GUIDE

STORMSHIELD CLIENT VPN IPSEC

GUIDE D'INSTALLATION ET D'UTILISATION

Version 1.0

Dernière mise à jour du document : 11 mai 2026

Référence : sns-fr-client_vpn_ipsec_guide_installation_utilisation-v1

Table des matières

Historique des modifications ... 4

Introduction ... 5

Installation du client VPN ... 6

Prérequis techniques ... 6

Système d'exploitation ... 6

Droits et privilèges ... 6

Ressources matérielles ... 6

Infrastructure VPN côté serveur ... 6

Certificats et PKI ... 6

Réseau ... 7

Signature numérique et version ... 7

Procédure d'installation du client ... 7

Installation manuelle ... 7

Installation administrée ... 8

Mise à jour du client VPN ... 9

Mise à jour manuelle ... 9

Mise à jour administrée ... 9

Désinstallation du client VPN ... 10

Désinstallation manuelle ... 10

Désinstallation administrée ... 10

Configuration manuelle du tunnel ... 11

Configuration d'un tunnel standard ... 11

Étape 1 (Paramètres généraux) ... 12

Étape 2 (Paramètres IKE) ... 13

Étape 3 (Paramètres ESP) ... 19

Configuration d'un tunnel « Diffusion Restreinte » ... 22

Étape 1 (Paramètres généraux) ... 23

Étape 2 (Paramètres IKE) ... 24

Étape 3 (Paramètres ESP) ... 24

Finalisation de la création du tunnel ... 25

Configuration de tunnels multiples ... 25

Configuration administrée du tunnel ... 27

Exportation et importation de la configuration ... 27

Licence ... 29

Configuration manuelle de la licence ... 29

Configuration administrée de la licence ... 29

Utilisation du client VPN ... 30

Lancement manuel ... 30

Lancement automatique ... 31

Journaux d'événements ... 32

Logs d'audits ... 32

Logs techniques ... 33

Menu « Paramètres généraux » 34
Menu « A propos de » 35

Historique des modifications

Date	Description
11 mai 2026	Nouveau document

Introduction

Bienvenue dans le guide d'installation et d'utilisation Stormshield Client VPN IPsec version 1.0.

NOTE
Stormshield commercialise sous le nom Stormshield Client VPN IPsec le client Cybels VPN du partenaire éditeur Ercom. Le document d'origine a été rédigé par Ercom et publié sur le site de *Documentation Technique Stormshield* avec leur accord.

Ce guide est destiné aux administrateurs du Client VPN Cybels en charge du déploiement, de la configuration et de l'exploitation de la solution. Ce guide a pour objectif de fournir une vision complète et opérationnelle de Cybels VPN, afin de garantir un accès distant sécurisé, fiable et conforme aux exigences de l'organisation.

Le client VPN permet aux utilisateurs autorisés d'accéder aux ressources internes de l'entreprise depuis des environnements distants, tout en assurant la confidentialité des échanges, l'authentification des utilisateurs et l'intégrité des données. Son intégration s'inscrit dans la stratégie globale de sécurité du système d'information et doit être administrée selon les bonnes pratiques en vigueur.

Cette documentation couvre l'ensemble des aspects nécessaires à l'administration de la solution, notamment :

- Les prérequis techniques
- Les étapes d'installation et de configuration
- La gestion des profils
- Les mécanismes d'authentification et de chiffrement
- Les procédures de supervision, de maintenance et de dépannage.

Ce guide constitue une référence destinée à accompagner les administrateurs tout au long du cycle de vie du client VPN, depuis sa mise en œuvre jusqu'à son exploitation quotidienne, afin d'assurer un service sécurisé performant et maîtrisé.

Cybels VPN existe sous 2 variantes :

- **Cybels VPN Essential** : incluant les fonctionnalités de base
- **Cybels VPN Premium** : en plus des fonctionnalités de base, offre des fonctionnalités plus avancées de déploiement et de paramétrage des configurations possibles.

Le logiciel Cybels VPN est fourni sous forme de package .MSI ce qui permet de bénéficier d'un standard reconnu garantissant une installation fiable, reproductible et automatisable, une gestion centralisée du cycle de vie (installation, mise à jour, désinstallation) ainsi qu'une intégration native avec les outils de déploiement et d'administration des environnements Windows.

Installation du client VPN

Prérequis techniques

Système d'exploitation

- PC sous Microsoft Windows 11 (versions 22H2 ou ultérieures)
- Édition professionnelle ou Entreprise recommandée

Droits et privilèges

- Privilèges nécessaires à l'installation logicielle sur le poste de travail (lors d'une installation manuelle)

Ressources matérielles

- Espace disque disponible : 500 Mo
- Pour le reste, se référer aux exigences de Windows 11 https://www.microsoft.com/fr-fr/windows/windows-11-specifications?r=1

Infrastructure VPN côté serveur

Avant exploitation du client VPN, les éléments suivants doivent être disponibles :

- Un serveur VPN configuré avec un ou plusieurs tunnels en IKEv2, selon la politique réseau souhaitée.
- Paramètres nécessaires à l'établissement du ou des tunnels VPN, fournis par l'administrateur. Ces paramètres incluent entre autre:
  - L'adresse du serveur VPN (IP ou FQDN)
  - Éventuellement, le ou les algorithmes cryptographiques (chiffrement, intégrité, échanges de clés) à utiliser
  - Éventuellement, la configuration réseau si celle-ci n'est pas fournie dynamiquement

Certificats et PKI

- Certificat de la CA et utilisateur disponibles sur le PC
- Certificat utilisateur :
  - Format compatible X.509 v3 minimum (détails à venir)
  - Provisionné sur le support souhaité (magasin Windows, carte à puce à venir ultérieurement)
- Certificat CA :
  - Installé dans le magasin des intermédiaires
  - Format compatible X.509 v3 minimum (détails à venir ultérieurement)

Réseau

- Le port UDP dédié aux échanges VPN (par défaut 4500, ou tout autre port personnalisé) doit être explicitement autorisé en entrée et en sortie sur le pare-feu local.
- Absence de conflits avec d'autres clients VPN installés (désinstallation préalable recommandée)

Signature numérique et version

Le programme d'installation du Client Cybels VPN est signé numériquement à l'aide d'un certificat émis par **ERCOM ENGINEERING RESEAUX COMMUNICATIONS SAS**. Cette signature permet de garantir l'authenticité du logiciel et d'assurer que le fichier d'installation n'a pas été altéré. La vérification peut être effectuée par l'administrateur ou l'utilisateur en consultant les propriétés du fichier MSI (clic droit), puis en accédant à l'onglet « Signatures numériques».

Procédure d'installation du client

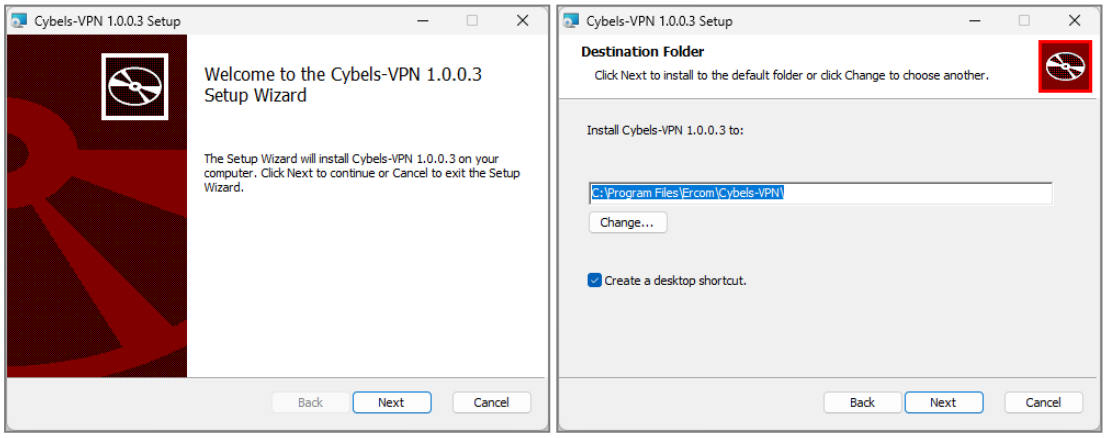
L'installation du client Cybels VPN s'effectue de plusieurs façons :

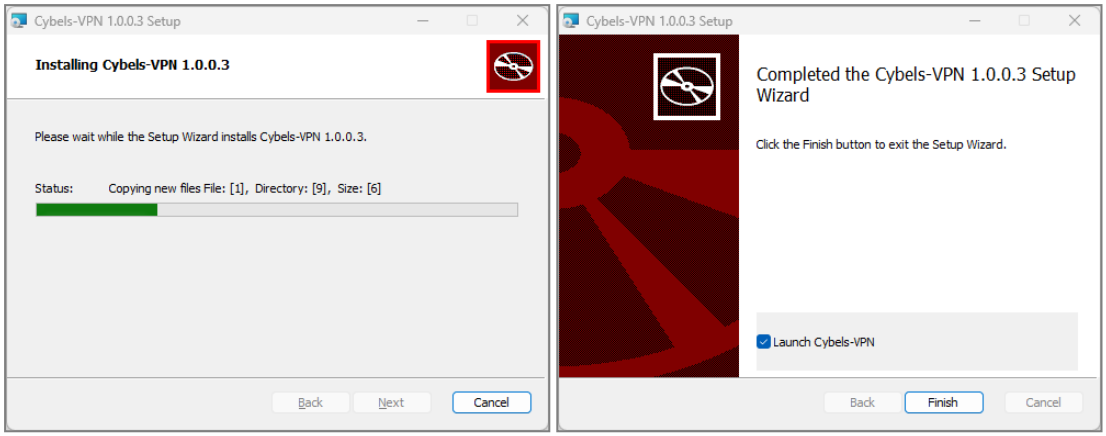
- **Mode d'installation manuelle** : s'adresse aussi bien à Cybels VPN Essential que Cybels VPN Premium et se déroule via l'interface graphique du client VPN
- **Mode d'installation administrée** : permet à l'administrateur de déployer automatiquement et de façon distribuée l'application sur un ensemble de PC. S'adresse à Cybels VPN Premium uniquement.

Installation manuelle

Via installateur du Client Cybels VPN (nécessite les droits d'administrateur local)

- Après téléchargement du package MSI, lancez l'application
- Laissez vous guider par l'assistant d'installation au fil des étapes





En cochant « Launch Cybels VPN », le client Cybels VPN démarre automatiquement une fois l'installation terminée.

