. Glissez le fichier que vous souhaitez importer sur la zone **Fichier à importer** ou cliquez sur le bouton **Choisir le fichier**[1], puis naviguez vers le fichier à importer. La boîte de dialogue s'agrandit et les champs **Nom de la configuration** et **Version du Client VPN** sont remplis avec les informations récupérées du fichier de configuration :

3. Le cas échéant, modifiez le nom de la configuration et la version du Client VPN.
4. Cliquez sur **Importer**. La configuration ainsi que les connexions et tunnels qu'elle contient sont importés et un message de confirmation s'affiche :

[1] Le nom du bouton peut être différent selon le système d'exploitation et le navigateur utilisé.



Si une configuration, une connexion ou un tunnel de même nom existe déjà dans le CMC, les noms des objets importés seront pourvus d'un suffixe (n) où n est le nombre d'instances du même objet.

Vous avez terminé l'importation de la configuration VPN.

5.4.5 Exporter une configuration

Seuls les utilisateurs qui disposent du droit de consultation des VPN sont habilités à exporter des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Lorsque vous avez terminé de définir une configuration VPN, vous pouvez l'exporter au format `*.tgb` pour la déployer sur le parc de Clients VPN ou au format `*.json` à des fins de sauvegarde.

Les configurations VPN exportées ne sont ni chiffrées, ni protégées par mot de passe. Il convient donc de les manipuler avec prudence pour empêcher qu'elles ne soient utilisées de manière abusive.
Vous pouvez importer la configuration VPN dans un Client VPN Windows Enterprise en vue de de la chiffrer avant de procéder au déploiement.

Pour modifier une configuration, procédez comme suit :

1. Accédez à la liste des configurations.
2. Dans la colonne **Actions**, cliquez sur le pictogramme avec trois points verticaux ⋮ pour développer le menu d'actions[1].

3. Sélectionnez l'option **Exporter**.

[1] Les options disponibles dans le menu d'action dépendent des droits de l'utilisateur.

Une boîte de dialogue **Exporter une configuration** s'affiche à l'écran :

4. Cliquez sur le bouton correspondant au format dans lequel vous souhaitez exporter la configuration VPN. Le fichier est téléchargé vers le dossier de téléchargement par défaut.

Vous avez terminé l'exportation de la configuration VPN.

5.4.6 Supprimer une configuration

Seuls les utilisateurs qui disposent du droit de suppression des VPN sont habilités à supprimer des configurations (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

La procédure de suppression d'une configuration s'apparente à la suppression d'une ligne de données.

☞ Pour une description détaillée de la procédure de suppression d'une ligne de données, reportez-vous à la section 3.4.3 Supprimer une ou plusieurs lignes.

⚠ La suppression d'une ligne est définitive. Une fois confirmée, cette opération ne peut pas être annulée. Néanmoins, la suppression d'une configuration n'entraîne pas la suppression des connexions et tunnels qui lui sont associés.

5.5 Gérer les paramètres dynamiques

5.5.1 Introduction

Compatibilité : Windows, macOS

Le CMC permet si besoin de configurer des paramètres dynamiques additionnels pour les Clients VPN macOS et Windows Enterprise.

☞ Reportez-vous au « Guide de référence » du CMC pour plus de précisions sur cette fonctionnalité.

5.5.2 Ajouter un paramètre dynamique

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à ajouter des paramètres dynamiques (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour ajouter un paramètre dynamique, procédez comme suit :

1. Accédez à l'onglet **AVANCÉ** du tunnel pour lequel vous souhaitez ajouter un paramètre dynamique.

La procédure est similaire qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Pour un tunnel IPsec/IKEv2, dans la liste déroulante **Étendue** du sous-bloc **Paramètres dynamiques** du bloc **Autres**, sélectionnez la phase à laquelle s'applique le paramètre dynamique :
   - IKE_AUTH
   - CHILD_SA

   Pour un tunnel OpenVPN, poursuivez directement avec l'étape 3.
3. Entrez le nom du paramètre dynamique dans le champ **Nom**.
4. Saisissez la valeur du paramètre dynamique dans le champ **Valeur**.

5. Cliquez sur le bouton + en fin de ligne. Le paramètre dynamique est ajouté à la liste des paramètres dynamiques définis.

6. Cliquez sur le bouton **ENREGISTRER** dans la partie droite du bandeau de titre de la page. Le tunnel est créé ou modifié et un message de confirmation correspondant s'affiche.

Si vous quittez la page sans enregistrer vos modifications au préalable, le paramètre dynamique ne sera pas ajouté.

5.5.3 Supprimer un paramètre dynamique

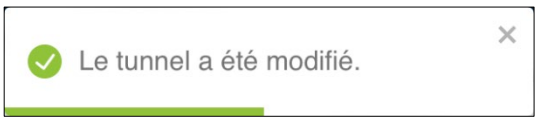
Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à supprimer des paramètres dynamiques (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour supprimer un paramètre dynamique de la liste des paramètres dynamiques définis, procédez comme suit :

1. Accédez à l'onglet **AVANCÉ** du tunnel pour lequel vous souhaitez supprimer un paramètre dynamique.

La procédure est similaire qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Dans la liste des paramètres dynamiques définis, cliquez sur le pictogramme **Supprimer ce paramètre**. Le paramètre est immédiatement retiré de la liste.
3. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est modifié et un message de confirmation s'affiche :



4. La page **Modifier le tunnel IPsec/IKEv2** ou **Modifier le tunnel OpenVPN** reste affichée. Vous pouvez poursuivre vos travaux en sélectionnant l'option de votre choix sur cette page ou dans le menu principal.

Si vous quittez la page sans enregistrer vos modifications au préalable, le paramètre dynamique ne sera pas supprimé.

5.6 Gérer les bureaux distants

5.6.1 Introduction

Compatibilité :

Le Client VPN Windows Enterprise permet de simplifier et de sécuriser automatiquement l'ouverture d'une session « Remote Desktop ».

☞ Reportez-vous au « Guide de référence » du CMC pour plus de précisions sur cette fonctionnalité.

5.6.2 Ajouter un partage de bureau distant

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à ajouter des partages de bureau distant (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour configurer le partage de bureau distant, procédez comme suit :

1. Accédez à l'onglet **AVANCÉ** du tunnel pour lequel vous souhaitez ajouter un partage de bureau distant.

La procédure est la même qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Dans le sous-bloc **Bureau distant** du bloc **Autres**, entrez un alias pour la connexion dans le champ **Alias**. Ce nom est utilisé pour identifier la connexion dans les différents menus du logiciel
3. Saisissez l'adresse IP ou le nom Windows du poste distant dans le champ **Adresse**.

4. Cliquez sur le bouton + en fin de ligne. Le partage de bureau distant est ajouté à la liste des bureaux distants définis.

5. Cliquez sur le bouton **ENREGISTRER** dans la partie droite du bandeau de titre de la page. Le tunnel est créé ou modifié et un message de confirmation correspondant s'affiche.

⚠ Si vous quittez la page sans enregistrer vos modifications au préalable, le partage de bureau distant ne sera pas ajouté.

ℹ Pour ouvrir cette connexion RDP en un seul clic, il est recommandé de la faire apparaître spécifiquement dans le **Panneau des Connexions**, du Client VPN Windows Enterprise, en utilisant la fonction de **Configuration des connexions** détaillée dans le chapitre Gestion du Panneau des Connexions du « Guide de l'administrateur » du Client VPN Windows Enterprise.

☞ Pour savoir comment supprimer un partage de bureau distant, reportez-vous à la section 5.6.3 Supprimer un partage de bureau distant.

5.6.3 Supprimer un partage de bureau distant

🔒 Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à supprimer des partages de bureau distant (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour supprimer un partage de bureau distant de la liste des bureaux distants définis, procédez comme suit :

1. Accédez à l'onglet **AVANCÉ** du tunnel pour lequel vous souhaitez supprimer un partage de bureau distant.

ℹ La procédure est similaire qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Dans la liste des partages de bureau distant définis, cliquez sur le pictogramme **Supprimer ce bureau distant**. Le partage de bureau distant est immédiatement retiré de la liste.
3. Cliquez sur le bouton **ENREGISTRER** dans la partie droite du bandeau de titre de la page. Le tunnel est modifié et un message de confirmation s'affiche :

4. La page **Modifier le tunnel IPsec/IKEv2** ou **Modifier le tunnel OpenVPN** reste affichée. Vous pouvez poursuivre vos travaux en

sélectionnant l'option de votre choix sur cette page ou dans le menu principal.

⚠ Si vous quittez la page sans enregistrer vos modifications au préalable, le partage de bureau distant ne sera pas supprimé.

5.7 Gérer les certificats utilisateurs

5.7.1 Généralités

Compatibilité : , , ,

Le CMC permet d'importer dans la configuration VPN des certificats utilisateurs au format PEM/PFX ou PKCS #12.

☞ Reportez-vous au « Guide de référence » du CMC pour plus de précisions sur les considérations à prendre en compte à cet égard.

5.7.2 Importer un certificat utilisateur dans une configuration VPN

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à importer un certificat utilisateur dans une configuration VPN (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Cette option n'est pas disponible pour un tunnel IPsec configuré en mode DR ni si une authentification par clé partagée ou EAP est déjà présente. Dans ce dernier cas, il convient de supprimer l'authentification par EAP et de l'ajouter après avoir importé le certificat utilisateur dans la configuration VPN.

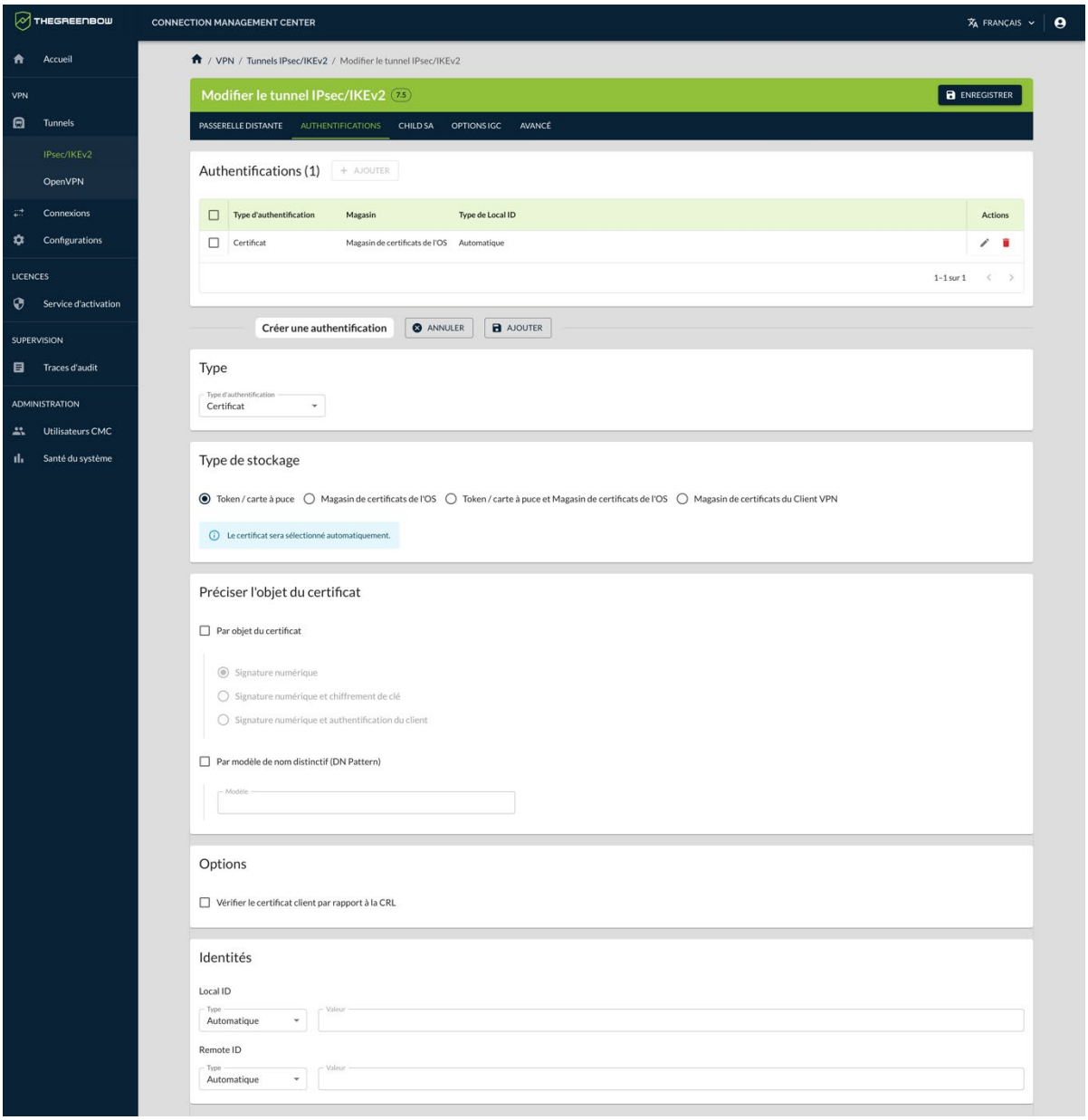
Pour importer un certificat utilisateur dans une configuration VPN, procédez comme suit :

1. Accédez à l'onglet **AUTHENTIFICATIONS** du tunnel IPsec/IKEv2 ou **AUTHENTIFICATION DU CLIENT** du tunnel OpenVPN pour lequel vous souhaitez importer le certificat.

La procédure est similaire qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Pour un tunnel IPsec/IKEv2, cliquez sur le bouton **+ Ajouter**.

Le volet **Créer une authentification** s'affiche :



Pour un tunnel OpenVPN, poursuivez directement avec l'étape 3.

3. Dans le bloc Type de stockage, sélectionnez l'option **Magasin de certificats du Client VPN**.

   Le bloc **Certificat PKCS #12** s'affiche :

4. Cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**.

Une boîte de dialogue **Importer un certificat** s'affiche :

5. Faites glisser un fichier au format souhaité (PEM/PFX ou PKCS #12) ou cliquez sur le bouton **Choisir le fichier**[1], puis naviguez vers le fichier à importer.
6. Saisissez le mot de passe associé au certificat dans le champ prévu à cet effet.

7. Cliquez sur le bouton **IMPORTER**. Le certificat est importé et un message de confirmation s'affiche :

[1] Le nom du bouton peut être différent selon le système d'exploitation et le navigateur utilisé.

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui l'a délivré et la date d'expiration :

8. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page. Le tunnel est créé ou modifié et un message de confirmation correspondant s'affiche.

⚠ Si vous quittez la page sans enregistrer vos modifications au préalable, le certificat ne sera pas ajouté.

☞ Pour savoir comment supprimer un certificat utilisateur de la configuration VPN, reportez-vous à la section 5.7.3 Supprimer un certificat utilisateur importé.

5.7.3 Supprimer un certificat utilisateur importé

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à supprimer un certificat utilisateur importé dans une configuration VPN (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour supprimer un certificat utilisateur importé dans une configuration VPN, procédez comme suit :

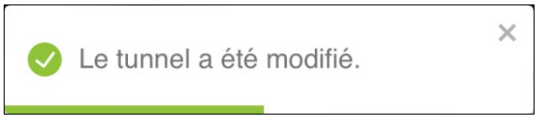
1. Accédez à la liste des tunnels.

ℹ La procédure est la même qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

2. Dans la colonne **Actions**, cliquez sur le pictogramme ✎ **Modifier** dans la ligne correspondant au tunnel pour lequel vous souhaitez supprimer le ou les certificats.
3. Pour un tunnel IPsec/IKEv2, naviguez vers l'onglet **AUTHENTIFICATIONS**.
   Pour un tunnel OpenVPN, naviguez vers l'onglet **AUTHENTIFICATION DU CLIENT**.

4. Dans le bloc **Certificat PKCS #12**, cliquez sur le pictogramme **Supprimer ce certificat**. Le certificat est immédiatement retiré de la liste.
5. Cliquez sur le bouton **ENREGISTRER** à droite dans le bandeau de titre de la page.

   Le tunnel est modifié et un message de confirmation s'affiche :



⚠ Si vous quittez la page sans enregistrer vos modifications au préalable, le certificat ne sera pas supprimé.

5.8 Gérer les autorités de certification de confiance

5.8.1 Généralités

Lorsque le Client VPN est configuré pour vérifier les certificats passerelle, les autorités de certification (CA) doivent être également accessibles.

La CA racine de la passerelle doit obligatoirement être importée dans la configuration.

Si la passerelle n'est pas configurée pour envoyer les CA, alors il est également nécessaire d'importer les CA intermédiaires dans la configuration.

ℹ Depuis la version 7.3 du Client VPN Windows Enterprise, il est possible de créer des configurations avec plus de trois autorités de certification (CA).

Les types de CA intermédiaires prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

Les types de CA racine prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

Pour des raisons de sécurité, l'utilisation du magasin de certificats Windows pour accéder aux CA n'est pas autorisé.

5.8.2 Importer le certificat d'une CA de confiance

Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à importer le certificat d'une CA de confiance dans une configuration VPN (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour importer le certificat d'une CA de confiance dans une configuration VPN, procédez comme suit :

1. Accédez à la liste des tunnels.
2. Dans la colonne **Actions**, cliquez sur le pictogramme **Modifier** dans la ligne correspondant au tunnel pour lequel vous souhaitez importer un certificat.
3. Pour un tunnel IPsec/IKEv12, accédez à l'onglet **OPTIONS IGC**.
   Pour un tunnel OpenVPN, accédez à l'onglet **AUTHENTIFICATION DE LA PASSERELLE**.