Installation administrée

L'installation du Client Cybels VPN peut être installée plus confortablement dans le mode d'installation administrée, ce qui a pour effet de permettre une installation à distance, en masse et silencieuse.

- Avec stratégie de groupe (GPO)/EMM/MDM, voir avec votre administrateur système pour la configuration.
- En ligne de commande (CLI) via invite de commande Windows

NOTE
Si les capacités natives du MSI permettent un déploiement en masse pour toutes les variantes (Essential et Premium), les fonctionnalités de configuration centralisée (paramétrage automatique des profils et des politiques de sécurité à distance) sont réservées à la version Cybels VPN Premium.

Mise à jour du client VPN

La mise à jour du client Cybels VPN permet de passer à une version plus récente du logiciel tout en conservant les paramètres, la configuration VPN.

Comme pour une installation, la mise à jour nécessite les droits d'administrateurs locaux.

Il n'est pas nécessaire de désinstaller la version précédente avant de lancer l'opération de mise à jour.

Mise à jour manuelle

- Après téléchargement du package, lancez l'application
- Laissez vous guider par l'assistant d'installation au fil des étapes

Le client Cybels VPN démarre automatiquement une fois l'installation terminée.

Mise à jour administrée

- Avec une stratégie de groupe (GPO)/EMM/MDM, voir avec votre administrateur système pour la configuration.
- En ligne de commande (nécessite les droits d'administrateur local)
  - Après téléchargement du package MSI, ouvrez l'invite de commandes Windows
  - Allez dans le dossier contenant le package téléchargé
  - Exécutez la commande suivante pour débuter le déploiement :

```
msiexec /i "CybelsVPN_Setup.msi" /qn /norestart
```

Détail de la commande :

- /i : Installe ou met à jour le produit.
- /qn : Mode "Quiet No UI" (installation totalement silencieuse en arrière-plan).
- /norestart : Empêche un redémarrage automatique du système si celui-ci est requis (optionnel).

Le client Cybels VPN démarre automatiquement une fois la mise à jour installée.

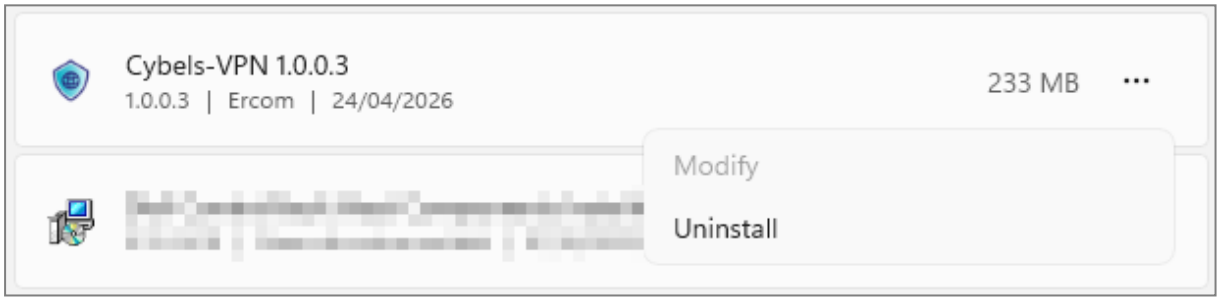
Désinstallation du client VPN

L'application peut être désinstallée du PC quelle que soit la variante Essential ou Premium initialement installée.
L'administrateur peut lancer cette désinstallation de plusieurs façons :

Désinstallation manuelle

Pour désinstaller le Client Cybels VPN (nécessite les droits d'administrateur local), suivez les étapes ci-dessous :

1. Ouvrez le **Panneau de configuration** Windows.
2. Sélectionnez **Désinstaller un programme**.
3. Sélectionnez Client Cybels VPN dans la liste de programmes.
4. Cliquez sur **Désinstaller** et suivez les instructions pour désinstaller le programme.



Désinstallation administrée

- Avec une **stratégie de groupe** (GPO), EMM/MDM, voir avec votre administrateur système pour la configuration.
- En ligne de commande (nécessite les droits d'administrateur local)

```
msiexec /x "CybelsVPN_Setup.msi" /qn
```

Une fois la désinstallation lancée, le dossier d'installation est supprimé, le service VPN n'est plus présent dans le gestionnaire des tâches, le raccourci Cybels VPN est supprimé et toutes les entrées relatives à l'application sont supprimées.

Par défaut, la désinstallation conserve les fichiers de configuration et les profils VPN de l'utilisateur. Cette mesure permet de restaurer immédiatement l'environnement de travail en cas de réinstallation ultérieure de l'application.

Configuration manuelle du tunnel

Cette partie couvre les paramètres essentiels pour paramétrer manuellement l'ensemble des options nécessaires à l'établissement d'un tunnel VPN, en supposant que l'installation se soit correctement déroulée et que les prérequis techniques soient respectés.

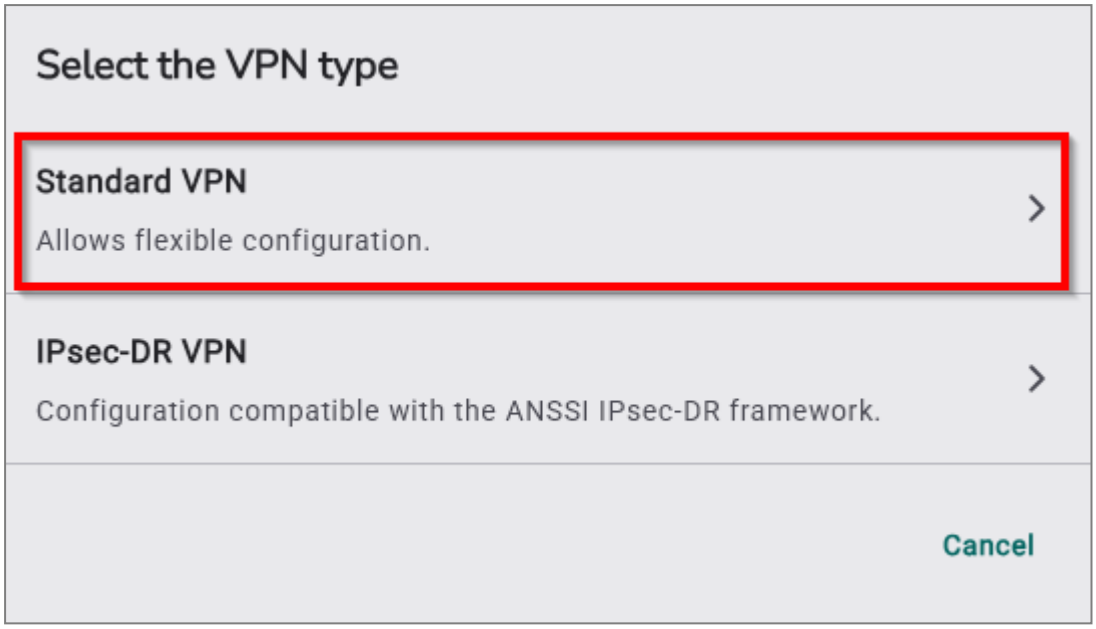
Configuration d'un tunnel standard

L'approche retenue pour le Tunnel Standard consiste à afficher l'intégralité des paramètres du tunnel IPsec, y compris ceux non modifiables. Cette visibilité permet à l'administrateur de valider précisément le comportement de l'application et de lever toute ambiguïté sur les paramètres appliqués.

Pour commencer la configuration d'un tunnel VPN, ouvrez l'application et cliquez sur le bouton « **Configurer votre premier VPN** ».

IMPORTANT
Il faut avoir au préalable importé le certificat utilisateur et le CA racine dans les emplacements de stockage Windows. L'application Cybels VPN ira chercher ces certificats respectivement dans le dossier Personnel (pour certificat utilisateur) et dans le dossier Autorités de certification racines de confiance (pour le CA racine) du magasin Windows de l'utilisateur actuel.

Puis sélectionnez le type de VPN souhaité, ici un VPN Standard.

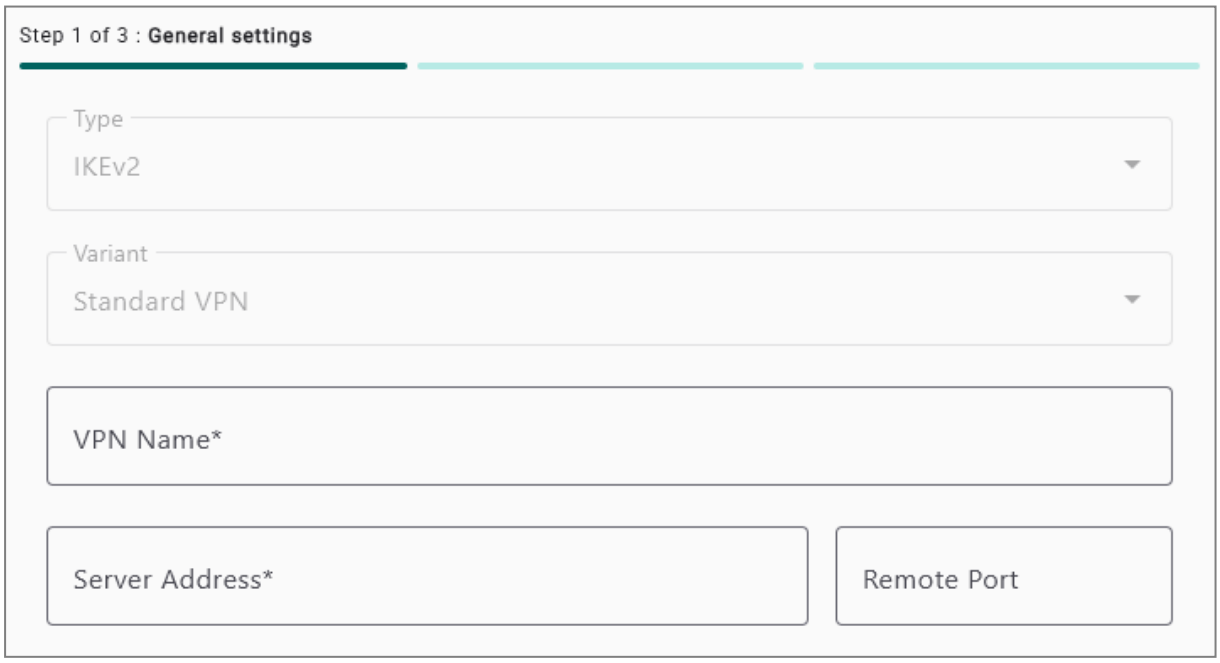


Étape 1 (Paramètres généraux)

Par la suite renseignez le nom du tunnel VPN que vous souhaitez créer, l'adresse du serveur et le port distant dans les champs « **Nom du VPN** », « **Adresse du serveur** » et « **Port distant** ». Si aucun port n'est paramétré alors la valeur par défaut 4500 s'applique.