La procédure est ensuite la même qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

4. Dans le bloc **CA de confiance**, cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**.

   Une boîte de dialogue **Importer un certificat** s'affiche :

5. Faites glisser un fichier au format de CA souhaité (PEM ou DER) ou cliquez sur le bouton **Choisir le fichier**[1], puis naviguez vers le fichier à importer.

[1] Le nom du bouton peut être différent selon le système d'exploitation et le navigateur utilisé.

6. Cliquez sur le bouton **IMPORTER**. Le certificat est importé et un message de confirmation s'affiche :

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui l'a délivré et la date d'expiration :

7. Cliquez sur le bouton **ENREGISTRER** dans la partie droite du bandeau de titre de la page. Le tunnel est créé ou modifié et un message de confirmation correspondant s'affiche.

⚠ Si vous quittez la page sans enregistrer vos modifications au préalable, le certificat ne sera pas ajouté.

☞ Pour savoir comment supprimer un certificat de CA de la configuration VPN, reportez-vous à la section 5.8.3 Supprimer un certificat de CA importé.

5.8.3 Supprimer un certificat de CA importé

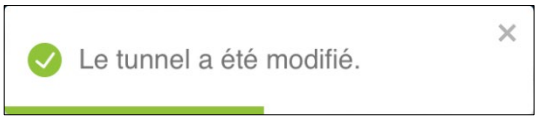
Seuls les utilisateurs qui disposent du droit d'édition des VPN sont habilités à supprimer un certificat de CA importé dans une configuration VPN (cf. section 4.2.1 Quels sont les droits des différents groupes d'utilisateurs et à quoi servent-ils ?).

Pour supprimer un certificat de CA importé dans une configuration VPN, procédez comme suit :

1. Accédez à la liste des tunnels.
2. Dans la colonne **Actions**, cliquez sur le pictogramme **Modifier** dans la ligne correspondant au tunnel pour lequel vous souhaitez supprimer le ou les certificats.
3. Pour un tunnel IPsec/IKEv12, accédez à l'onglet **OPTIONS IGC**. Pour un tunnel OpenVPN, accédez à l'onglet **AUTHENTIFICATION DE LA PASSERELLE**.

La procédure est ensuite la même qu'il s'agisse d'un tunnel IPsec/IKEv2 ou OpenVPN.

4. Dans le bloc **CA de confiance**, cliquez sur le pictogramme **Supprimer ce certificat** . Le certificat est immédiatement retiré de la liste.
5. Cliquez sur le bouton **ENREGISTRER** dans la partie droite du bandeau de titre de la page. Le tunnel est modifié et un message de confirmation s'affiche :



Si vous quittez la page sans enregistrer vos modifications au préalable, le certificat ne sera pas supprimé.

5.9 Gérer les règles manuelles du Mode filtrant

5.9.1 Introduction

Compatibilité :

Le Client VPN Windows Enterprise permet de filtrer les flux entrants et sortants du poste. Il est activé dès lors que le Client VPN Windows Enterprise ne se trouve pas sur le réseau de confiance.

Dans le CMC, certaines règles sont définies de manière automatique. Vous pouvez les compléter par des règles manuelles. La procédure pour ce faire est décrite ci-dessous.

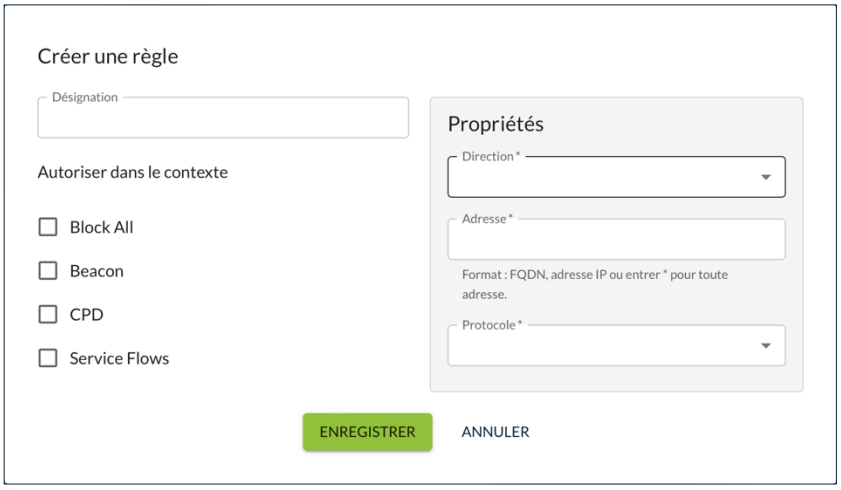
☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée de cette fonctionnalité.

5.9.2 Ajouter une règle manuelle

Pour ajouter une règle, procédez comme suit :

1. Accédez à l'onglet **MODE FILTRANT** de la configuration pour laquelle vous souhaitez ajouter une règle manuelle.
2. Dans le bloc **Mode filtrant**, cliquez sur le bouton **+ CRÉER UNE RÈGLE**.

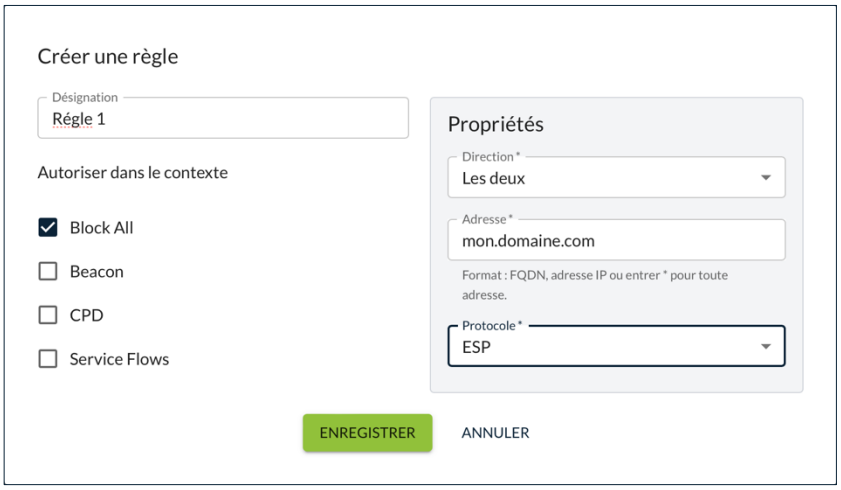
La boîte de dialogue **Créer une règle** s'affiche :



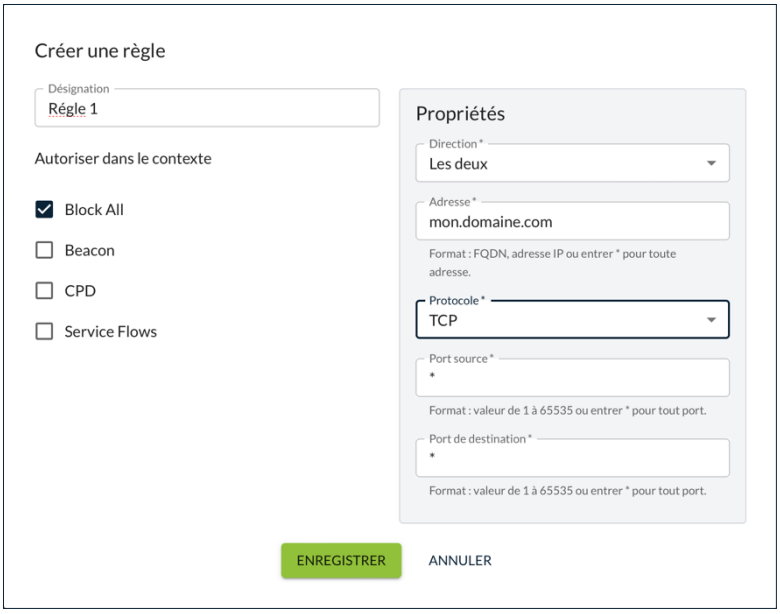
3. Saisissez une **Désignation** dans le champ prévu à cet effet. Il s'agit d'une chaîne de caractères libre, sans espace, à l'exclusion de `DYN_RULE_*`[1] qui est réservée à TheGreenBow.
4. Cochez le ou les contextes pour lesquels la règle doit être autorisée.
5. Dans la section **Propriétés**, sélectionnez la **Direction** du point de vue du poste de travail :
   - Descendant
   - Ascendant
   - Les deux
6. Dans le champ **Adresse**, saisissez un nom de domaine pleinement qualifié (FQDN), une adresse IP ou * pour toute adresse.
7. Dans la liste déroulante **Protocole**, sélectionnez le valeur souhaitée :
   - ICMP
   - TCP
   - UDP
   - ESP
   - ALL pour tout protocole

   Les champs sous la liste déroulante s'adaptent en fonction du protocole sélectionné.
8. Si vous avez sélectionné le protocole **ESP**, passez à l'étape suivante.

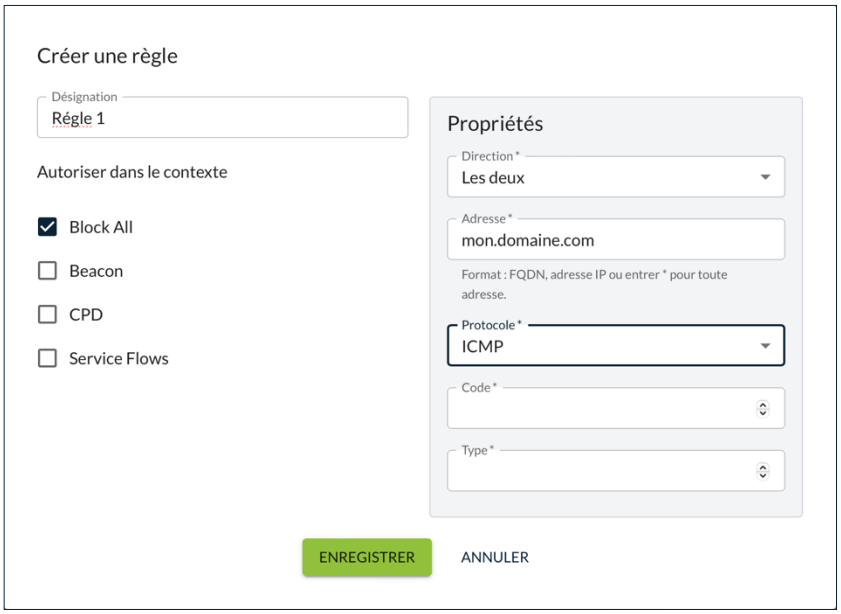
[1] Toute chaîne de caractères `DYN_RULE_1` à `DYN_RULE_N` est à proscrire.



Si vous avez sélectionné le protocole **TCP**, **UDP** ou **ALL**, renseignez une valeur comprise entre 1 et 65565 ou * pour tout port dans les champs **Port source** et le **Port de destination**.



Si vous avez sélectionné le protocole **ICMP**, renseignez une valeur comprise entre 0 et 15 ou * pour tous les codes ICMP dans le champ **Code** et une valeur comprise entre 0 et 18 ou * pour tous les types ICMP dans le champ **Type**.



9. Cliquez sur le bouton **ENREGISTRER**. La règle est ajoutée à la liste des règles manuelles.

⚠ N'oubliez pas d'enregistrer la configuration, en cliquant sur le bouton **ENREGISTRER** en haut à droite dans la barre de titre de la page avant de la quitter. Autrement, les modifications effectuée seront perdues.

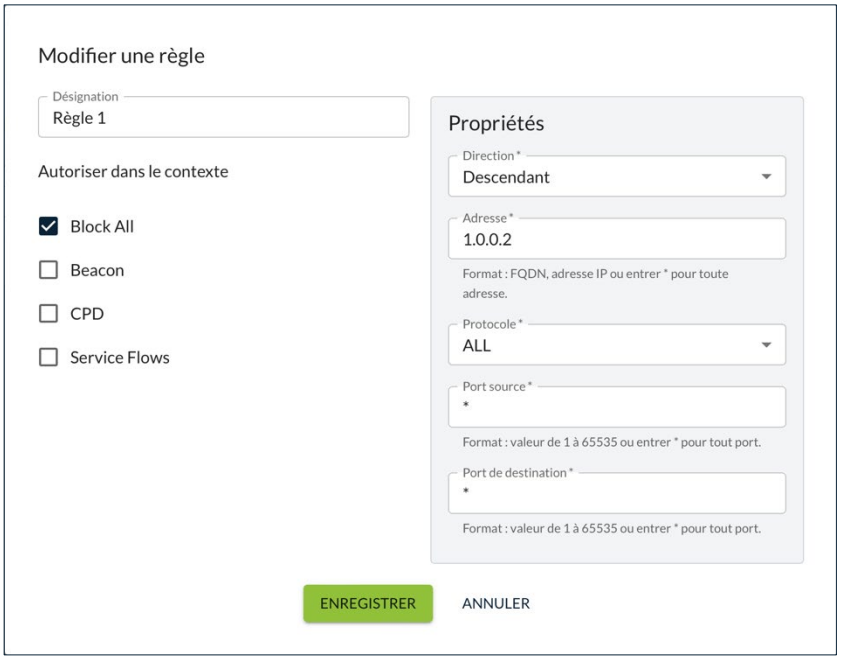
Dans la liste des règles manuelles, dès que vous avez ajouté au moins une règle, les pictogrammes **Modifier**, **Dupliquer** et **Supprimer** vous permettent d'intervenir sur ces règles.

5.9.3 Modifier une règle manuelle

Pour modifier une règle, procédez comme suit :

1. Accédez à l'onglet **MODE FILTRANT** de la configuration pour laquelle vous souhaitez modifier une règle manuelle.
2. Dans la liste des **Règles manuelles** du bloc **Mode filtrant**, cliquez sur le pictogramme **Modifier**.

La boîte de dialogue **Modifier** s'affiche :



3. Effectuez les modifications souhaitées, puis cliquez sur le bouton **ENREGISTRER**.

⚠ N'oubliez pas d'enregistrer la configuration, en cliquant sur le bouton **ENREGISTRER** en haut à droite dans la barre de titre de la page avant de la quitter. Autrement, les modifications effectuée seront perdues.

5.9.4 Dupliquer une règle manuelle

Pour dupliquer une règle, procédez comme suit :

1. Accédez à l'onglet **MODE FILTRANT** de la configuration pour laquelle vous souhaitez dupliquer une règle manuelle.
2. Dans la liste des **Règles manuelles** du bloc **Mode filtrant**, cliquez sur le pictogramme **Dupliquer**. Une copie de la règle dupliquée est ajoutée à la liste des règles manuelles.
3. Cliquez sur le pictogramme **Modifier** au niveau de la règle dupliquée pour y apporter vos modifications. Pour cela, procédez comme décrit à la section 5.9.3 Modifier une règle manuelle.

⚠ N'oubliez pas d'enregistrer la configuration, en cliquant sur le bouton **ENREGISTRER** en haut à droite dans la barre de titre de la page avant de la quitter. Autrement, la règle dupliquée ne sera pas conservée.

5.9.5 Supprimer une règle manuelle

Pour dupliquer une règle, procédez comme suit :

1. Accédez à l'onglet **MODE FILTRANT** de la configuration pour laquelle vous souhaitez supprimer une règle manuelle.
2. Dans la liste des **Règles manuelles** du bloc **Mode filtrant**, cliquez sur le pictogramme **Supprimer**. Une boîte de dialogue s'affiche pour vous demander de confirmer la suppression :

3. Cliquez sur le bouton **SUPPRIMER**. La règle est supprimée de la liste des règles manuelles.

⚠ N'oubliez pas d'enregistrer la configuration, en cliquant sur le bouton **ENREGISTRER** en haut à droite dans la barre de titre de la page avant de la quitter. Autrement, la règle ne sera pas supprimée.

6 Gestion des licences

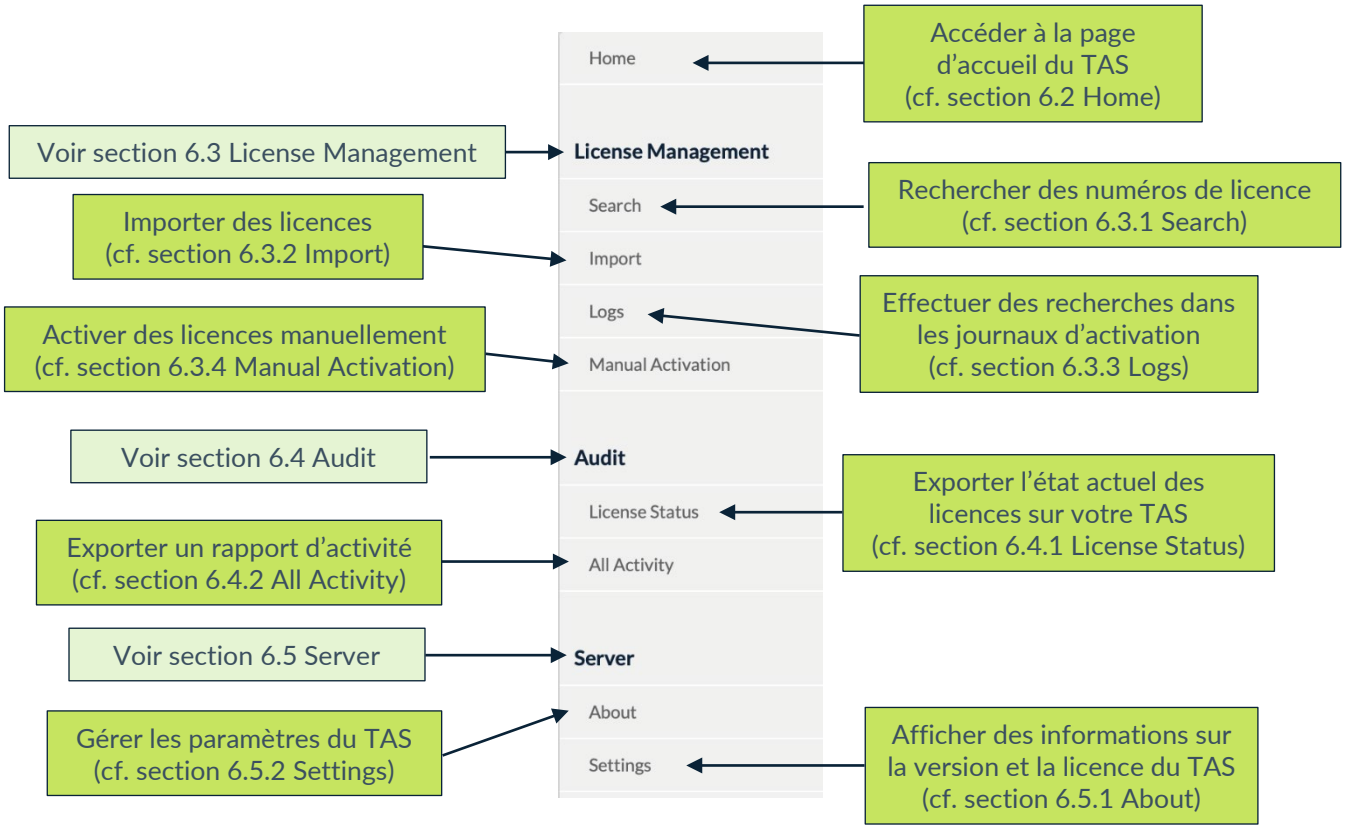
6.1 Présentation

Une fois le service d'activation préparé, vous pouvez commencer à l'utiliser immédiatement. Si le service d'activation n'a pas été préparé pour le CMC, vous verrez une page **Server Activation** (Activation du serveur) s'afficher lorsque vous sélectionnez l'option **Serveur d'activation** dans la rubrique **LICENCES** du menu principal du CMC.

☞ Pour savoir comment préparer une instance existante ou générer une nouvelle instance du service d'activation en vue de son une utilisation dans le CMC, reportez-vous au Guide d'installation du CMC.

Si vous êtes familier avec le serveur d'activation TheGreenBow (TAS), la gestion des licences dans le CMC est pratiquement identique. La gestion des utilisateurs est dévolue au CMC et certaines fonctions d'exportation ne sont plus disponibles.

Le menu du TAS a été repris à l'intérieur de la page **Serveur d'activation**. Par conséquent, il est uniquement disponible en anglais. Il contient plusieurs éléments regroupés sous différentes rubriques :

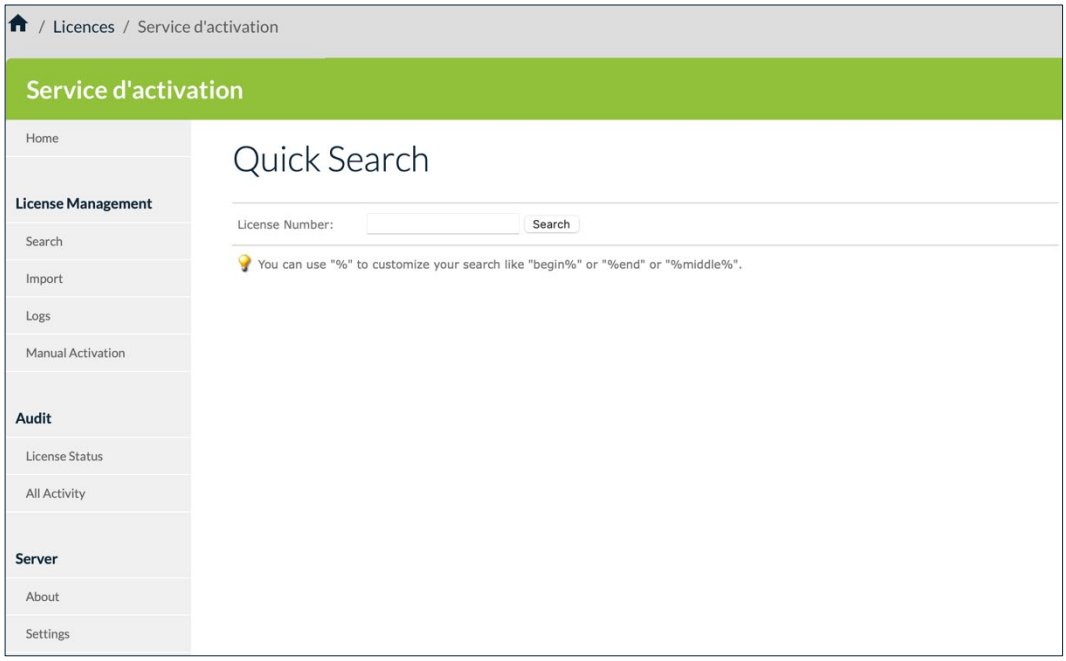


Chaque option est décrite ci-dessous dans le même ordre qu'elle figure dans le menu. Vous pouvez également cliquer sur les liens dans les descriptions ci-dessus pour accéder directement à la section correspondante.

Les captures d'écran présentées ci-après font abstraction du menu et des autres éléments d'interface du CMC dans lesquels le service d'activation s'inscrit, afin de se concentrer uniquement sur les fonctionnalités de ce dernier.

6.2 Home

La page d'accueil du service d'activation est la page qui s'affiche par défaut lorsque vous cliquez sur l'option **Serveur d'activation** sous la rubrique **LICENCES** du menu principal du CMC.



Elle contient un champ **Quick Search** (Recherche rapide) qui vous permet de rechercher rapidement un ou plusieurs numéros de licence.

Vous pouvez utiliser le caractère générique « % » pour représenter un ou plusieurs caractères dans votre recherche, p. ex. « début% », « %fin » ou « %milieu% ».

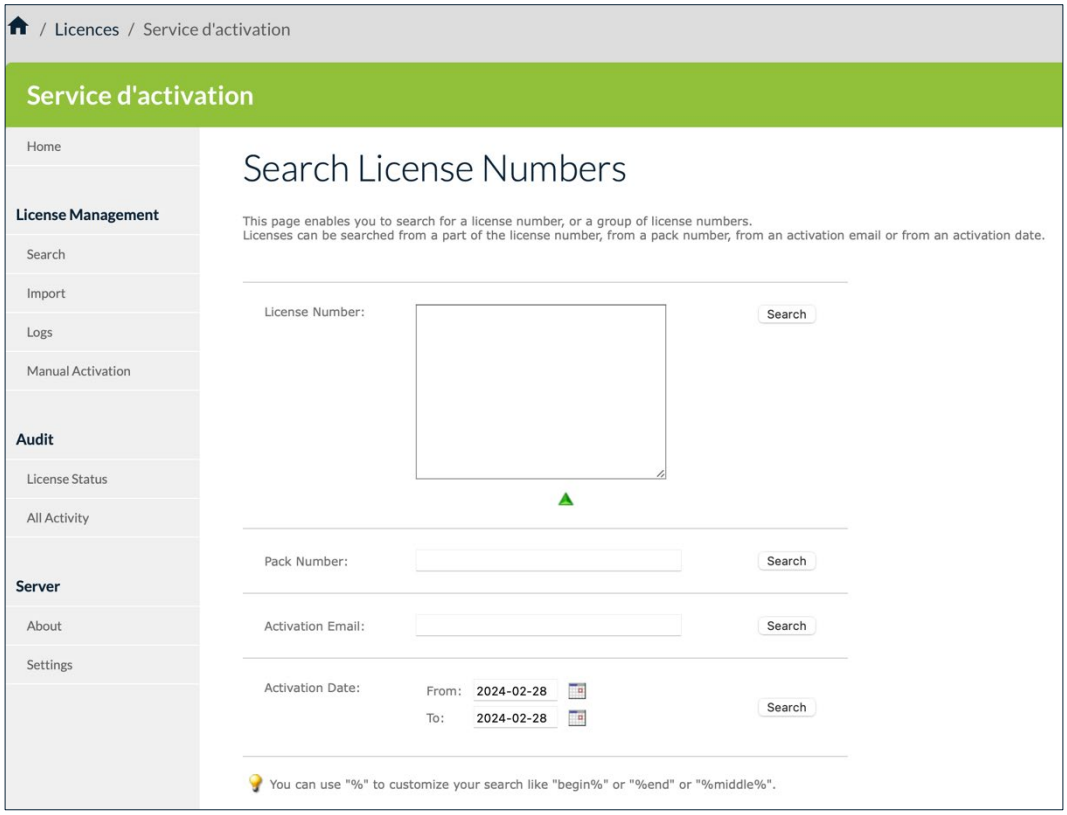
6.3 License Management

La rubrique **License Management** (Gestion des licences) comprend les options de menu suivantes :

- **Search** (Rechercher) permet de rechercher des numéros de licence (cf. section 6.3.1 Search) ;
- **Import** (Importer) permet d'importer des licences (cf. section 6.3.2 Import) ;
- **Logs** (Journaux) permet d'effectuer des recherches dans les journaux d'activation (cf. section 6.3.3 Logs) ;
- **Manual Activation** (Activation manuelle) permet d'activer des licences manuellement (cf. section 6.3.4 Manual Activation).

6.3.1 Search

L'option de menu **Search** (Rechercher) ouvre la page **Search License Numbers** (Rechercher numéros de licence).



Le service d'activation vous permet de rechercher des numéros de licence selon plusieurs critères :

- **License Number** (Numéro de licence) pour un ou plusieurs numéros de licence ;
- **Pack Number** (Numéro de pack) pour les numéros de licence faisant partie d'un groupe ;

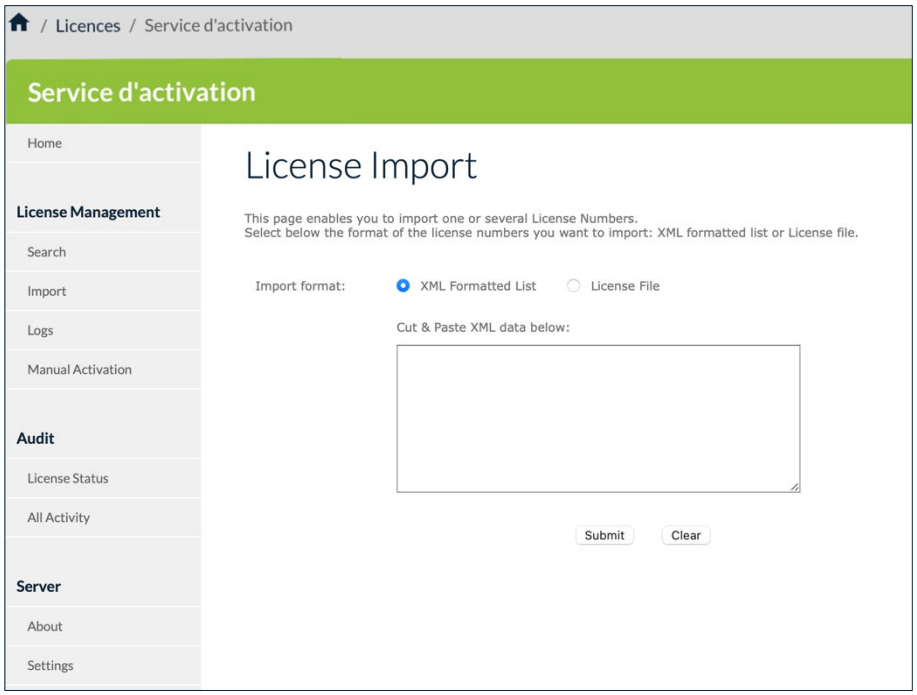
- **Activation Email** (E-mail d'activation) saisi par les utilisateurs lors de l'activation du logiciel ;
- **Activation Date** (Date d'activation) pour une date ou une période donnée.

Pour tous les champs de la page **Search License Numbers** (Rechercher numéros de licence), vous pouvez utiliser le caractère générique « % » pour représenter un ou plusieurs caractères dans votre recherche, p. ex. « début% », « %fin » ou « %milieu% ».

Lorsqu'un numéro de licence particulier est trouvé, vous pouvez vérifier s'il a été activé et visualiser les détails relatifs à l'activation, tels que la date, l'heure et l'e-mail d'activation.

6.3.2 Import

L'option de menu **Import** (Importer) ouvre la page **License Import** (Importation de licences).



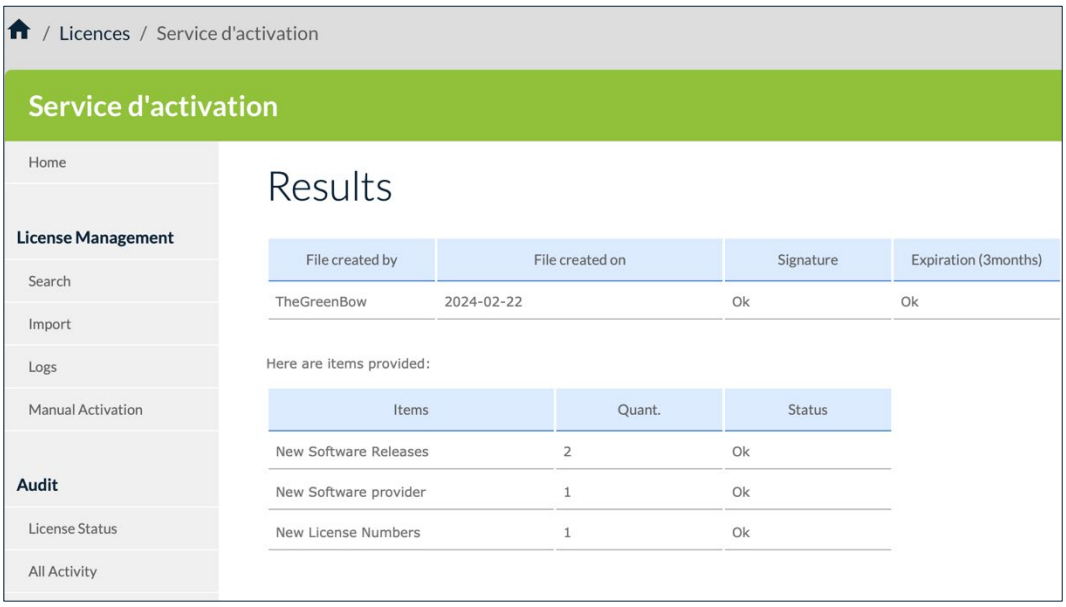
À l'installation, le service d'activation ne contient aucun numéro de licence de Client VPN. TheGreenBow fournit les numéros de licence pour ses logiciels VPN dans des fichiers XML que vous pouvez importer.

Pour importer un fichier de licence au format XML, suivez les étapes ci-dessous :

1. Dans le menu de gauche, sous **License Management** (Gestion des licences), cliquez sur **Import** (Importer) pour afficher la page **License Import** (Importation de licences).
2. Sous **Import format** (Format d'importation), cliquez sur **License File** (Fichier de licence). Un bouton **Parcourir...** (ou équivalent en fonction de votre navigateur) s'affiche. Cliquez sur **Parcourir...**, sélectionnez le fichier de licence au format XML que vous souhaitez téléverser, puis cliquez sur **Submit** (Envoyer).

Vous pouvez également cliquer sur **XML Formatted List** (Liste au format XML), coller le contenu du fichier dans le champ prévu à cet effet, puis cliquer sur **Submit** (Envoyer).