L'adresse du serveur VPN est l'adresse IP ou le DNS public de la passerelle VPN à laquelle le client se connecte pour établir le tunnel IPsec. Il s'agit du point d'entrée du tunnel. Actuellement limité au protocole IPv4.

Le protocole de négociation et de gestion du tunnel IPsec est de type Internet Key Exchange version 2 (IKEv2) offrant un haut niveau de sécurité, de performance y compris en mobilité.

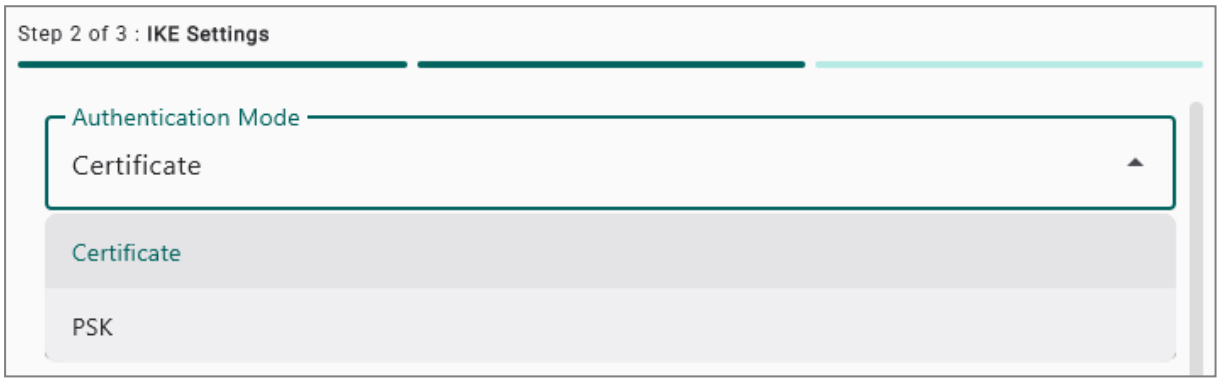


Une fois cette étape n°1 réalisée, cliquez sur le bouton « **Suivant** ».

Étape 2 (Paramètres IKE)

L'étape n°2 définit la méthode utilisée par le poste et la passerelle pour s'authentifier et prouver leur identité.

> **NOTE**
> La configuration choisie doit être strictement alignée avec les paramètres définis sur la passerelle VPN.



Parmi ces paramètres il y a le « **Mode d'authentification** » : **certificat** ou **PSK** (Pre-shared Key), respectivement basé sur certificat ou clé partagée.

Dans la configuration du tunnel VPN, les modes d'authentification déterminent comment les deux extrémités du tunnel prouvent leur identité avant d'établir la connexion sécurisée.
Les modes « certificate » et « PSK » correspondent aux deux méthodes d'authentification IKE les plus courantes.

Pour le mode « **Certificat** », chaque extrémité du tunnel (client et serveur) utilise un certificat numérique X.509, signé par une autorité de certification (CA) pour prouver son identité. Le certificat contient une clé publique, la clé privée associée reste secrète et la confiance est établie via la CA.

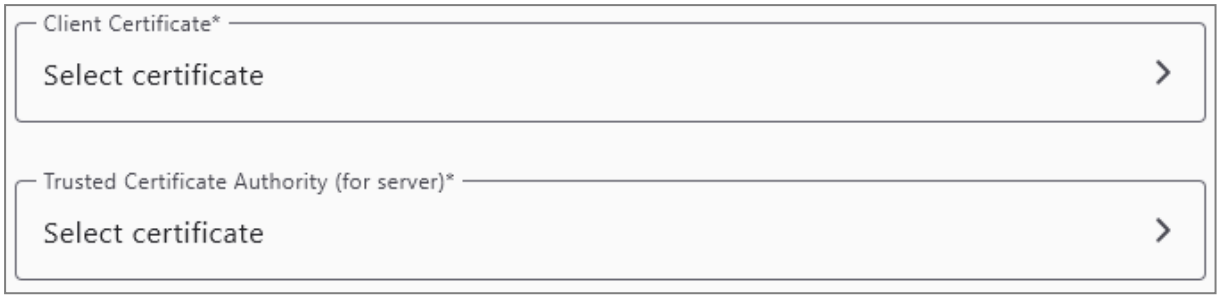
Pour le mode « **PSK** », les deux extrémités partagent un secret commun (mot de passe), configuré manuellement et identique de chaque côté. Le client et le serveur prouvent qu'ils connaissent la même clé, si la clé répond alors le tunnel est établi.

Mode d'authentification « certificat »

Prérequis : Avant de sélectionner ce mode, assurez-vous que :

- Un certificat utilisateur valide est présent sur le poste (magasin Windows ou support matériel).
- Le certificat de la CA (Autorité de Certification) du serveur est installé dans le magasin de certificats Windows.

Si le mode d'authentification « certificat » est sélectionné : il faudra ensuite sélectionner le certificat client ainsi que l'autorité de certification de confiance (CA) côté serveur, parmi ceux détectés automatiquement par le client, et listés sous forme d'une liste déroulante en cliquant sur le symbole >.



Le **certificat client** est le certificat numérique X.509 installé sur le poste de l'utilisateur et est utilisé pour authentifier de manière forte le client VPN lors de l'établissement du tunnel sécurisé. Lorsque le client Cybels VPN utilise l'authentification par certificat, le client présente son certificat au serveur pendant la négociation IKE.

Ce certificat a préalablement été importé dans le support d'hébergement selon les exigences de sécurité, les capacités du poste client et de la politique de gestion des certificats.

Plusieurs options d'hébergement sont possibles :

- Le magasin de certificat utilisateur Windows avec protection logicielle de la clé privée
- Un support matériel sécurisé (clé USB cryptographique, carte à puce)

Les emplacements de stockage matériels sont uniquement disponibles dans la version Cybels VPN Premium.

NOTE
Afin de simplifier la sélection et de minimiser les risques d'erreurs, l'application filtre automatiquement les certificats. Ne sont pas listés :

- Les certificats expirés ou dont la date de validité est future.
- Les certificats utilisant une version X.509 inférieure à v3.
- Les certificats auto-signés (ces derniers ne sont pas autorisés en tant que certificats utilisateurs).

L'**autorité de certification de confiance (pour le serveur)** est l'autorité de certification (CA) dont le certificat est utilisé par le client VPN pour vérifier l'authenticité du certificat présenté par le serveur VPN. Le client n'accepte la connexion que si le certificat du serveur est signé par cette autorité et correspond à l'identité attendue.

NOTE
De la même manière, seules les autorités valides sont listées. Sont exclus :

- Les certificats CA expirés ou dont la date de validité est future.
- Les certificats CA de version X.509 inférieure à v3.
- Note : Contrairement aux certificats clients, les certificats CA auto-signés sont acceptés et listés.

De même, la CA aura été préalablement importée dans le support d'hébergement selon les exigences de sécurité, les capacités du poste client et de la politique de gestion des certificats.

Le champ suivant « **Vérification de la révocation du serveur** » concerne le mécanisme de sécurité permettant au client Cybels VPN de vérifier que le certificat du serveur VPN présenté lors de la connexion n'a pas été révoqué par la PKI qui l'a émis.

Cette vérification garantit que le client VPN ne fait pas confiance à un serveur dont le certificat a été explicitement déclaré non fiable par la CA.

L'administrateur active ou non le contrôle de validité du certificat serveur en cliquant sur les boutons « **Oui** » ou « **Non** ».

La vérification de la révocation s'effectue directement dans le flux VPN durant la négociation IKE, en s'appuyant sur le protocole OCSP « *in-band* », défini dans la RFC 4806.

Le bloc suivant concerne les identifications locale et distante. L'identification locale est l'identité que le client présente au serveur tandis que l'identification distante est l'identité que le client attend du serveur.

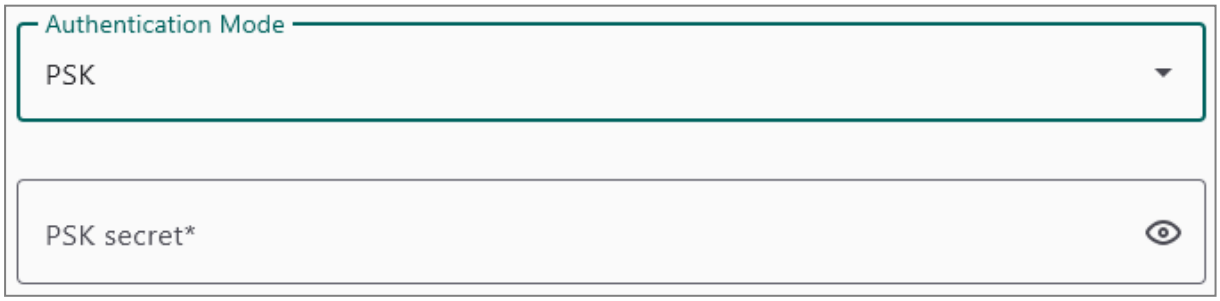
Ces identités sont utilisées lors de l'authentification et doivent être cohérentes avec les certificats ou les clés configurées.

L'administrateur a le choix grâce au menu déroulant entre plusieurs modes :

- **FQDN** (Fully Qualified Domain Name) : il s'agit d'un nom de domaine complet qui correspond généralement au CN ou DNS du certificat serveur (ex : vpn.entreprise.tld)
- **EMAIL** : il s'agit de l'identité au format adresse e-mail utilisée en tant qu'identifiant logique qui correspond souvent au SubjectAltName du certificat client
- **ASN.1 DN** : il s'agit de l'identité basée sur le Distinguished Name du certificat X.509 encodé en ASN.1 qui correspond exactement au Subject du certificat

Mode d'authentification « PSK »

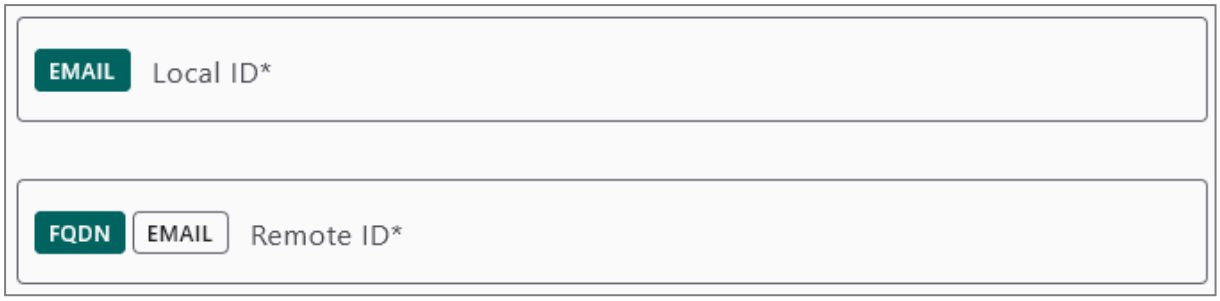
Si le mode d'authentification « **PSK** » est sélectionné il faudra ensuite renseigner la valeur de la clé pré-partagée dans le champ « **Secret PSK** »



Cette clé est utilisée lors de la négociation IKE pour s'authentifier et prouver que le client et le serveur sont légitimes.

L'administrateur peut afficher le mot de passe saisi en cliquant sur l'icône **œil**. Un second clic permet de le masquer à nouveau.

Ensuite il faut entrer les informations concernant **ID local** et **ID distant** basés sur **FQDN** ou **Email**

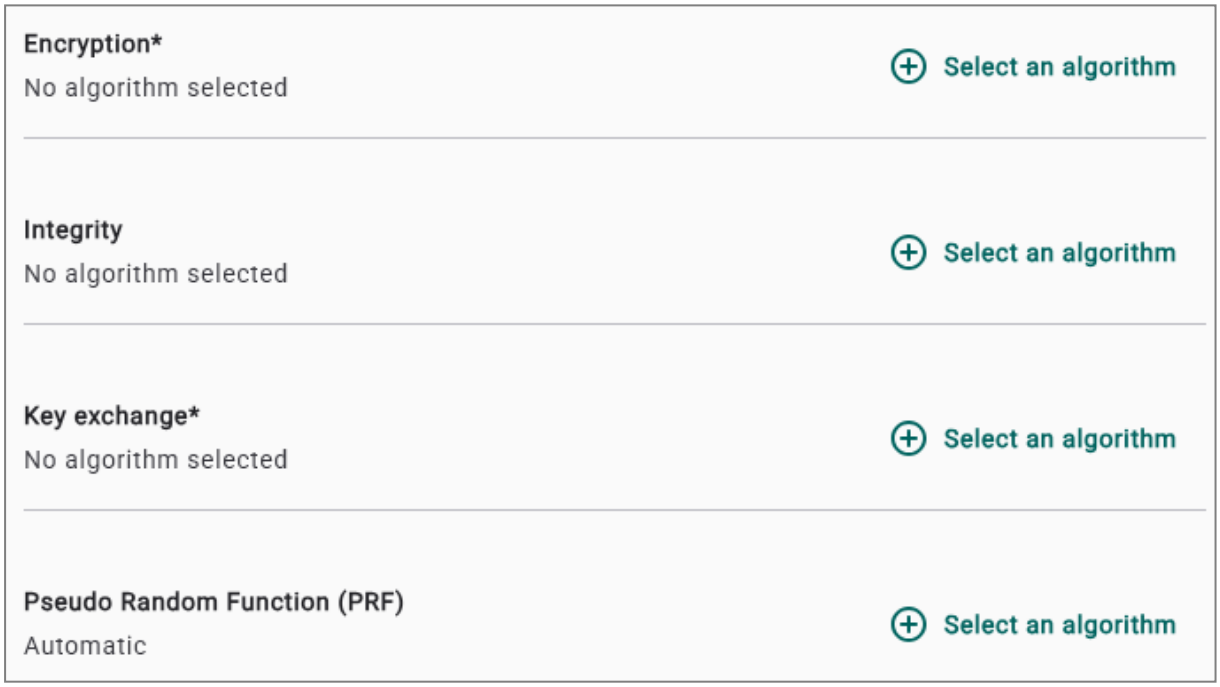


L'ID local et l'ID distant servent à identifier formellement chaque extrémité du VPN lors de la négociation IKE afin de permettre à chaque équipement (PC et serveur VPN) de savoir qu'il est en train d'établir le tunnel et vérifier qu'il s'agit du bon pair.

L'administrateur choisit le format des ID en sélectionnant « FQDN » ou « EMAIL ».

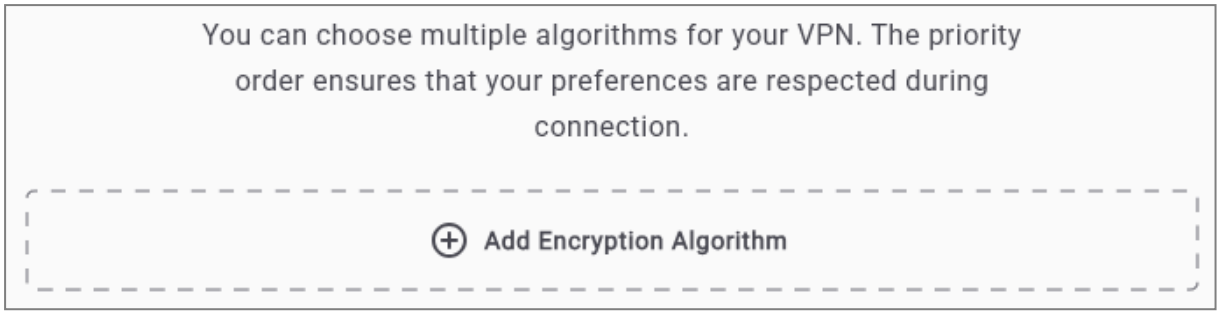
Cryptographie pour IKE (mode certificat ou PSK)

Dans la partie suivante, l'administrateur configure les aspects cryptographiques souhaités pour le tunnel VPN. Les algorithmes touchant au chiffrement, à l'intégrité, à l'échange de clé et à la fonction pseudo aléatoire sont à sélectionner parmi plusieurs propositions.



Pour ce faire, l'administrateur commence par cliquer sur « Sélectionner un algorithme » dans l'ordre présenté dans l'interface pour chaque bloc (chiffrement, intégrité, échange de clé et PRF).

Par exemple, en commençant par le bloc « **Chiffrement** », la fenêtre suivante s'affiche, permettant d'ajouter un ou plusieurs algorithmes de chiffrement en cliquant sur « **Add Encryption Algorithm** ».



Les algorithmes de chiffrement suivants sont disponibles :

- AES CBC 128, AES CBC 192, AES CBC 256, AES CTR 128, AES CTR 192, AES CTR 256, AES GCM-16 128, AES GCM-16 192, AES GCM-16 256

Les algorithmes d'intégrité suivants sont disponibles :

- SHA 256, SHA 384, SHA 512

Les algorithmes d'échange de clé suivants sont disponibles :

- Group 14 MODP 2048-bit, Group 15 MODP 3012-bit, Group 16 MODP 4096-bit, Group 17 MODP 6144-bit, Group 18 MODP 8192-bit, Group 19 ECP 256-bit, Group 20 ECP 384-bit, Group 21 ECP 521-bit, Group 28 ECP 256-bit, Group 29 ECP 384-bit, Group 30 ECP 512-bit

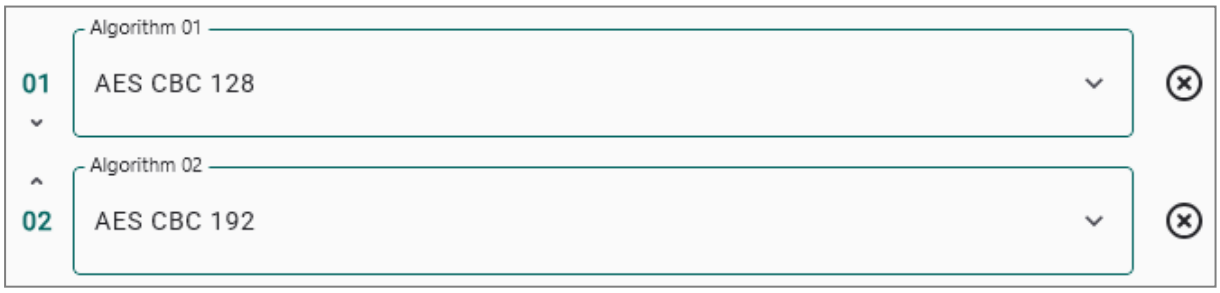
Les algorithmes de fonction pseudo aléatoire suivants sont disponibles :

- SHA 256, SHA 384, SHA 512

Les algorithmes de signature suivants sont disponibles :

- RSA PKCS#1 v1.5 SHA-2 256, RSA PKCS#1 v1.5 SHA-2 384, RSA PKCS#1 v1.5 SHA-2 512, ECDSA SHA-2 256, ECDSA SHA-2 384 DER, ECDSA SHA-2 512 DER, ECDSA 256 RAW

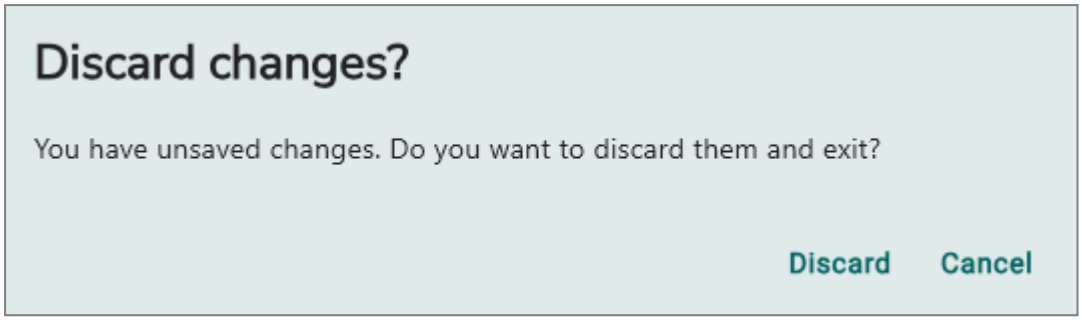
Il est possible de choisir plusieurs algorithmes parmi la liste ci-dessus et également de définir un ordre de priorité en jouant avec les flèches situées autour des numéros. Par exemple, ci-dessous AES CBC 128 sera prioritaire par rapport à AES CTR 192 car positionné en choix n°1.