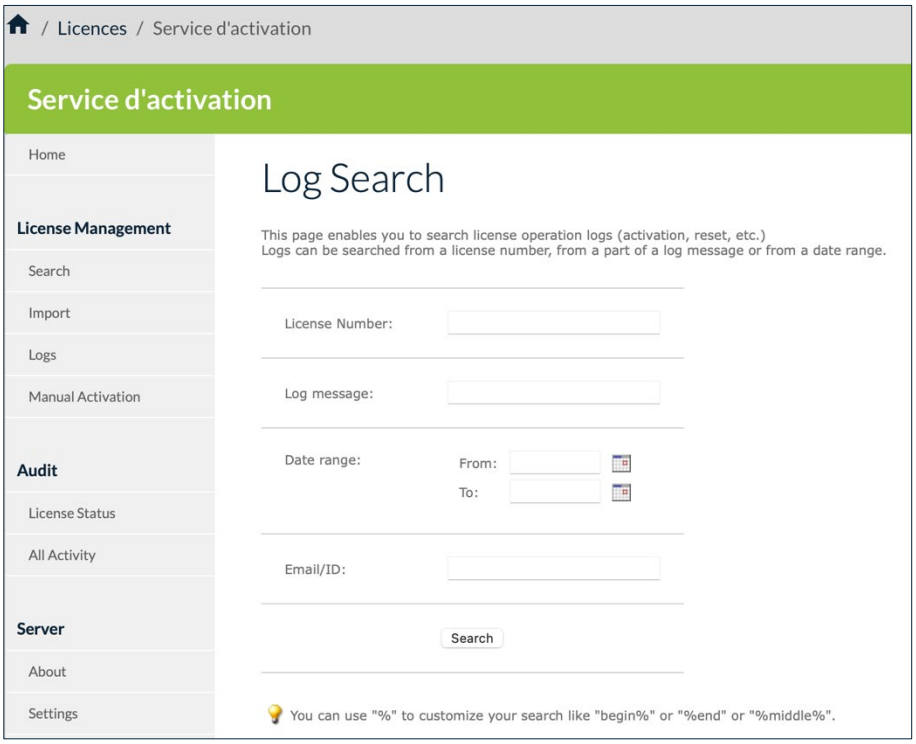
3. Tous les numéros de licence seront importés automatiquement et le message de confirmation suivant s'affichera sur la page **Results** (Résultats) :



Si le fichier de licence au format XML a été modifié ou que sa signature est incorrecte, une alerte s'affiche. Dans ce cas, contactez le support client : https://www.thegreenbow.com/fr/support/assistance/support-technique/.

6.3.3 Logs

L'option de menu **Logs** (Journaux) ouvre la page **Log Search** (Recherche dans les journaux).



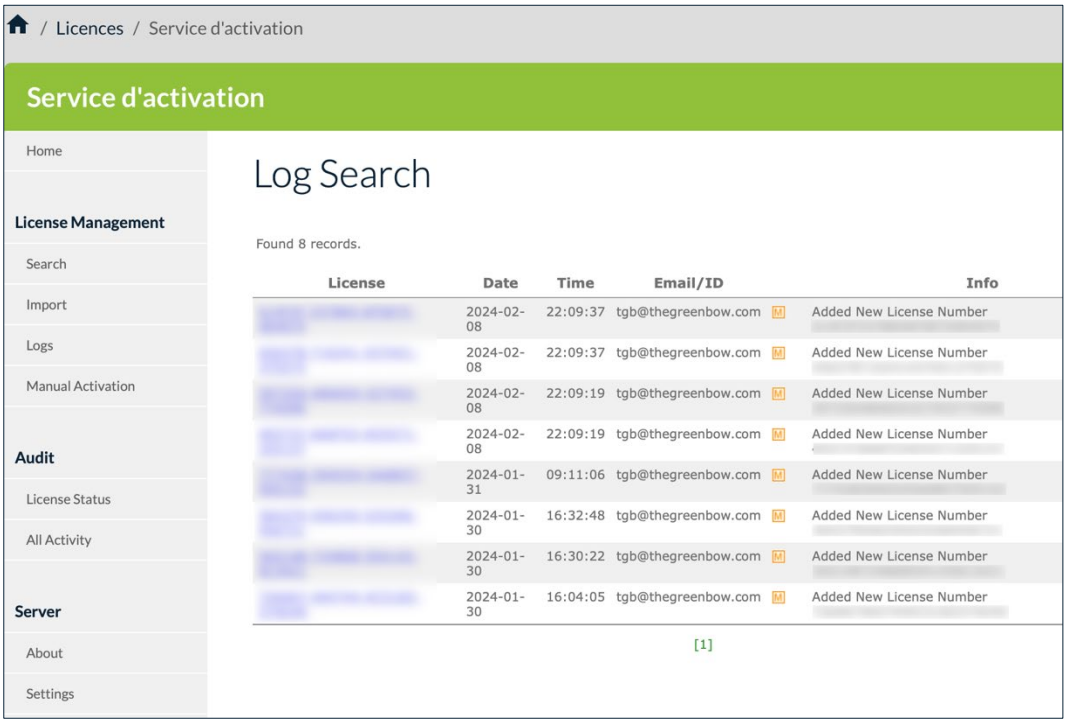
Le service d'activation vous permet d'effectuer des recherches dans les journaux d'activation de tout poste de travail.

Pour effectuer une recherche dans ces journaux, suivez les étapes ci-dessous :

1. Dans le menu de gauche, sous **License Management** (Gestion des licences), cliquez sur **Logs** (Journaux) pour afficher la page **Log Search** (Recherche dans les journaux).
2. Entrez un numéro de licence ou tout texte de journalisation qui a pu être enregistré, p. ex. "Added new" (Ajout nouveau), "License Number" (Numéro de licence) ou "Activation OK".

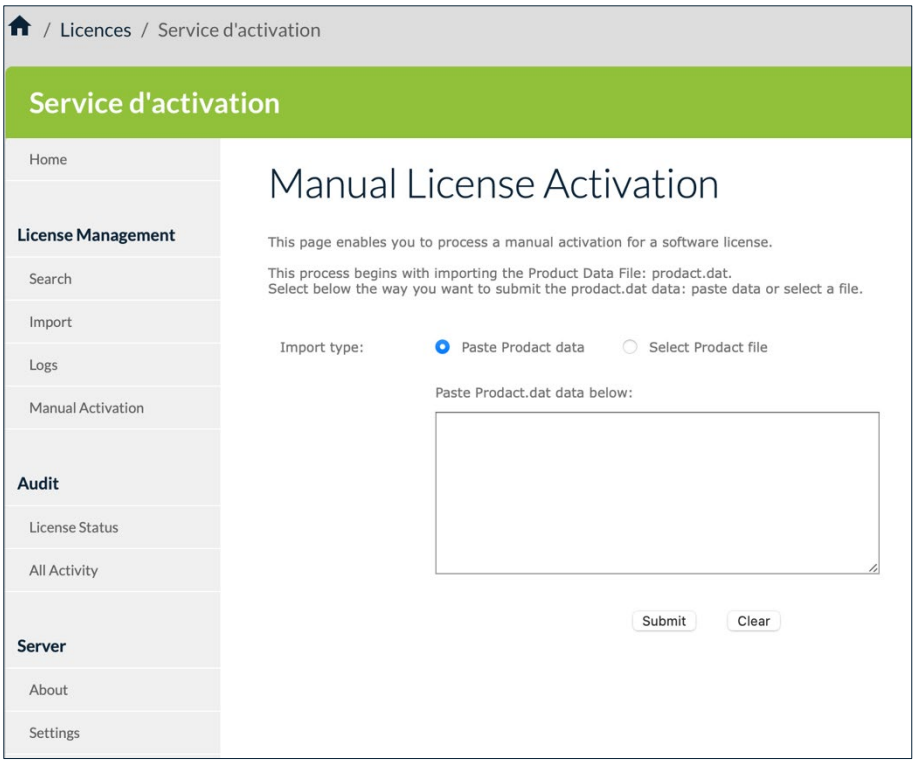
Pour tous les champs de la page **Log Search** (Recherche dans les journaux), vous pouvez utiliser le caractère générique « % » pour représenter un ou plusieurs caractères dans votre recherche, p. ex. « début% », « %fin » ou « %milieu% ».

3. Si votre recherche aboutit, vous verrez s'afficher une page comme la suivante :



6.3.4 Manual Activation

L'option de menu **Manual Activation** (Activation manuelle) ouvre la page **Manual License Activation** (Activation manuelle de licences).



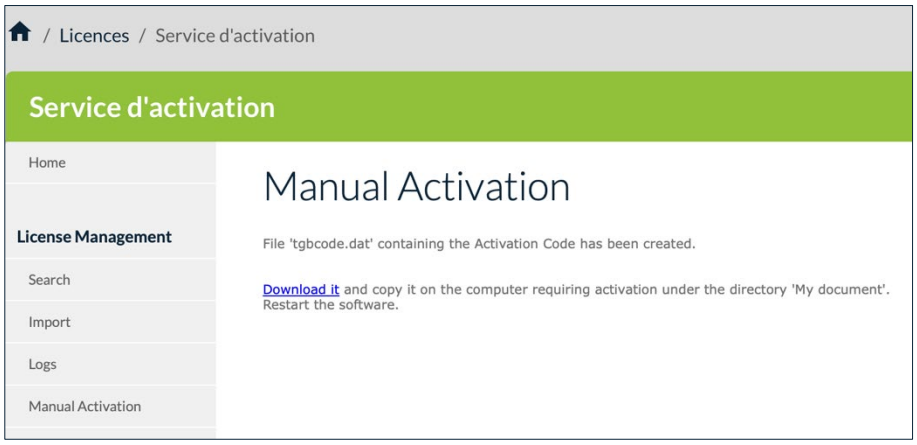
En plus de pouvoir activer automatiquement les licences logicielles en ligne, les responsables informatiques peuvent aussi activer les licences manuellement.

Pour traiter une activation manuelle, suivez les étapes ci-dessous :

1. Récupérez le fichier `prodact.dat` à partir de l'ordinateur sur lequel vous souhaitez activer le logiciel. Le fichier `prodact.dat` se trouve sous Documents (si votre OS est Windows). Il est généré à chaque tentative d'activation du logiciel.
2. Au niveau du service d'activation, dans le menu de gauche, sous **License Management** (Gestion des licences), cliquez sur **Manual Activation** (Activation manuelle) pour afficher la page **Manual License Activation** (Activation manuelle de licences).
3. Sous **Import type** (Type d'import), cliquez sur **Select Prodact file** (Sélectionner fichier Prodact). Un bouton **Parcourir...** (ou équivalent en fonction de votre navigateur) s'affiche. Cliquez sur **Parcourir...**, sélectionnez le fichier `prodact.dat` que vous souhaitez téléverser, puis cliquez sur **Submit** (Envoyer).

Vous pouvez également cliquer sur **Paste Prodact data** (Coller données Prodact), coller le contenu du fichier dans le champ prévu à cet effet, puis cliquer sur **Submit** (Envoyer).

4. Un fichier d'activation sera généré et proposé en téléchargement dans l'écran suivant :



5. Pour terminer le processus d'activation manuelle, cliquez sur **Download it** (Télécharger le fichier) et enregistrez le fichier d'activation dans le dossier à partir duquel vous avez récupéré le fichier `prodact.dat` sur le poste sur lequel vous souhaitez activer le logiciel. Le logiciel sera activé automatiquement au prochain démarrage.

Si vous rencontrez un problème au cours du processus d'activation, un message d'erreur s'affichera avec un code d'erreur. Pour plus d'informations sur les codes d'erreur d'activation, veuillez consulter notre section d'assistance sur notre site web : https://thegreenbow.com/fr/support/assistance/.

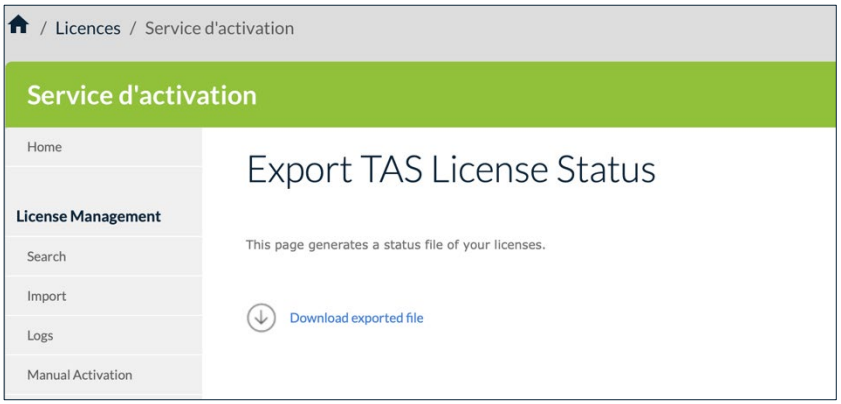
6.4 Audit

La rubrique **Audit** comprend les options de menu suivantes :

- **License Status** (Informations sur les licences) permet d'exporter l'état actuel des licences dans votre service d'activation (cf. section 6.4.1 License Status) ;
- **All Activity** (Toute l'activité) permet d'exporter un rapport d'activité (cf. section 6.4.2 All Activity).

6.4.1 License Status

L'option de menu **License Status** (Information sur les licences) ouvre la page **Export TAS License Status** (Exporter les informations sur les licences).



La page **Export TAS License Status** (Exporter les informations sur les licences) permet de générer un Rapport de situation sur les licences.

Le fichier exporté est au format CSV et contient les informations suivantes concernant chacune de vos licences :

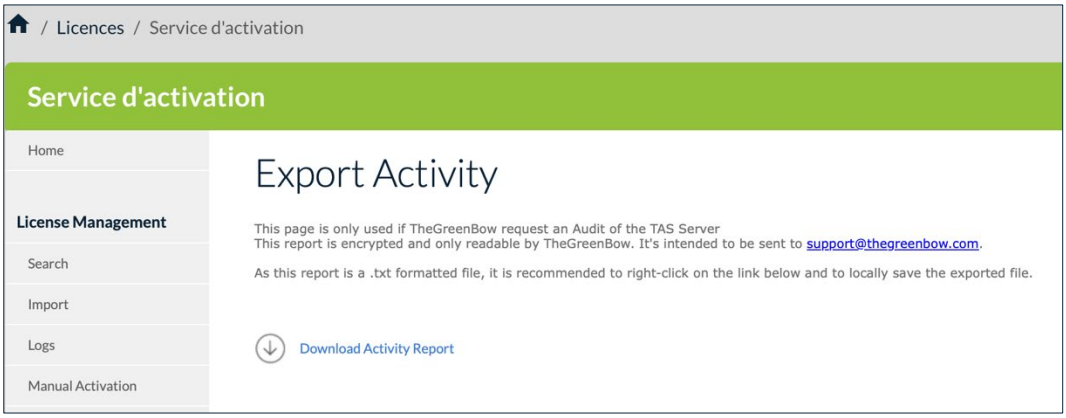
- numéro de licence,
- numéro de pack,
- nombre d'activations autorisées,
- nombre d'activations effectuées,
- nombre de réinitialisations,
- date d'expiration de la licence,
- nom de produit,
- signature.

Ce fichier CSV est sécurisé par une signature numérique.

Si notre équipe support vous demande de lui transmettre ce fichier, cliquez sur **Download exported file** (Télécharger le fichier exporté) pour télécharger le fichier CSV, puis envoyez-le à support@thegreenbow.com.

6.4.2 All Activity

L'option de menu **All Activity** (Toute l'activité) ouvre la page **Export Activity** (Exporter l'activité).



Cette page permet de générer, chiffrer, puis exporter un Rapport d'activité. Le rapport est destiné à notre équipe support.

Si notre équipe support vous demande de lui transmettre ce fichier, cliquez avec le bouton droit de la souris sur **Download Activity Report** (Télécharger le rapport d'activité) et sélectionnez **Enregistrer la cible du lien sous...** (ou équivalent en fonction de votre navigateur) pour enregistrer le fichier texte à l'emplacement de votre choix, puis envoyez-le à support@thegreenbow.com.

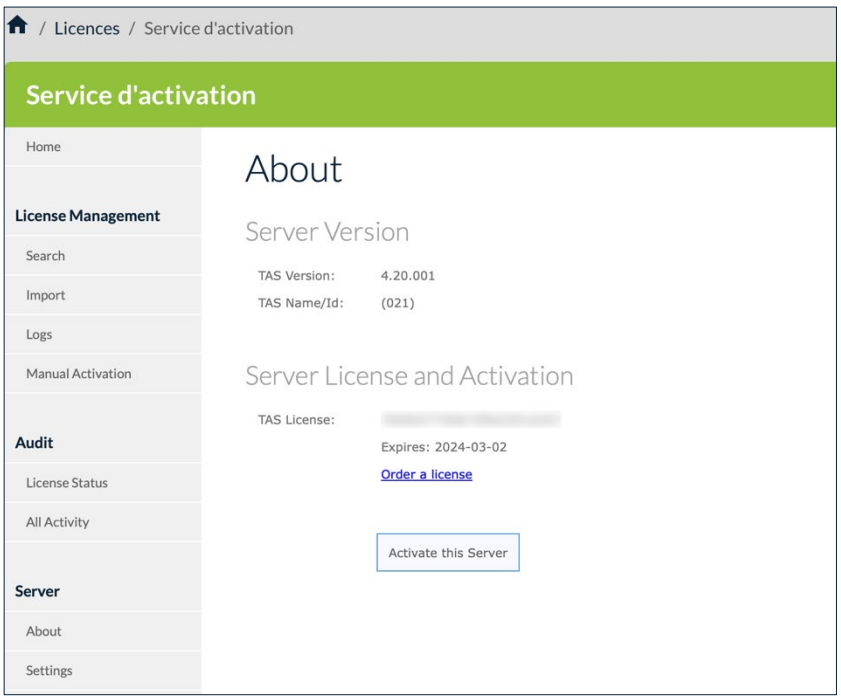
6.5 Server

La rubrique **Server** (Server) comprend les options de menu suivantes :

- **About** (À propos) affiche des informations sur la version et la licence du service d'activation (cf. section 6.5.1 About) ;
- **Settings** (Paramètres) permet de gérer les paramètres du service d'activation (cf. section 6.5.2 Settings).

6.5.1 About

L'option de menu **About** (À propos) ouvre la page **About** (À propos).



Cette page affiche des informations sur la version et la licence du serveur.

Elle permet aussi de réactiver le service après avoir renouvelé un abonnement. Pour cela, cliquez sur **Activate this Server** (Activer ce serveur).