Une fois les choix faits pour ce premier bloc relatif aux algorithmes de chiffrement, cliquez sur le bouton « Valider » pour enregistrer les choix.

Ensuite il convient de poursuivre la même démarche de sélection d'algorithmes avec les blocs « Intégrité », « Échange de clé » et « Fonction pseudo aléatoire (PRF) ». Dans le cas de PRF il y a une option de sélection automatique (par défaut) signifiant que tous les algorithmes sont supportés pour simplifier l'interopérabilité.

À tout moment il est possible de revenir en arrière voire de ne pas enregistrer la sélection en cours en cliquant sur « Abandonner ». Dans ce cas, un popup avertit l'administrateur.



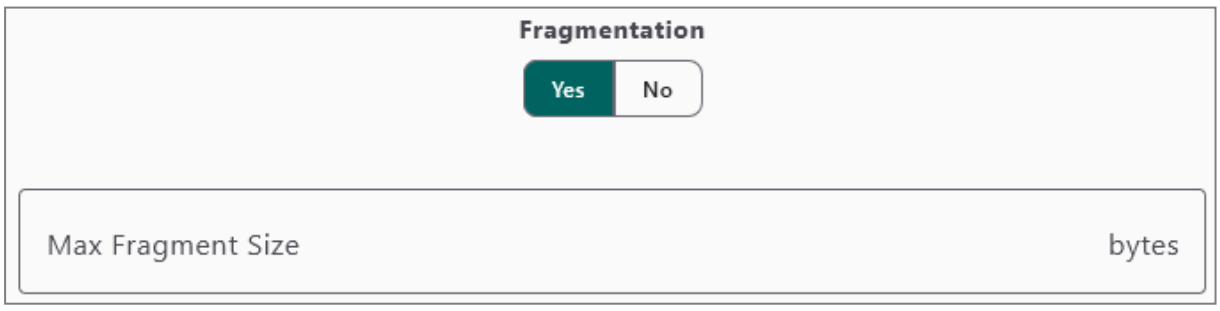
Le champ suivant concerne la durée de vie de l'association correspondant à la période de validité de l'association IKE avant son renouvellement obligatoire (IKE reauth).

A l'expiration de cette durée (exprimée en secondes), le client lance une **réauthentification complète** des deux extrémités (peers). Ce processus génère de nouvelles clés de chiffrement pour garantir la sécurité continue du tunnel.

Si aucune valeur n'est entrée, alors la durée de vie par défaut est appliquée. Elle est de 14440 secondes.

NOTE
Le processus de renouvellement peut entraîner une brève interruption de la connectivité (généralement de 2 à 3 secondes) le temps de valider la nouvelle session.

Vient ensuite le paramétrage de la fragmentation permettant de découper les messages volumineux pour faciliter leur passage sur certains réseaux restrictifs.



L'administrateur choisit grâce au bouton « Oui » ou « Non » l'activation de cette fragmentation.

- Désactivé (Non) : Le client ne propose pas la fragmentation.
- Activé (Oui) : Le client propose l'usage de la fragmentation à la passerelle.
- Taille des paquets : Définit le seuil de découpe en octets (Valeur par défaut : 1280 octets).

NOTE
L'activation côté client est une proposition. Pour que la fragmentation soit réellement effective, elle doit être simultanément activée et supportée sur le serveur VPN.

Enfin, le dernier menu est la sélection du « Mode childless ». Dans ce mode seule la connexion de contrôle VPN est établie, sans créer le tunnel de données. Il n'y a pas d'échange de trafic réseau chiffré.

Le fonctionnement est le suivant :

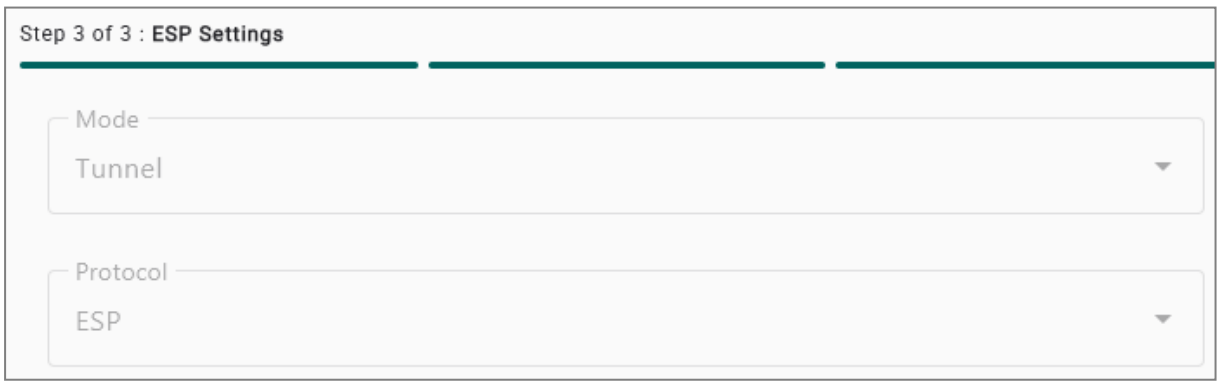
- Si activé (Oui) : L'application établit uniquement le canal de contrôle initial. Le tunnel de données (Child SA) n'est créé que lorsqu'un trafic réseau effectif est détecté. Cela permet de ne pas consommer de ressources sur la passerelle tant qu'aucune donnée ne circule.
- Si désactivé (Non) : Le tunnel de données est créé systématiquement et immédiatement après la réussite de l'authentification IKE, même en l'absence de trafic.

Étape 3 (Paramètres ESP)

L'étape n°3 permet de configurer la politique de protection des flux de données.

- Mode « Tunnel » (Imposé) : Contrairement au mode transport, le mode Tunnel encapsule l'intégralité du paquet IP d'origine (données + en-têtes). C'est le seul mode permettant de masquer l'architecture interne du réseau client vis-à-vis du réseau public.
- Protocole « ESP » (Imposé) : L'application s'appuie exclusivement sur l' Encapsulating Security Payload. C'est le protocole de référence assurant simultanément la confidentialité (chiffrement), l'intégrité et l'authentification des échanges.

NOTE
Ces deux champs sont affichés dans l'interface pour permettre à l'administrateur de confirmer la conformité du tunnel, mais ils sont verrouillés pour prévenir toute configuration affaiblie.



Choix des algorithmes

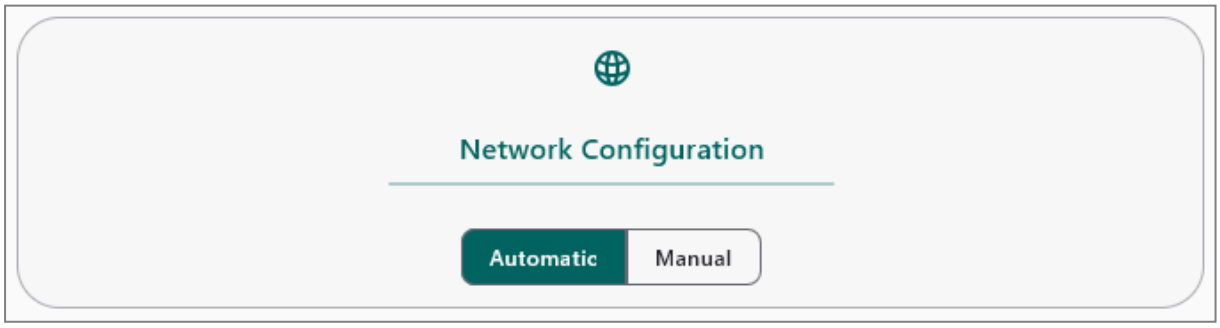
L'administrateur sélectionne ensuite les algorithmes correspondant au chiffrement, à l'intégrité et à l'échange de clé de façon similaire à ce qui a été paramétré à l'étape n°2 en cliquant sur « **Sélectionner un algorithme** » pour chacun des paramètres ci-dessous.

Durée de vie de l'association et configuration réseau

Puis définit si besoin la « **Durée de vie de l'association** » correspondant à la période pendant laquelle les clés ESP et ses paramètres de sécurité restent valides (rekey). La valeur est exprimée en secondes. Si aucune valeur n'est entrée, alors la durée de vie par défaut est appliquée. Elle est de 900 secondes.

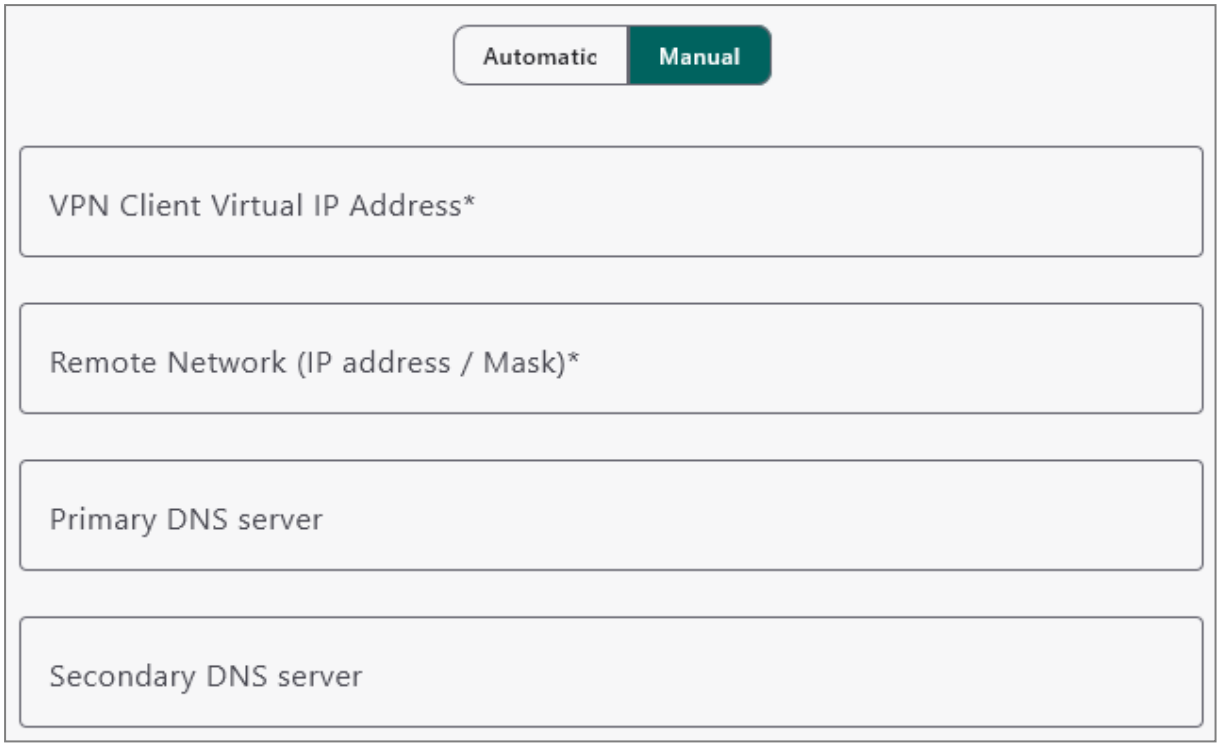
NOTE
Le processus de rekey est conçu pour être transparent et ne provoque généralement aucune coupure de flux, contrairement à la réauthentification IKE qui peut entraîner une brève interruption.

L'administrateur définit le mode de Configuration Réseau « **Automatique** » ou « **Manuel** ». Ce paramétrage implique la définition des caractéristiques du trafic réseau à protéger, c'est-à-dire le trafic qui doit passer par le tunnel IPsec.



En mode automatique (également appelé 'Configuration Payloads' dans IKEv2), les paramètres réseau sont automatiquement fournis par le serveur distant IPsec.

En mode manuel l'administrateur configure l'ensemble des champs suivants **Adresse IP** », « **Réseau distant** », « **Serveur DNS principal** » et « **Serveur DNS secondaire** »



- L'adresse IP est utilisée pour le routage du trafic et peut également être utilisée pour l'identification unique du client sur le réseau.
- Le réseau distant correspond au réseau qui se trouve de l'autre côté du tunnel VPN auquel le client doit accéder. Le format attendu est exprimé en notation CIDR adresse *IP/masque*.
- Le serveur DNS principal est le serveur de résolution de noms de domaines prioritaire et doit être accessible depuis le réseau ou le VPN
- Le serveur DNS secondaire prendra le relais en cas d'erreur ou mauvaise configuration du principal.

Extended Sequence Number (ESN)

En dernier lieu, l'administrateur active ou non l'ESN. Ce paramètre permet d'utiliser des numéros de séquence plus longs (64 bits au lieu de 32 bits) pour les paquets IPsec.

Sans l'ESN (sélectionner « **Non** ») le compteur est sur **32 bits** et peut déborder rapidement sur des liens très rapides ou des tunnels très actifs.

Avec l'ESN (sélectionner « **Oui** ») le compteur passe à **64 bits**, le risque de débordement est quasi nul et le tunnel est davantage robuste pour le long terme.

Pour finir cette étape 3, cliquez sur le bouton « **Créer le tunnel** »

Les algorithmes de signature implémentés sont RSA PKCS#1 v1.5 SHA-2 256, RSA PKCS#1 v1.5 SHA-2 384, RSA PKCS#1 v1.5 SHA-2 512, ECDSA SHA-2 256, ECDSA SHA-2 384 DER, ECDSA SHA-2 512 DER, ECDSA 256 RAW

NOTE
Il n'y a pas de sélection possible en terme d'algorithmes pour la signature. C'est le contenu du certificat qui définit l'algorithme de signature utilisé.

Configuration d'un tunnel « Diffusion Restreinte »

Le client Cybels VPN (dans sa version Premium) permet la configuration automatique de tunnels VPN respectant le référentiel IPsec Diffusion Restreinte (DR) tel que défini par l'ANSSI.

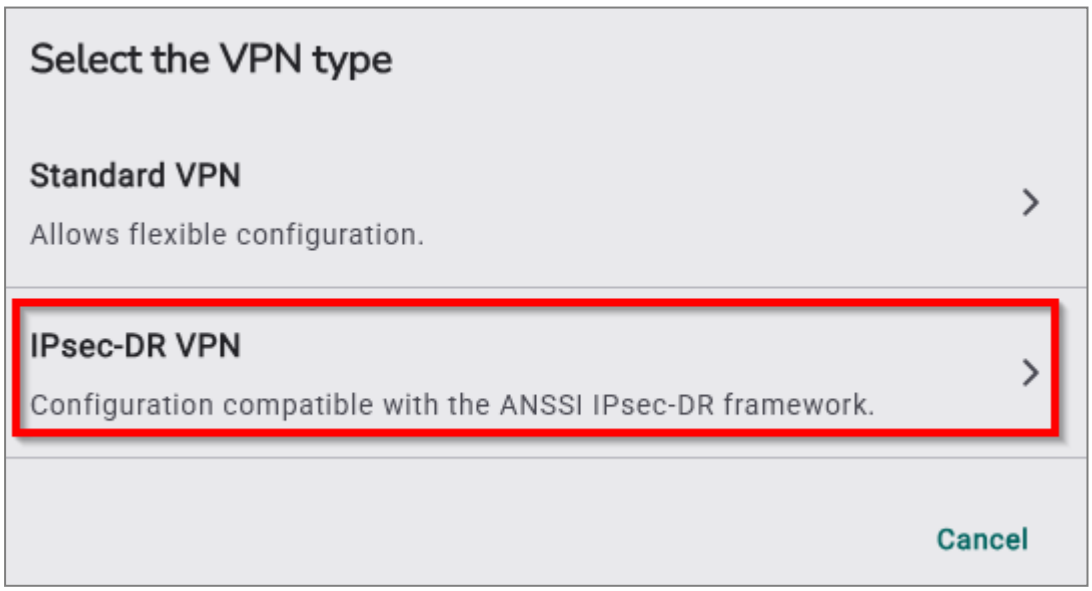
Le profil IPsec DR vise à garantir un niveau de sécurité élevé et homogène pour les VPN IPsec utilisés dans :

- Les administrations,
- Les opérateurs d'importance vitale (OIV),
- Les systèmes manipulant des données sensibles mais non classifiées secret-défense.

Dans ce mode, l'administrateur est dispensé de la sélection manuelle de l'ensemble des paramètres imposés par le profil IPsec DR (suites cryptographiques, mode Childless, etc.). L'application applique nativement ces réglages dès l'initialisation, garantissant une configuration conforme au référentiel de l'ANSSI tout en limitant drastiquement les risques d'erreurs humaines.

IMPORTANT
Pour que la connexion aboutisse, la passerelle VPN (pare-feu ou concentrateur) doit elle aussi être configurée en mode conforme IPsec DR. Tous les équipements de l'architecture doivent respecter ces exigences de l'ANSSI.

Pour initier la configuration d'un tunnel VPN IPsec DR, cliquez sur « **Ajouter un VPN** » puis sélectionnez « **VPN IPsec DR** »



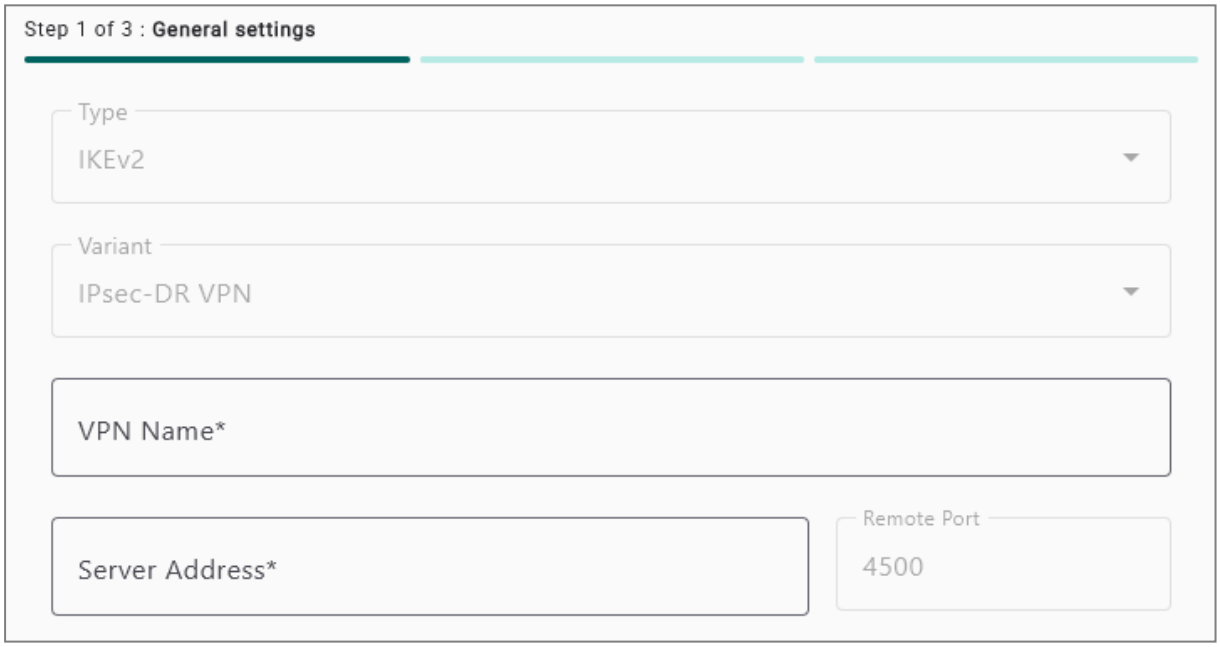
Étape 1 (Paramètres généraux)

Par la suite renseignez le nom du tunnel VPN que vous souhaitez créer ainsi que l'adresse du serveur dans les champs « **Nom du VPN** » et « **Adresse du serveur** » (IP ou FQDN de la passerelle VPN).

NOTE
Le support est actuellement limité au protocole IPv4

Le port par défaut est **4500 (NAT-T)** lorsque ce mode est sélectionné.

NOTE
Conformément au profil de sécurité imposé, ce port est non modifiable afin de garantir l'utilisation du standard de traversée de NAT requis par le référentiel.



Paramètres cryptographiques

Les suites cryptographiques sont pré-configurées selon les exigences du mode IPsec DR. Par souci de clarté, ces paramètres sont masqués dans l'interface.