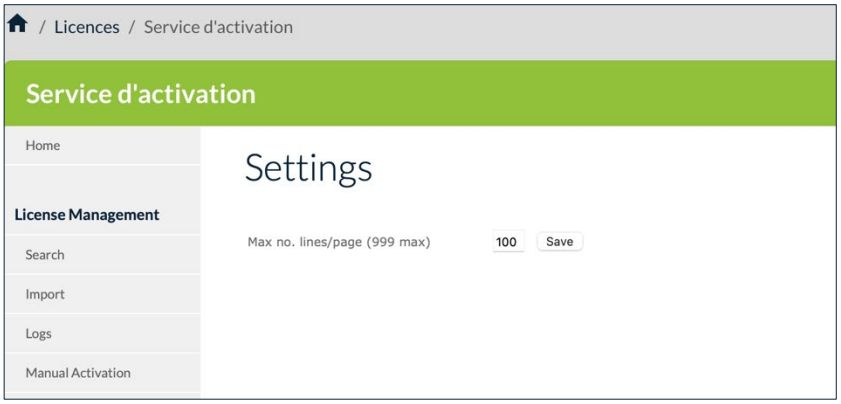
Si vous devez renouveler votre licence, cliquez sur **Order a license** (Commander une licence). Cela ouvrira un nouveau courrier électronique dans votre client de messagerie par défaut, vous permettant d'envoyer un e-mail à notre équipe commerciale.

6.5.2 Settings

L'option de menu **Settings** (Paramètres) ouvre la page **Settings** (Paramètres). Celle-ci vous permet de définir le nombre de lignes par page.

Pour accéder à la page **Settings** (Paramètres), dans le menu de gauche, sous **Server** (Serveur), cliquez sur **Settings** (Paramètres).

La page **Settings** (Paramètres) s'affiche :



Si une recherche retourne une très grande quantité de données, vous pouvez définir le nombre de lignes affichées par page web sous **Max no. lines/page (999 max)** (Nombre max. de lignes/page (999 max.)). Le nombre de lignes par page ne peut pas dépasser 999.

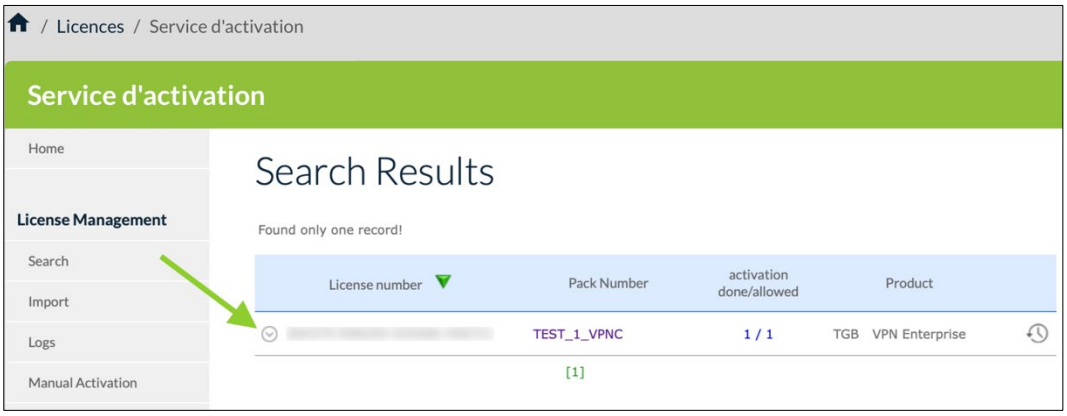
6.6 Réinitialisation des numéros de licence

En cas de perte d'un ordinateur ou d'un disque dur endommagé, le service d'activation vous permet de réinitialiser l'activation d'une licence afin de pouvoir la réutiliser pour l'activation sur un autre poste.

6.6.1 Réinitialisation d'une activation unique

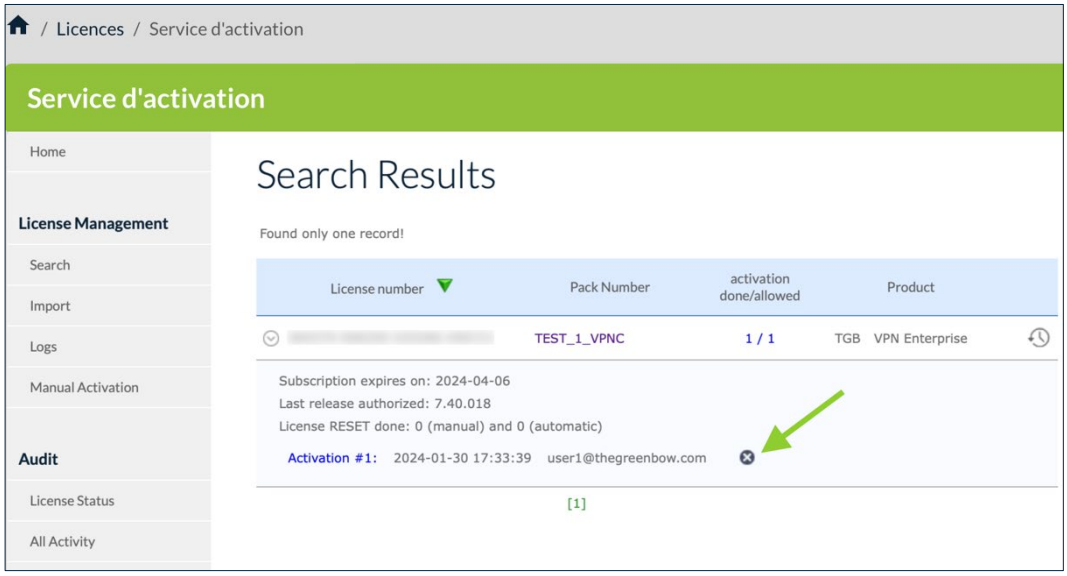
Pour réinitialiser une activation unique, procédez de la manière suivante :

1. Dans le menu de gauche, sous **License Management** (Gestion des licences), cliquez sur **Search** (Rechercher) pour afficher la page **Search License Numbers** (Recherche de numéros de licence).
2. Utilisez l'un des champs de recherche pour rechercher la licence qui doit être réinitialisée afin de pouvoir l'activer sur un autre poste. Vous pouvez rechercher des licences en fonction de l'e-mail d'activation ou du numéro de licence lui-même (cf. section 6.3.1 Search). La page **Search Results** (Résultats de la recherche) s'affiche :



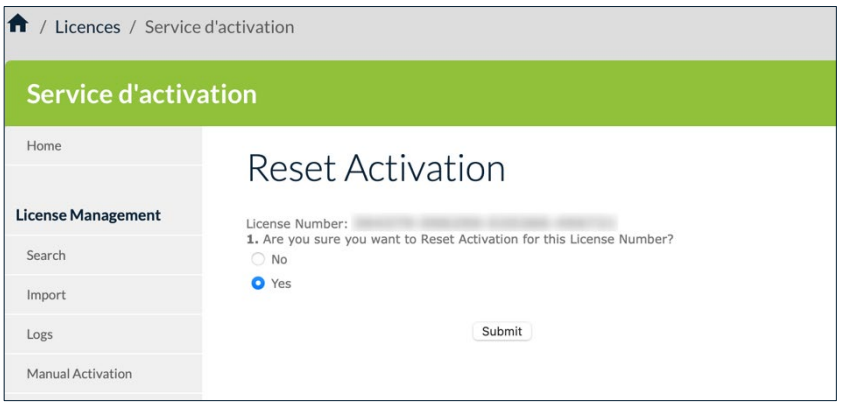
3. Cliquez sur l'icône en forme de flèche à côté du numéro de licence pour afficher les détails concernant cette activation.

   La page se présente alors comme suit :

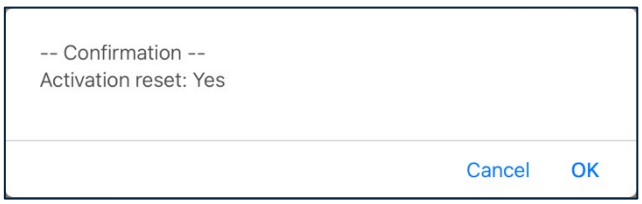


4. Cliquez sur l'icône de réinitialisation (⊗) à droite de l'activation que vous souhaitez réinitialiser.

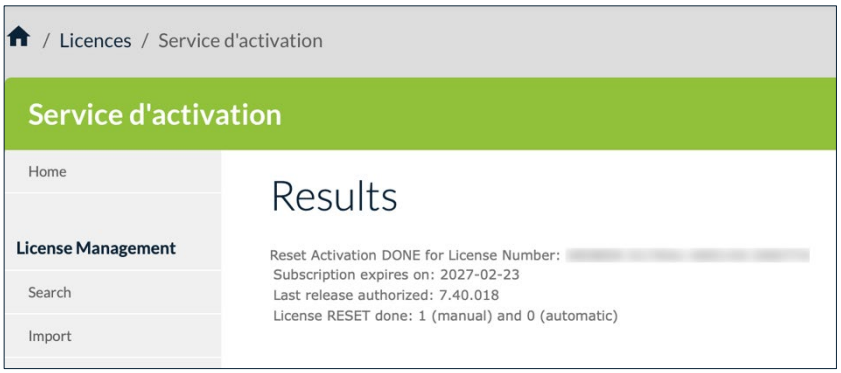
   La page **Reset Activation** (Réinitialiser l'activation) s'affiche :



5. Sélectionnez **Yes** (Oui), puis cliquez sur **Submit** (Envoyer). Le message de confirmation suivant s'affiche :



6. Cliquez sur **OK**. La page **Results** (Résultats) s'affiche avec des informations sur la réinitialisation que vous venez d'effectuer :

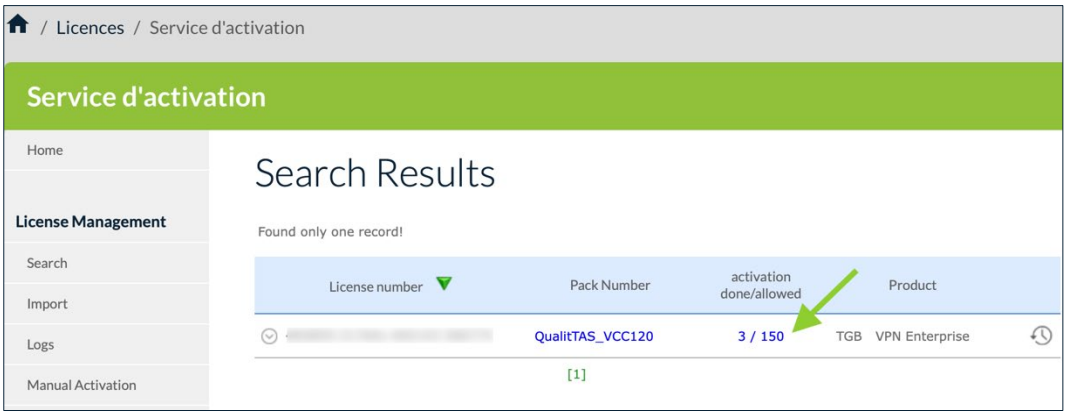


Vous avez réussi la réinitialisation de l'activation pour cette licence. Vous pouvez activer la licence sur un autre poste.

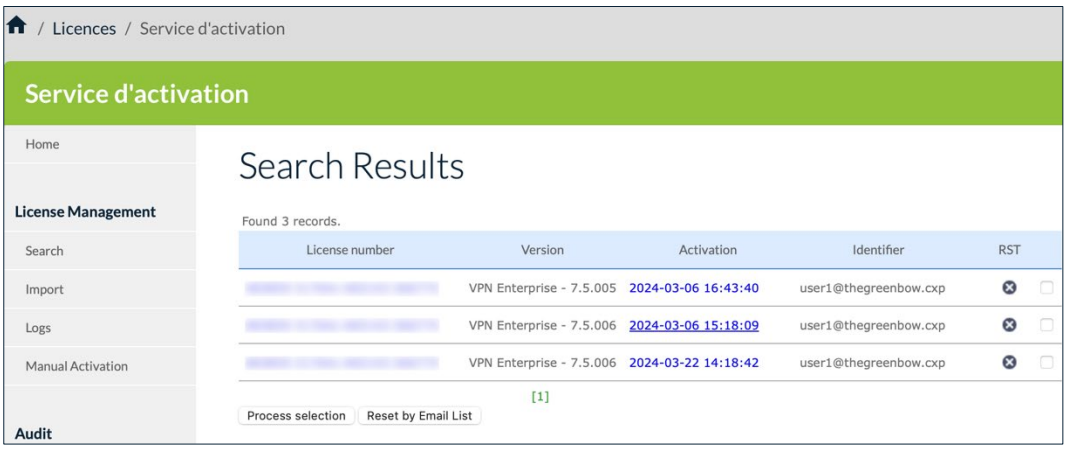
6.6.2 Réinitialisation de plusieurs activations

Pour réinitialiser plusieurs activations, procédez de la manière suivante :

1. Reprenez les étapes 1 et 2 de la section 6.6.1 Réinitialisation d'une activation unique pour rechercher une licence ou un groupe de licences.



2. Sur la page **Search Results** (Résultats de recherche), cliquez sur les chiffres dans la colonne **activation done/allowed** (activation effectuée/autorisée). Une nouvelle vue de la page **Search Results** (Résultats de la recherche) s'affiche avec toutes les activations pour la licence correspondante :



3. Réinitialisez une ou plusieurs activations de l'une des manières suivantes :
    - cliquez sur l'icône de réinitialisation (⊗) dans la colonne **RST** sur la ligne correspondant à l'activation que vous souhaitez réinitialiser ;
    - cochez la case à la fin de chaque ligne que vous souhaitez réinitialiser, puis cliquez sur **Process selection** (Traiter la sélection) ;
    - cliquez sur le bouton **Reset by Email List** (Réinitialiser par liste d'e-mails).

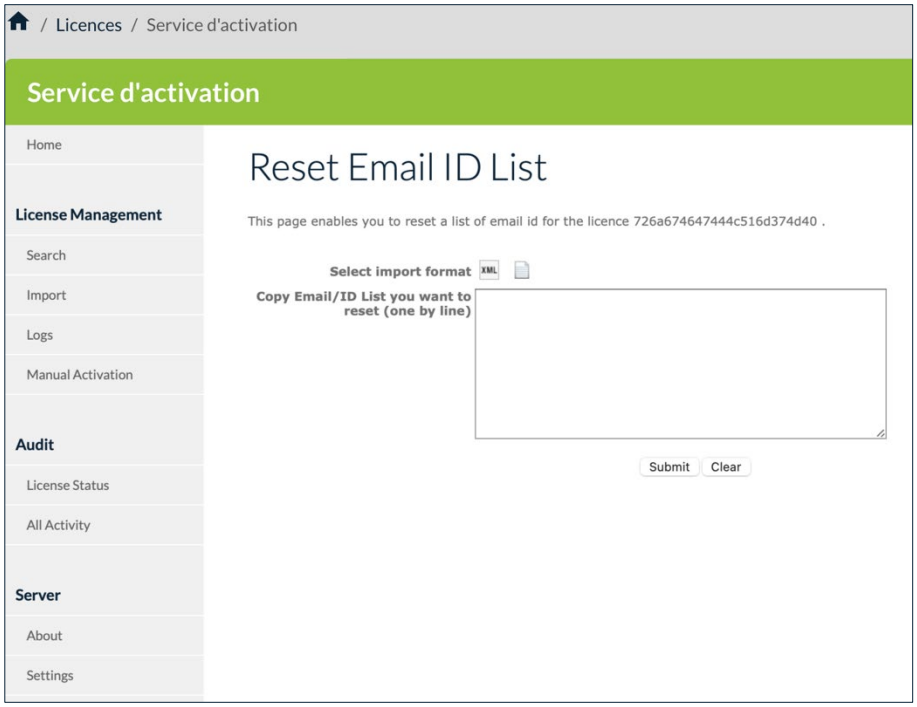
Dans les deux premiers cas, la page **Reset Activation** (Réinitialiser l'activation) s'affiche pour confirmer votre demande (comme à l'étape 4 de la section 6.6.1 Réinitialisation d'une activation unique ci-dessus). Sélectionnez **Yes** (Oui), puis cliquez sur **Submit** (Envoyer). Une invite de commande s'affiche vous demandant de confirmer une dernière fois avant d'effectuer la réinitialisation.

Dans le troisième cas, la page **Reset Email ID List** (Réinitialiser liste d'identifiants / e-mails) s'affiche (cf. section 6.6.3 Réinitialisation d'activations à partir d'une liste d'identifiants / d'adresses e-mail ci-dessous).

6.6.3 Réinitialisation d'activations à partir d'une liste d'identifiants / d'adresses e-mail

Pour réinitialiser des activations à partir d'une liste d'identifiants / d'adresses e-mail, procédez de la manière suivante :

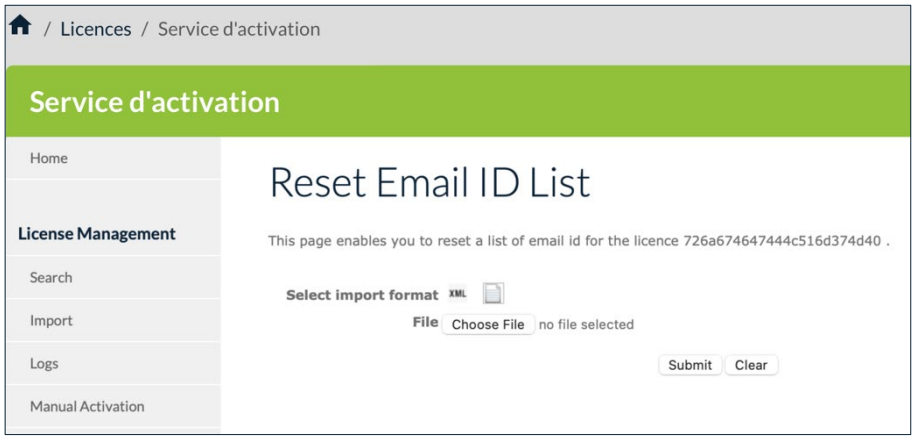
1. Reprenez les étapes 1 et 2 de la section 6.6.2 Réinitialisation de plusieurs activations pour rechercher une licence ou un groupe de licences.
2. Cliquez sur le bouton **Reset by Email List** (Réinitialiser par liste d'e-mails). La page **Reset Email ID List** (Réinitialiser liste d'identifiants / e-mails) s'affiche :



3. Collez une liste d'identifiants / d'adresses e-mail que vous souhaitez réinitialiser dans le champ prévu à cet effet (un par ligne), puis cliquez sur **Submit** (Envoyer).

   Vous pouvez également cliquer sur l'icône représentant un fichier pour sélectionner un fichier contenant une liste d'identifiants / d'adresses e-mail que vous souhaitez réinitialiser. La vue de la page **Reset Email ID**

List (Réinitialiser liste d'identifiants / e-mails) change et se présente désormais comme suit :



Cliquez sur **Browse** (Parcourir), sélectionnez le fichier souhaité, puis cliquez sur **Submit** (Envoyer).

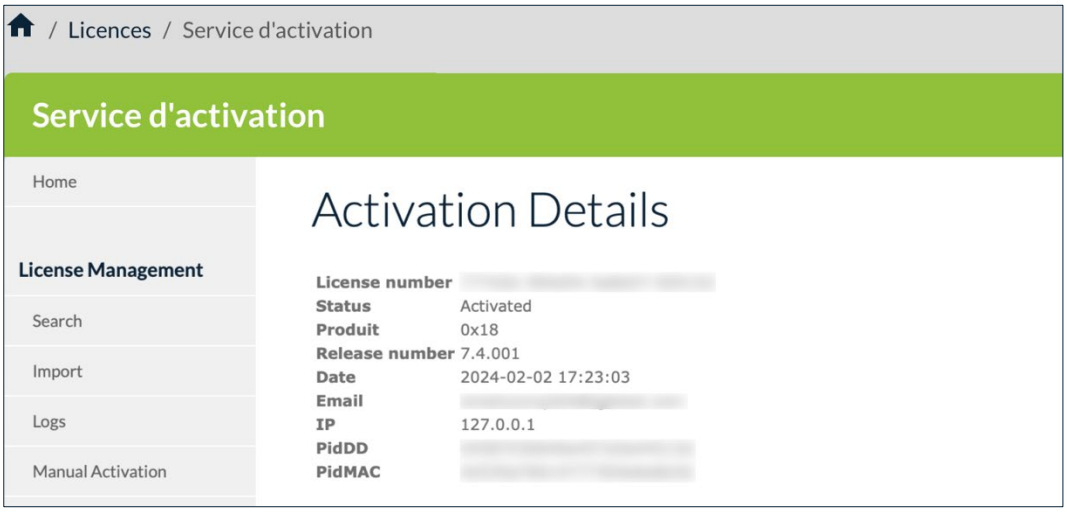
4. Dans les deux cas, la page **Reset Activation** (Réinitialiser l'activation) s'affiche, après avoir cliqué sur **Submit** (Envoyer), pour vous demander de confirmer votre demande (de la même manière qu'à l'étape 4 de la section 6.6.1 Réinitialisation d'une activation unique ci-dessus). Sélectionnez **Yes** (Oui), puis cliquez sur **Submit** (Envoyer). Une invite de commande s'affiche vous demandant de confirmer une dernière fois avant d'effectuer la réinitialisation.

6.6.4 Affichage des détails de l'activation

Vous pouvez afficher une page **Activation Details** (Détails de l'activation) avec plus de détails sur une activation donnée. Pour cela, procédez de l'une des manières suivantes :

- À partir de la page **Search Results** (Résultats de la recherche), cliquez sur l'icône en forme de flèche à côté du numéro de licence pour afficher les détails concernant cette activation. Maintenant, cliquez sur le lien correspondant à l'activation pour laquelle vous souhaitez afficher les détails.
- À partir de la page **Search Results** (Résultats de la recherche), cliquez sur les chiffres dans la colonne **activation done/allowed** (activation effectuée/autorisée) pour afficher la liste des activations pour cette licence. Maintenant, cliquez sur la date d'activation dans la colonne **Activation**.

Dans les deux cas, une page **Activation Details** (Détails de l'activation), comme celle présentée à titre d'exemple ci-dessous, s'affiche :



6.7 Actions courantes de gestion des licences

6.7.1 Introduction

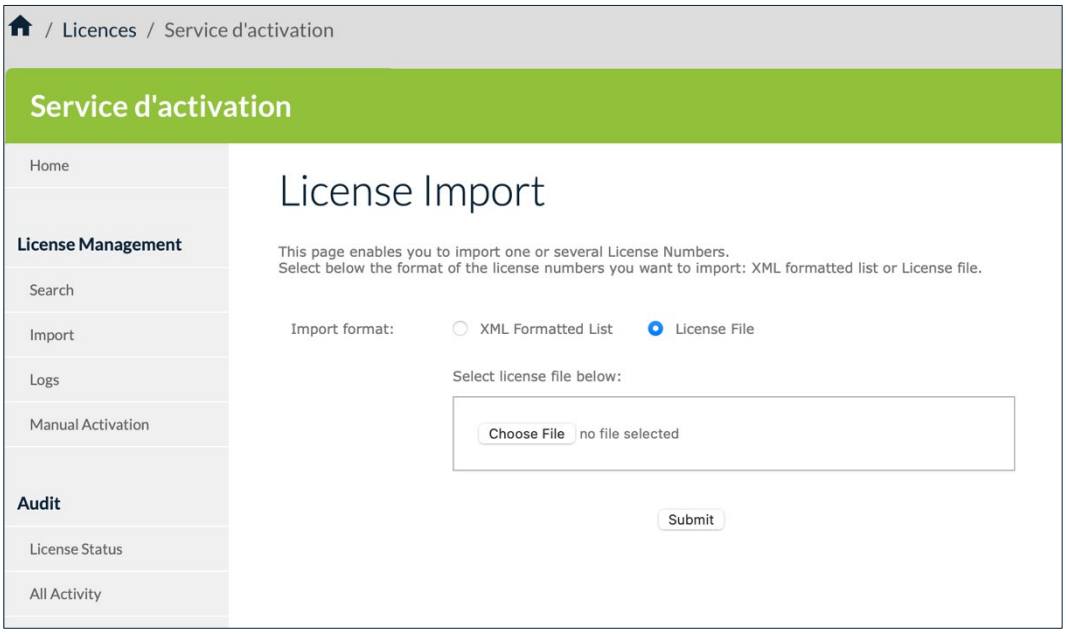
Ci-dessous, vous trouver une description succincte des actions les plus courantes que vous pouvez effectuer avec le service d'activation.

6.7.2 Importer des numéros de licence

À l'installation, le service d'activation ne contient aucun numéro de licence de Client VPN. TheGreenBow fournira vos numéros de licence dans des fichiers XML que vous pouvez importer.

Pour importer un fichier de licence au format XML, procéder de la manière suivante :

1. Dans le menu de gauche, sous **License Management** (Gestion des licences), cliquez sur **Import** (Importer) pour afficher la page **License Import** (Importation de licences).

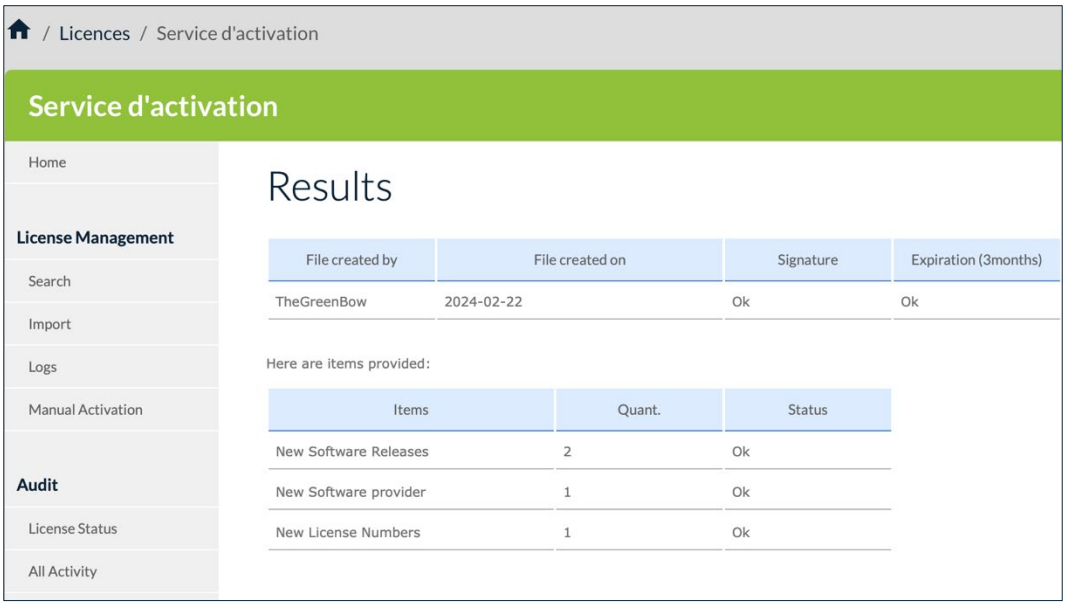


2. Sous **Import format** (Format d'importation), cliquez sur **License File** (Fichier de licence). Un bouton **Parcourir...** (ou équivalent en fonction de votre navigateur) s'affiche. Cliquez sur **Parcourir...**, sélectionnez le fichier de licence au format XML que vous souhaitez téléverser, puis cliquez sur **Submit** (Envoyer).

   Vous pouvez également cliquer sur **XML Formatted List** (Liste au format XML), coller le contenu du fichier dans le champ prévu à cet effet, puis cliquer sur **Submit** (Envoyer).

Vous pouvez également cliquer sur **XML Formatted List** (Liste au format XML), coller le contenu du fichier dans le champ prévu à cet effet, puis cliquer sur **Submit** (Envoyer).

3. Tous les numéros de licence seront importés automatiquement et une page **Results** (Résultats) s'affichera avec des informations similaires aux suivantes :

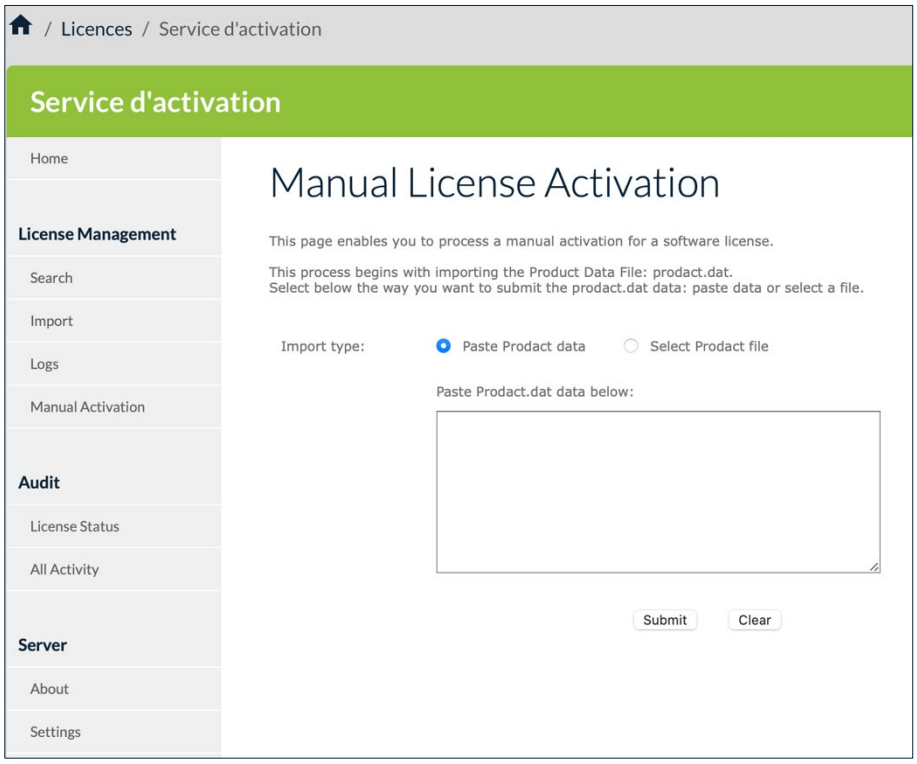


Si le fichier de licence au format XML a été modifié ou que sa signature est incorrecte, une alerte s'affiche. Dans ce cas, contactez le support technique https://www.thegreenbow.com/fr/support/assistance/support-technique.

6.7.3 Activer manuellement une licence

Pour activer manuellement une licence, procédez comme suit :

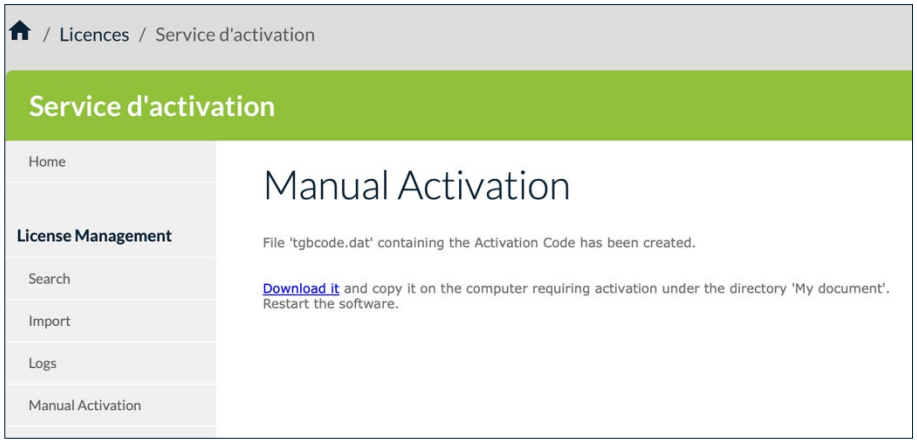
1. Récupérez le fichier `prodact.dat` à partir de l'ordinateur sur lequel vous souhaitez activer le logiciel. Le fichier `prodact.dat` se trouve sous **Documents** (si votre OS est Windows). Il est généré à chaque tentative d'activation du logiciel.
2. Dans le menu principal du CMC, sous **LICENCES**, sélectionnez **Serveur d'activation**.
3. Dans le menu de gauche du service d'activation, sous **License Management** (Gestion des licences), sélectionnez **Manual Activation** (Activation manuelle) pour afficher la page **Manual License Activation** (Activation manuelle de licences).



4. Sous **Import type** (Type d'import), cliquez sur **Select Prodact file** (Sélectionner fichier Prodact). Un bouton **Parcourir...** (ou équivalent en fonction de votre navigateur) s'affiche. Cliquez sur **Parcourir...**, sélectionnez le fichier `prodact.dat` que vous souhaitez téléverser, puis cliquez sur **Submit** (Envoyer).

Vous pouvez également cliquer sur **Paste Prodact data** (Coller données Prodact), coller le contenu du fichier dans le champ prévu à cet effet, puis cliquer sur **Submit** (Envoyer).

5. Un fichier d'activation sera généré et proposé en téléchargement dans l'écran suivant :



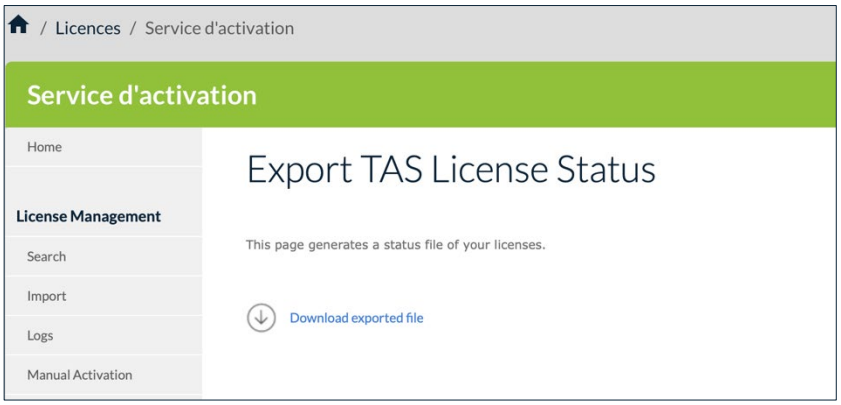
6. Pour terminer le processus d'activation manuelle, cliquez sur le lien de téléchargement **Download it** (Télécharger le fichier) et enregistrez le fichier d'activation dans le dossier à partir duquel vous avez récupéré le fichier `prodact.dat` sur le poste sur lequel vous souhaitez activer le logiciel. Le logiciel sera activé automatiquement au prochain démarrage.