À titre informatif, l'application propose les combinaisons suivantes lors de la négociation :

	Chiffrement	Intégrité	Échange de clés	PRF
Suite 1	AES GCM-16 256	Aucune*	Groupe 19 (ECP 256 bits)	SHA 256
Suite 2	AES GCM-16 256	Aucune*	Groupe 28 (Brainpool ECP 256 bits)	SHA 256
Suite 3	AES CTR 256	SHA 2 256	Groupe 19 (ECP 256 bits)	SHA 256
Suite 4	AES CTR 256	SHA 2 256	Groupe 28 (Brainpool ECP 256 bits)	SHA 256

(*) L'intégrité est nativement assurée par le mode de chiffrement GCM.

Étape 2 (Paramètres IKE)

Par défaut, le mode d'authentification dans la variante IPsec DR est de type « **Certificat** ». Le mode PSK (clé partagée) est désactivé et ne peut pas être sélectionné pour un tunnel IPsec DR.

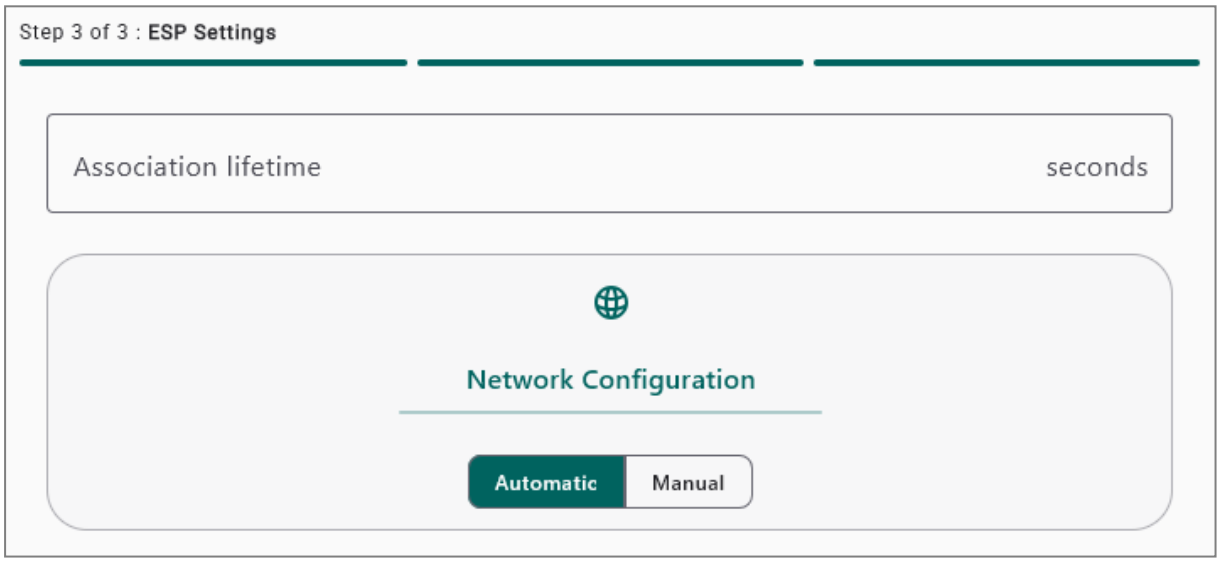
Pour la configuration de cette étape, voir Mode d'authentification « certificat »

Par défaut le mode Childless est activé et imposé conformément au référentiel IPsec DR.

Étape 3 (Paramètres ESP)

L'étape n°3 consiste à renseigner les paramètres ESP (Encapsulating Security Payload) servant à protéger les données qui transitent dans le VPN.

L'administrateur choisit la durée de vie de l'association et la configuration réseau « automatique » ou « manuel ».



Voir Durée de vie de l'association et configuration réseau

Paramètres cryptographiques

Les suites cryptographiques sont pré-configurées selon les exigences du mode IPsec DR. Par souci de clarté, ces paramètres sont masqués dans l'interface.

À titre informatif, l'application propose les combinaisons suivantes lors de la négociation :

	Chiffrement	Intégrité	Échange de clés
Suite 1	AES GCM-16 256	Aucune*	Groupe 19 (ECP 256 bits)
Suite 2	AES GCM-16 256	Aucune*	Groupe 28 (Brainpool ECP 256 bits)
Suite 3	AES CTR 256	SHA 2 256	Groupe 19 (ECP 256 bits)
Suite 4	AES CTR 256	SHA 2 256	Groupe 28 (Brainpool ECP 256 bits)

(*) L'intégrité est nativement assurée par le mode de chiffrement GCM.

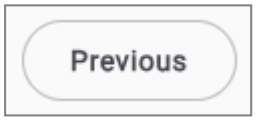
L'algorithme de signature implémenté est : ECDSA 256 RAW

Pour finir cette étape 3, cliquez sur le bouton « **Créer le tunnel** »

Finalisation de la création du tunnel

Le client VPN affiche un récapitulatif de l'ensemble des paramètres définis lors des étapes 1, 2 et 3, permettant à l'administrateur d'apporter des modifications si besoin en cliquant sur le bouton « **Retour à la configuration** » ou bien en acquittant la configuration en cliquant sur « **Enregistrer la configuration** »

En cliquant sur le bouton « Retour à la configuration », l'administrateur est redirigé vers l'étape 3 et peut naviguer entre les différentes étapes grâce au bouton « Précédent »



En cliquant sur le bouton « Enregistrer la configuration », le tunnel est créé. Un message toast indique que ce dernier a été créé avec succès.

Et l'ensemble des paramètres sont regroupés dans les onglets « **Général** », « **IKE** » et « **Child SA** » pour consultation.

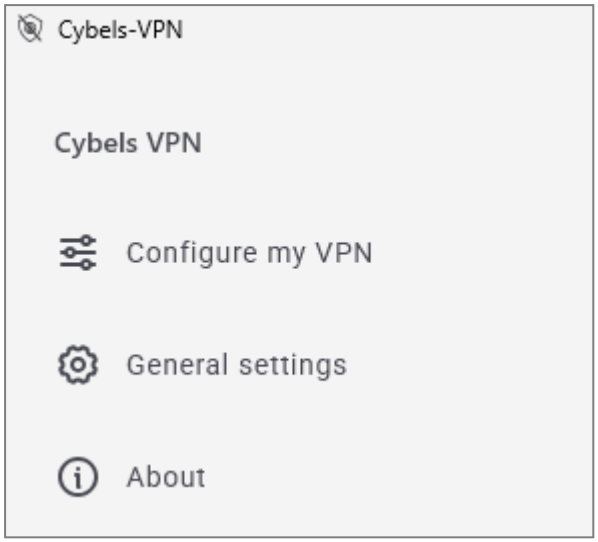
Actions supplémentaires

L'administrateur dispose de 2 boutons supplémentaires sur cette page récapitulative pour « **Éditer** » ou « **Supprimer** » le tunnel créé.

Configuration de tunnels multiples

Il est possible de configurer plusieurs tunnels VPN. Pour ce faire, il suffit d'appliquer les mêmes étapes décrites pour la création d'un tunnel.

L'ensemble des tunnels configurés se trouve dans le menu latéral « **Configurer mes VPN** » de l'application.



Ainsi, il est possible en cliquant sur ce menu de visualiser, obtenir des informations, éditer et supprimer les tunnels.
Dans l'exemple ci-dessous, 2 tunnels ont été configurés : test et Cybels VPN Client

Sur la page d'accueil de l'application, l'ensemble des VPN configurés sont affichés.
Dans l'exemple ci-dessous, 2 VPN sont disponibles :

Dès lors qu'une pastille verte est visible à côté du VPN, cela signifie que le tunnel de ce VPN est actif.

Le chapitre suivant décrit l'activation d'un tunnel VPN.

NOTE
Même s'il est possible de configurer plusieurs tunnels, seul un tunnel peut être actif à la fois.

Configuration administrée du tunnel

Cette partie couvre les paramètres essentiels pour paramétrer de façon administrée l'ensemble des options nécessaires à l'établissement d'un tunnel VPN, en supposant que l'installation se soit correctement déroulée et que les prérequis techniques soient respectés.

IMPORTANT
Il faut avoir au préalable importé le certificat utilisateur et le CA racine dans les emplacements de stockage Windows. L'application Cybels VPN ira chercher ces certificats respectivement dans le dossier Personnel (pour certificat utilisateur) et dans le dossier Autorités de certification racines de confiance (pour le CA racine) du magasin Windows de l'utilisateur actuel.

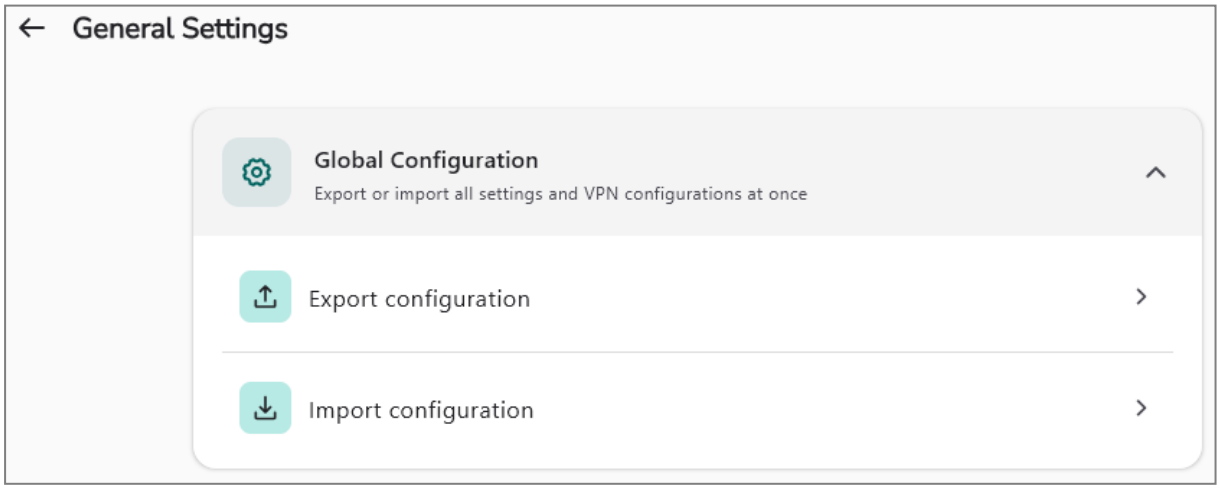
La notion administrée signifie que l'administrateur :

1. Définit, exécute les étapes de configuration manuelle (voir Configuration manuelle du tunnel) sur un poste PC et finalise la création de la configuration.
2. Procède à l'exportation de cette configuration (voir Exportation et importation de la configuration)
3. Déploie cette configuration sur plusieurs postes utilisateurs de façon manuelle via l'application Cybels VPN (import de configuration) ou bien avec les outils d'administration de type EMM/GPO.