Si vous rencontrez un problème au cours du processus d'activation, un message d'erreur s'affichera avec un code d'erreur. Pour plus d'informations sur les codes d'erreur d'activation, veuillez consulter notre section d'assistance sur notre site web : https://thegreenbow.com/fr/support/assistance/.

6.7.4 Générer un fichier d'état des licences

Pour générer un fichier d'état des licences, procédez comme suit :

1. Dans le menu de gauche, sous **Audit**, sélectionnez **License Status** (Information sur les licences) pour afficher la page **Export TAS License Status** (Exporter les informations sur les licences).



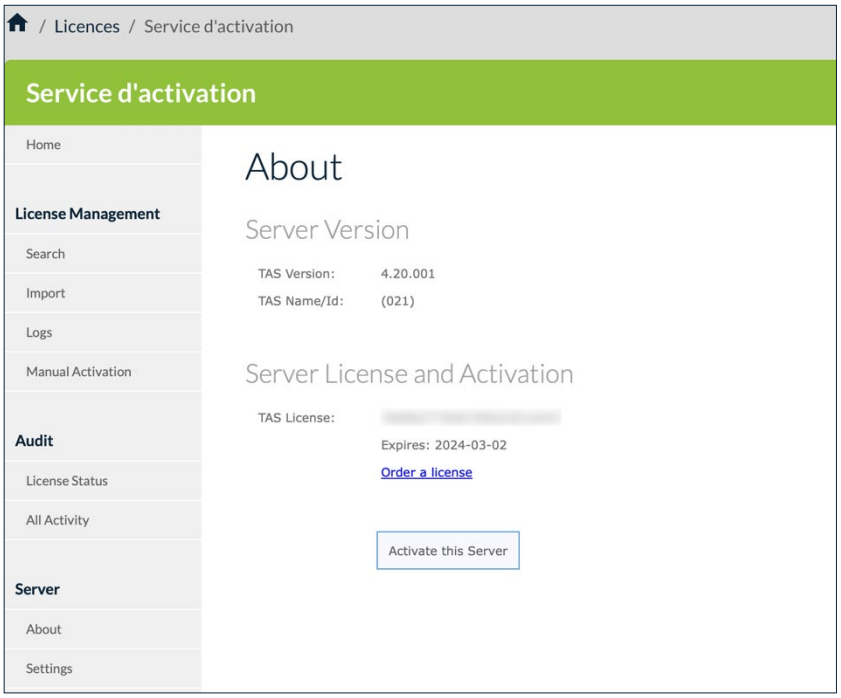
2. Cliquez sur le lien de téléchargement **Download exported file** (Télécharger le fichier exporté) pour télécharger le fichier CSV.
3. Exploitez ce fichier pour vos besoins ou envoyez-le à notre équipe support lorsqu'elle vous demande de le lui transmettre.

☞ Pour plus d'informations sur les informations que contient le fichier d'état des licences, reportez-vous à la section 6.4.1 License Status.

6.7.5 Consulter les informations du service d'activation

Pour consulter des informations sur la version, la licence et l'activation du service d'activation, procédez comme suit :

1. Dans le menu de gauche, sous **Server** (Serveur), sélectionnez **About** (À propos) pour afficher la page **About** (À propos).

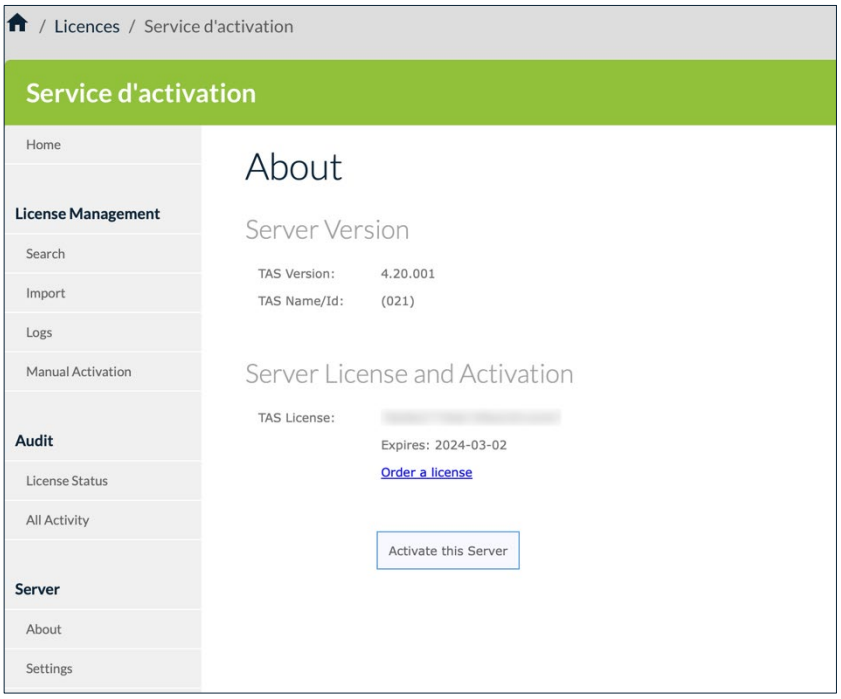


2. Relevez les informations qui vous intéressent, p. ex. la version du service d'activation ou la date d'expiration de la licence.

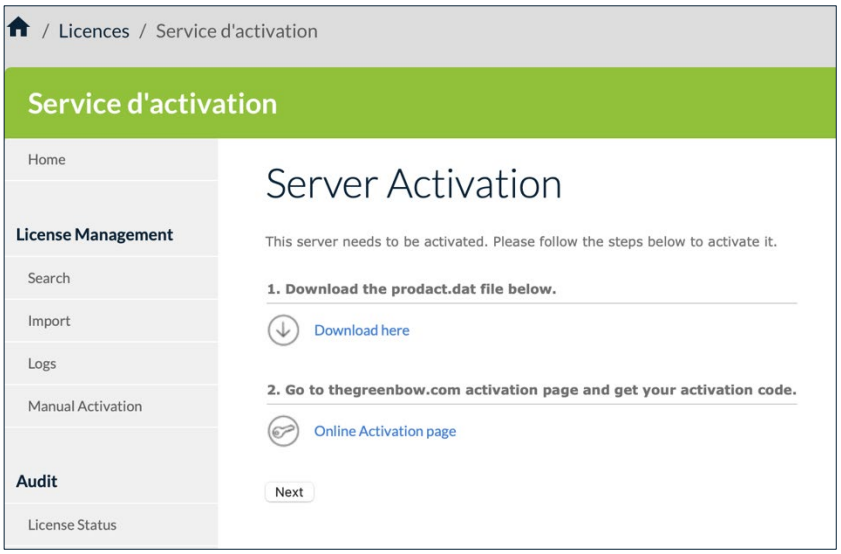
6.7.6 Réactiver le service d'activation

Pour réactiver le service après avoir renouvelé un abonnement, procédez comme suit :

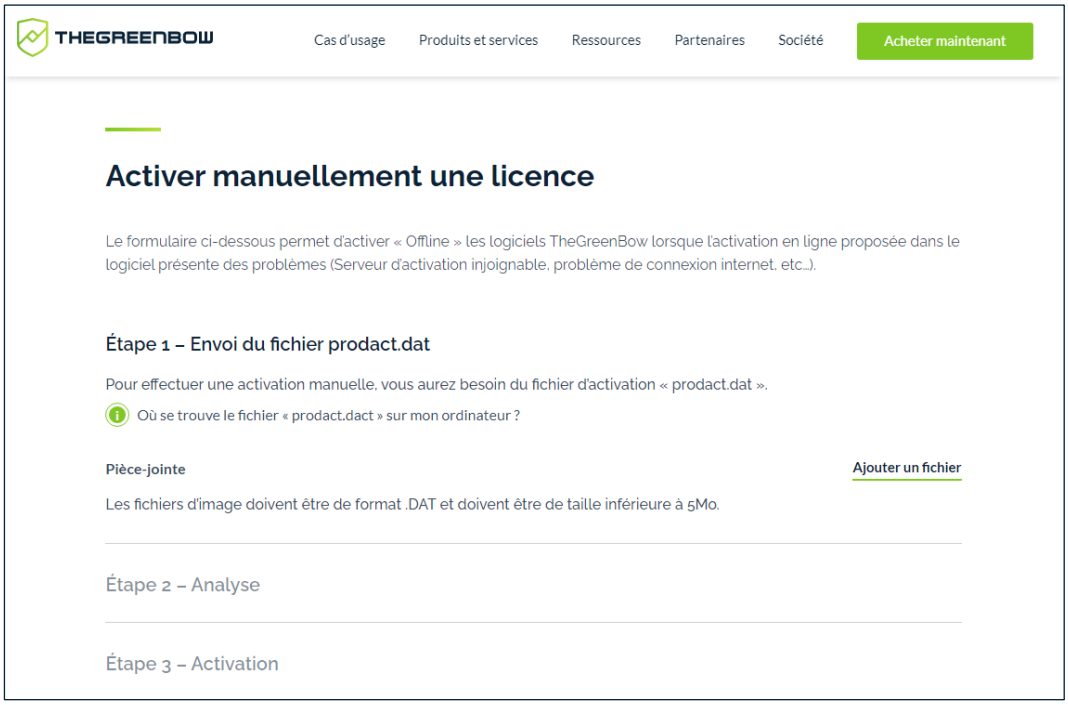
1. Dans le menu de gauche, sous **Server** (Serveur), sélectionnez **About** (À propos) pour afficher la page **About** (À propos).



2. Cliquez sur **Activate this Server** (Activer ce serveur). La page **Server Activation** (Activation du serveur) s'affiche :

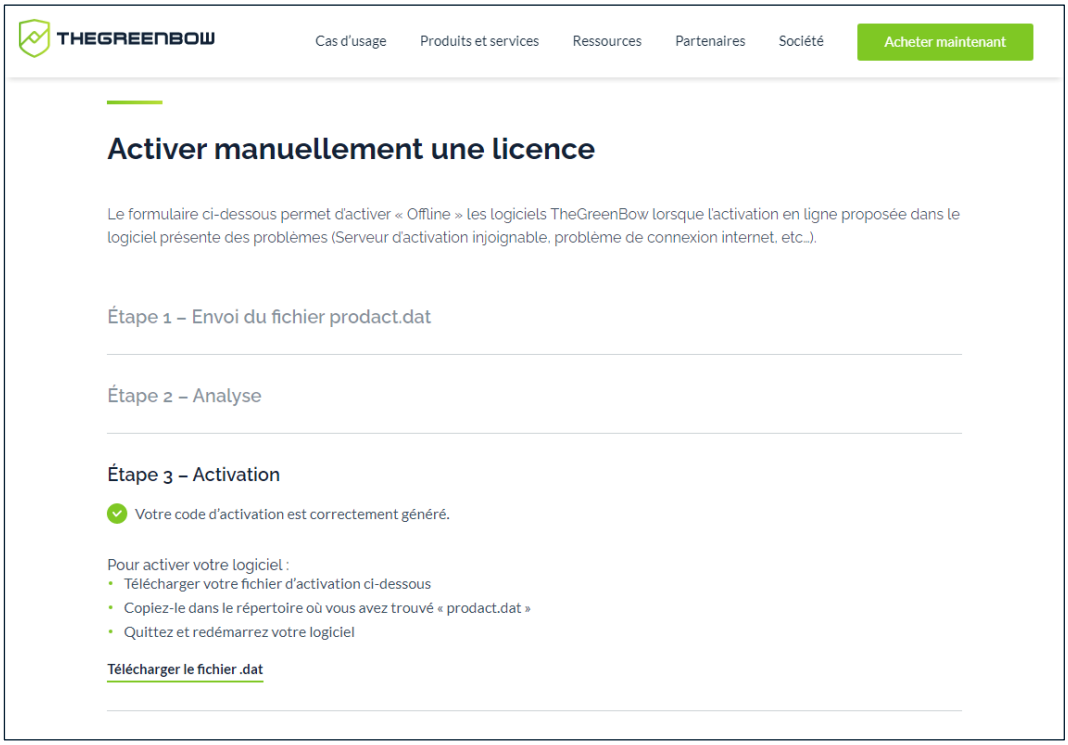


3. Cliquez sur le lien de téléchargement **Download here** (Télécharger ici) pour télécharger le fichier `prodact.dat` du service d'activation.
4. Si votre CMC est sur un réseau disposant d'un accès à internet, cliquez sur le lien **Online Activation page** (Page d'activation en ligne). La page d'activation en ligne du site TheGreenBow s'affiche :



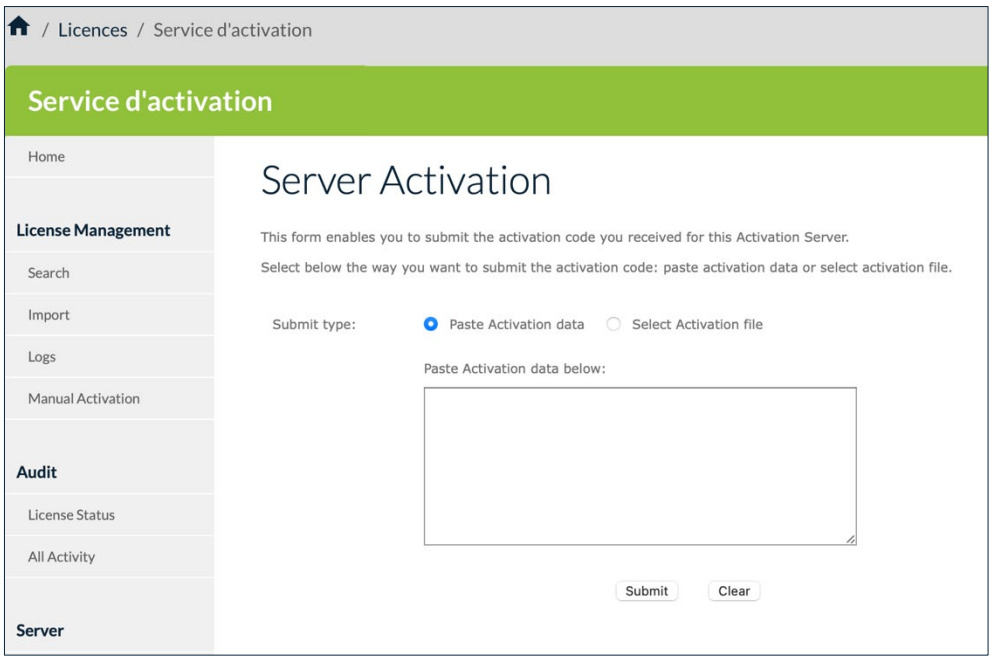
Si votre CMC se situe sur un réseau ne disposant pas d'un accès à internet, transférez le fichier `prodact.dat` vers un poste connecté à internet et ouvrez la page d'activation en ligne dans un navigateur.

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

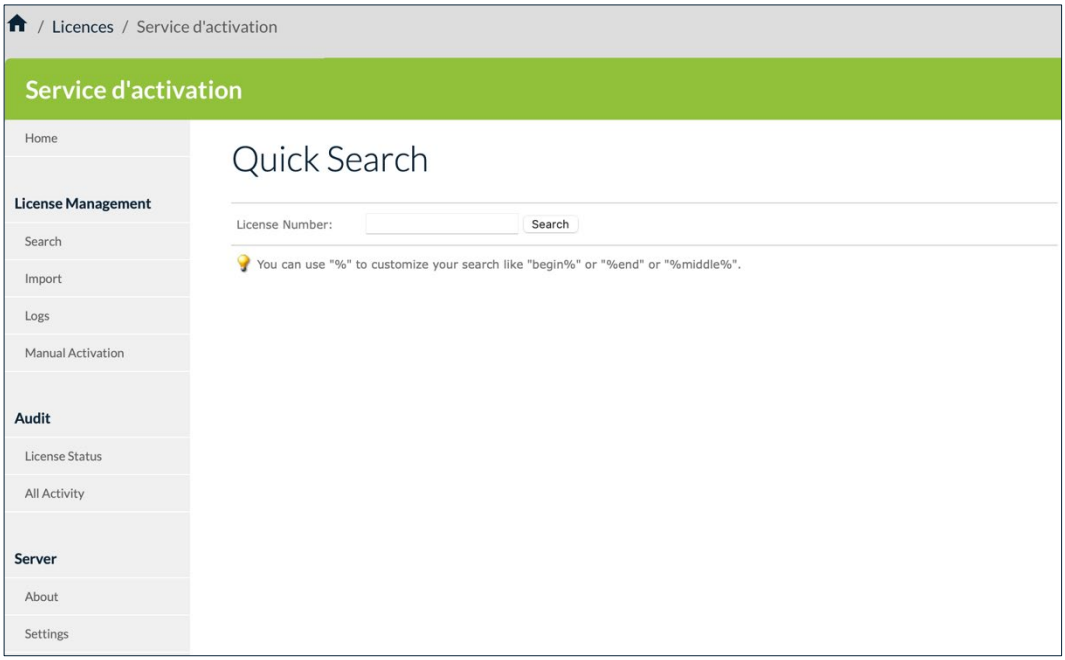


Ce fichier a un nom de la forme : `tgbcode_[date]_[code].dat` (par exemple : `tgbcode__20240415_1029.dat`).

8. Téléchargez ou transférez le fichier `tgbcode_[date]_[code].dat` sur le CMC pour lequel vous souhaitez activer le service d'activation.
9. Revenez à la page **Server Activation** (Activation du serveur) du service d'activation, puis cliquez sur **Next** (Suivant). Le formulaire suivant s'affiche dans la page **Server Activation** (Activation du serveur).



10. Cliquez sur **Select Activation file** (Sélectionner le fichier d'activation). Un bouton **Parcourir...** (ou équivalent en fonction de votre navigateur) s'affiche. Cliquez sur **Parcourir...** et sélectionnez le fichier d'activation à partir de l'emplacement où vous l'avez enregistré. Cliquez ensuite sur **Submit** (Envoyer). La page **Home** (Accueil) du service d'activation s'affiche :

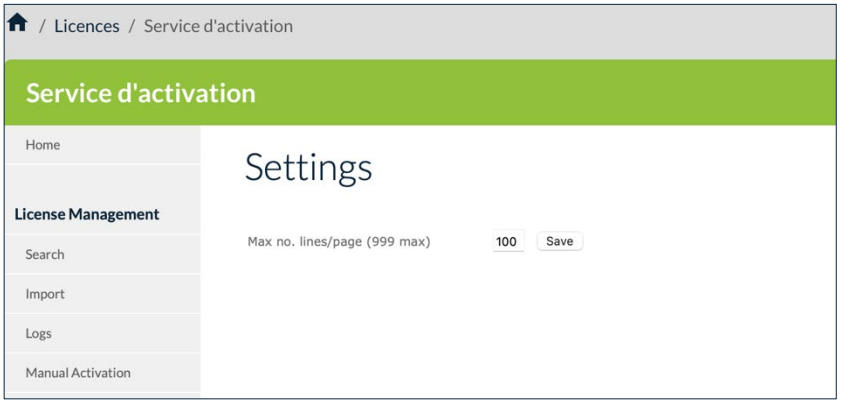


Vous avez réactivé le service d'activation. La date d'expiration de la licence a été mise à jour.

6.7.7 Modifier le nombre de lignes affichées par page

Pour modifier le nombre de lignes affichées par page, procédez comme suit :

1. Dans le menu de gauche, sous **Server** (Serveur), sélectionnez **Settings** (Paramètres) pour afficher la page **Settings** (Paramètres).



2. Saisissez le nombre maximal de lignes que vous souhaitez voir affichées par page.
3. Cliquez sur **Save** (Enregistrer).

7 Supervision

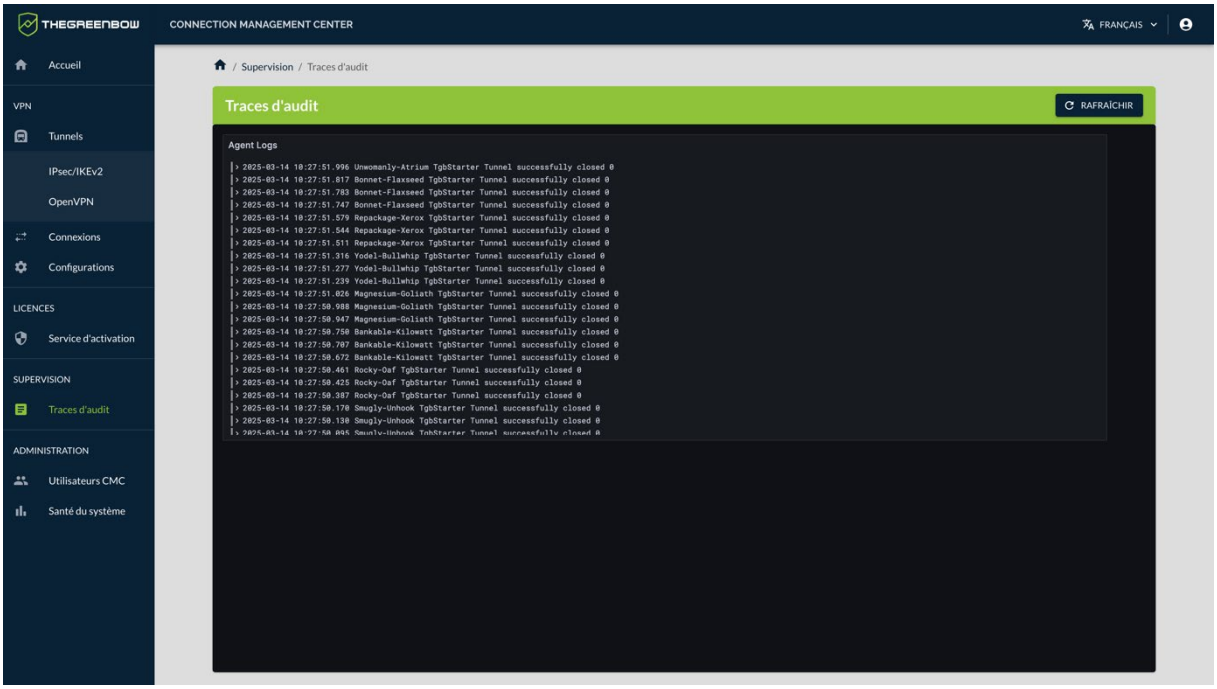
7.1 Présentation

La rubrique **SUPERVISION** du menu principal contient une seule page **Traces d'audit** destinée au suivi des logs remontés par les Secure Connection Agents (SCA) installés sur les postes de travail du parc. La communication entre le SCA et le CMC est sécurisé sur la base d'une méthode d'authentification mutuelle appelée TLS mutuel ou mTLS.

☞ Reportez-vous au « Guide de l'administrateur » du SCA pour une description détaillée de cette fonctionnalité et de sa mise en place.

7.2 Traces d'audit

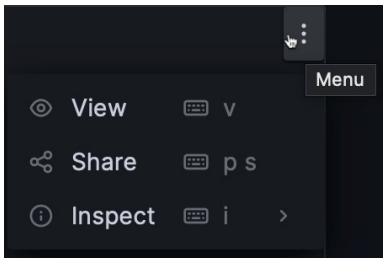
Pour afficher la fenêtre **Traces d'audit**, dans le menu principal, sous la rubrique **SUPERVISION**, sélectionnez **Traces d'audit**. La page **Traces d'audit** s'affiche :



La page **Traces d'audit** présente un tableau de bord constitué d'une liste agrégée, nommée **Agent Logs**. Celle-ci contient tous les logs remontés par les Secure Connection Agents (SCA) installés sur les postes de travail du parc informatique au cours de la dernière heure.

Un menu contextuel dans le coin supérieur droit des panneaux du tableau de bord s'affiche au survol avec le pointeur de la souris. Cliquez sur le

pictogramme **Menu** avec les trois points verticaux pour développer le menu :



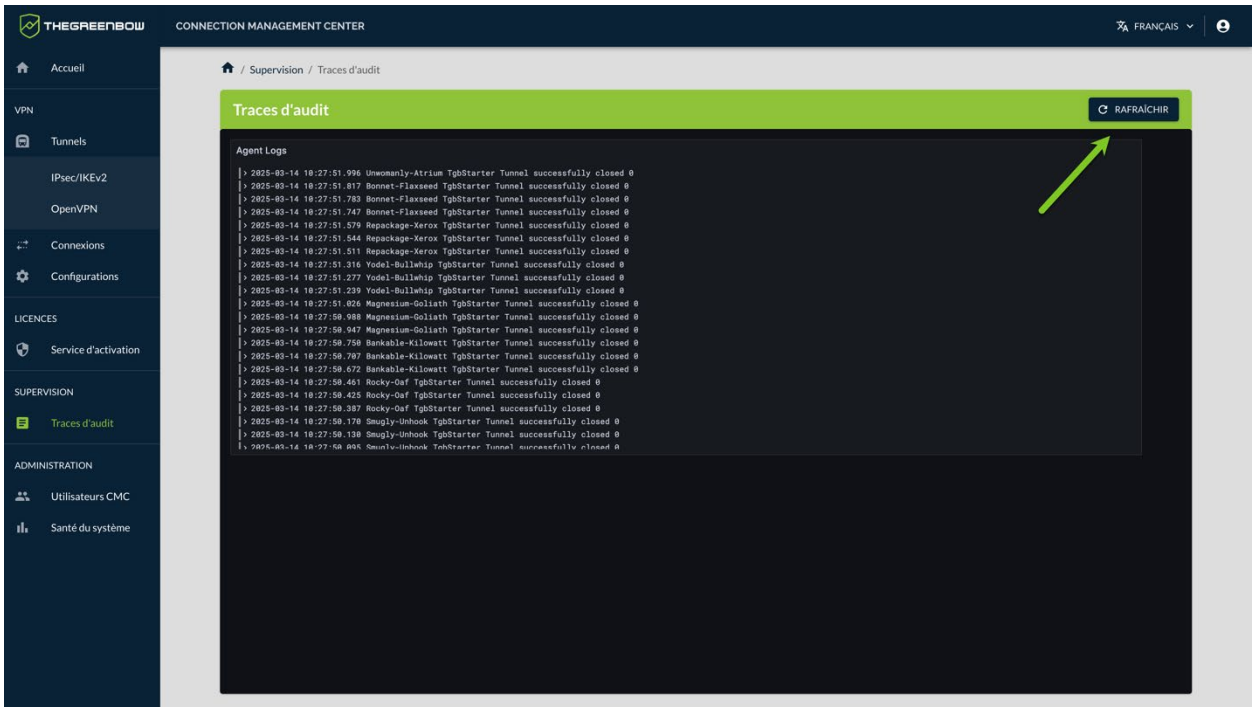
Ce menu permet d'agrandir l'affichage, de partager les données, de visualiser les données, de consulter des statistiques et de télécharger les données aux formats CSV et TXT.

Dans la liste **Agent Logs**, cliquez sur le pictogramme **See log details** au début d'une ligne de log pour afficher les détails.

Les détails s'affichent sous la ligne concernée :

Ces informations détaillées permettent notamment de relever l'adresse IP du poste de travail ayant généré l'entrée et le niveau de gravité.

Pour faciliter leur lecture, les informations présentées dans la liste **Agent Logs** sont figées à l'instant où la page **Traces d'audit** a été ouverte. Si vous souhaitez actualiser les informations affichées, il suffit de cliquer sur le bouton **RAFRAÎCHIR** situé en haut à droite dans le bandeau de titre de la page.



Des tableaux de bord personnalisés peuvent être élaborés avec l'aide de TheGreenBow. N'hésitez pas à contacter notre service commercial pour plus de précisions au sujet de nos prestations supplémentaires.

7.3 Qu'est-ce que l'agrégation de logs ?

L'agrégation des logs désigne le mécanisme de collecte, de normalisation et de consolidation de logs provenant de différents postes de travail équipés du Secure Connection Agent (SCA) au sein du parc de l'organisation.

7.4 Quelles informations peut-on surveiller ?

Parmi les informations de la liste **Agent Logs**, les éléments suivants peuvent être particulièrement intéressants à surveiller :

- heure d'établissement d'un tunnel ;
- tentatives infructueuses d'ouverture d'un tunnel ;
- adresse IP d'un poste de travail remontant des incidents graves ;
- santé du poste ;
- utilisation du tunnel de remédiation.

8 Maintenance

8.1 Introduction

Ce chapitre décrit les opérations de maintenance du CMC. Il s'agit ici essentiellement de la sauvegarde des bases de données des configurations VPN et des licences.

8.2 Mise à jour du système

⚠ Les administrateurs du CMC ne doivent pas gérer eux-mêmes les mises à jour métier ou des paquets, qu'il s'agisse du système d'exploitation ou de la pile de services HashiStack au cœur du produit.

Le CMC est constitué d'un ensemble de logiciels qui correspond à une version précise du système d'exploitation sous-jacent installé sur la Machine CMC. En cas d'évolution du produit, du système d'exploitation ou de la pile HashiStack, ou en cas de détection d'une CVE, la mise à jour doit obligatoirement se faire à l'aide de l'installeur sur la machine pilote et avec l'assistance du support technique TheGreenBow.

☞ Pour savoir comment contacter le support technique, reportez-vous à la section 9.3 Support.

8.3 Instancier un conteneur de l'installeur

Avant de pouvoir lancer les commandes de sauvegarde, d'export, de restauration et de redémarrage décrites ci-dessous, vous devez disposer de l'archive du dossier `instance_cmc` réalisée en fin d'installation (reportez-vous au « Guide d'installation » du CMC).

8.4 Sauvegarde

8.4.1 Sauvegardes quotidiennes automatiques

Les sauvegardes sont effectuées de manière automatique toutes les nuits.

8.4.2 Effectuer une sauvegarde des bases de données

Pour créer une sauvegarde de la base de données des configurations VPN (Postgres) et des licences (MariaDB), procédez comme suit :

1. Lancez la commande suivante pour instancier un conteneur Docker :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest bash
```

2. Naviguez vers le dossier `inventories`, puis exécutez la commande suivante pour lancer la tâche automatisée :

```
make launch_backup
```

La sauvegarde est d'abord stockée dans le volume Nomad, puis elle est archivée dans le nœud SRE.

8.4.3 Exporter une sauvegarde vers un répertoire local

Les fichiers de sauvegarde sont stockés dans le dossier `/opt/backup` du nœud SRE.

Pour créer une archive au format `.tar.gz` et la transférer vers le répertoire local actuel, procédez comme suit :

1. Lancez la commande suivante pour instancier un conteneur Docker :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest bash
```

2. Naviguez vers le dossier `inventories`, puis exécutez la commande suivante pour lancer la tâche automatisée :

```
make fetch_backup
```

Cette commande crée une archive au format `archive_backup_[date].tar.gz`.

3. Copiez cette archive vers votre répertoire local.
4. Supprimez l'archive de l'hôte distant.

Vous avez récupéré la sauvegarde en local et vous l'avez supprimé du CMC. Vous pouvez désormais l'archiver à l'emplacement de votre choix.

8.4.4 Sauvegarder et exporter en une seule étape

Vous pouvez également créer une sauvegarde et copier l'archive en local en une seule étape. Pour cela, procédez comme suit :

1. Lancez la commande suivante pour instancier un conteneur Docker :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest bash
```

2. Naviguez vers le dossier `inventories`, puis exécutez la commande suivante pour lancer la tâche automatisée :

```
make export_backup
```

La sauvegarde est effectuée et l'archive est copiée directement vers le répertoire local à partir duquel vous lancez la commande.

8.5 Restaurer les données d'une sauvegarde locale

8.5.1 Introduction

Dès lors que vous avez récupéré les fichiers de sauvegarde dans votre répertoire local, vous pouvez effectuer une restauration à partir de ces fichiers en exécutant des tâches automatisées.

8.5.2 Restaurer une sauvegarde de la base de données des configurations VPN

Pour restaurer une sauvegarde PostgreSQL, procédez comme suit :

1. Copiez le fichier de sauvegarde `postgres_configuration.sql` dans le répertoire local à partir duquel vous lancez la commande de restauration.
2. Exécutez la tâche automatisée suivante :

```
make restore_postgres
```

8.5.3 Restaurer une sauvegarde de la base de données des licences

Pour restaurer une sauvegarde MariaDB, procédez comme suit :

1. Copiez le fichier de sauvegarde `mariadb_tas.sql` dans le répertoire local à partir duquel vous lancez la commande de restauration.
2. Exécutez la tâche automatisée suivante :

```
make restore_mariadb
```

8.6 Exporter des logs du CMC vers le répertoire local

Les fichiers journaux (*logs*) sont stockés dans le répertoire `/var/log` sur le nœud SRE.

Les logs exportés sont les suivants :

Logs système :

- `/var/log/auth.log`
- `/var/log/kern.log`
- `/var/log/syslog`
- `/var/log/user.log`

Les logs du conteneur et quelques informations système :

- `/var/log/all_logs/`

Pour créer une archive au format `.tar.gz` et la transférer vers votre répertoire local actuel, procédez comme suit :

1. Lancez la commande suivante pour instancier un conteneur Docker :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest bash
```

2. Naviguez vers le dossier `inventories`, puis exécutez la commande suivante pour lancer la tâche automatisée :

```
make export_logs
```

Après avoir lancé la commande ci-dessus, vous trouverez une archive nommée `archive_logs_[date_du_jour].tar.gz` dans votre répertoire local.

8.7 Redémarrage

Le CMC est conçu pour fonctionner en continu sans interruption. Il n'est pas possible de simplement redémarrer la machine CMC en redémarrant le système d'exploitation, parce que l'outil de gestion des secrets Vault est scellé. Tous les services sous-jacents au CMC dépendent de Vault pour fonctionner.

Si pour des raisons de maintenance ou de migration du serveur vous êtes amenés à redémarrer le CMC, ou si le support technique vous le demande, procédez de la manière suivante :

1. Sur la machine pilote, lancez la commande suivante pour instancier un conteneur Docker :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest
```

2. Lorsque le menu s'affiche, entrez 3, puis appuyez sur la touche Entrée. Cette opération descelle Vault, redémarre le CMC et initialise tous les modules.

Lorsque le redémarrage est terminé, vous pouvez quitter la machine pilote et utiliser le CMC à partir de l'interface web.

9 Contact

9.1 Information

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

9.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

9.3 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