Cette fonctionnalité de configuration est utile pour faire une sauvegarde de configuration avant d'éventuels modifications ou tests mais aussi pour construire une configuration « témoin » et la répliquer sur plusieurs postes, ce qui a pour avantage un gain de temps par rapport à une configuration manuelle sur plusieurs postes unitairement.

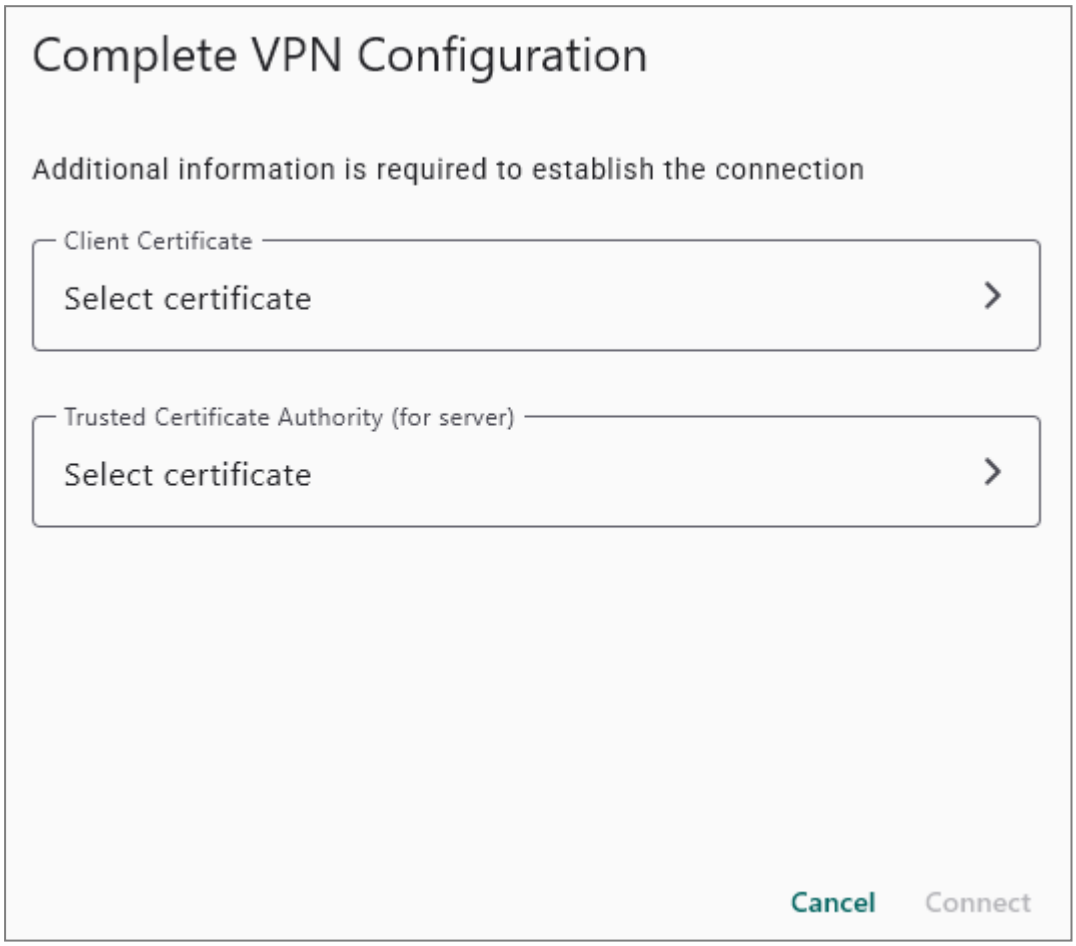
Exportation et importation de la configuration

Via l'interface du client VPN, l'administrateur se rend dans les paramètres généraux de l'application Cybels VPN et sélectionne « **Exporter la configuration** ». L'application génère un fichier conformément à la configuration créée manuellement.



Après export, il est également possible d'éditer puis d'importer cette configuration en cliquant sur « **Importer une configuration** » sur un ou plusieurs postes PC.

NOTE
Après l'import d'une configuration, les paramètres personnels (PSK ou certificat utilisateur) doivent être complétés afin de finaliser la configuration et ensuite pouvoir effectuer le lancement du tunnel VPN.



Pour faciliter les déploiements en masse et à distance, cette configuration peut également être déployée via des outils d'administration type EMM/GPO. Ce paramétrage est disponible dans la version *Cybels VPN Premium*.

- Il conviendra de déposer ce fichier de configuration dans le répertoire suivant **C:\ProgramData\Ercom\Cybels-VPN**
- Ce fichier devra respecter la nomenclature suivante **vpn_config.json**

Licence

Pour activer la solution Cybels VPN, l'administrateur doit renseigner une clé de licence valide, que ce soit dans le cas de configuration du client Cybels VPN Essential ou bien Cybels VPN Premium.

Configuration manuelle de la licence

Depuis l'interface du client Cybels VPN, ouvrez le menu « Paramètres généraux » et accédez au champ concernant la Licence afin de saisir la clé fournie par votre distributeur.

Configuration administrée de la licence

Après export de la configuration, ouvrez ce fichier avec un éditeur de texte, puis saisissez la clé fournie par votre distributeur en respectant strictement le format attendu.

Après avoir enregistré les modifications, importez cette nouvelle configuration puis déployez la sur le ou les postes PC souhaités avec l'outil d'administration de votre choix EMM ou GPO.

Utilisation du client VPN

Lancement manuel

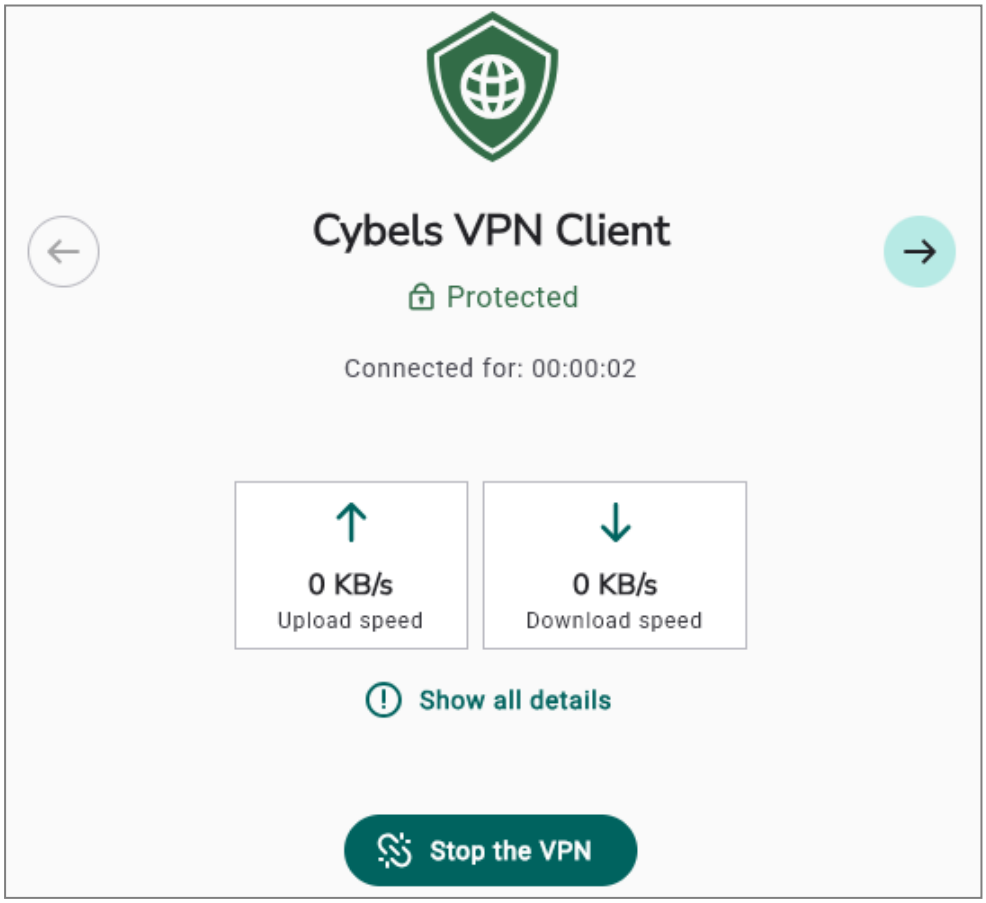
Le lancement manuel de Cybels VPN consiste à initier volontairement une connexion sécurisée entre le poste de l'utilisateur et le réseau distant via le tunnel chiffré.

La connexion reste active jusqu'à une déconnexion manuelle ou en cas de perte réseau / expiration.

Cliquez sur le bouton dédié « **Démarrer le VPN** » pour démarrer la session VPN. Veillez à ce que le PC soit bien connecté à Internet.

L'application indique un démarrage effectif du VPN en affichant plusieurs indicateurs tels que :

- Le statut « **Protégé** » précédé du symbole cadenas
- Le logo de l'application en vert
- La durée depuis laquelle le tunnel est monté via le champ « **Connecté depuis** : … »
- Le nom du tunnel, dans l'exemple ci-dessous « **Cybels VPN Client** »
- Les débits ascendants et descendants exprimés en Ko/s
- Des détails supplémentaires dans « **Afficher tous les détails** », afin de visualiser l'ensemble des paramètres négociés à l'établissement du tunnel, sur base de la configuration effectuée par l'administrateur.



Et cliquez sur « **Arrêter le VPN** » pour rompre le tunnel.

La connexion reste établie jusqu'à une action de déconnexion volontaire, une perte prolongée du signal réseau ou l'expiration de la session.

Lancement automatique

A venir ultérieurement dans Cybels VPN Premium

Journaux d'événements

Le client Cybels VPN intègre un mécanisme de journalisation permettant d'enregistrer les événements liés au fonctionnement de l'application dans son contexte d'exécution local.

Ces fichiers de logs contiennent notamment des informations telles que le démarrage et l'arrêt de l'application, les paramètres de configuration, les ouvertures et fermeture du tunnel ainsi que les messages d'erreurs, avertissements et informations.

Ces logs sont collectés et consultables en local depuis le poste de l'utilisateur via le gestionnaire d'événements Windows (aussi appelé Observateur d'événements) accessible via le menu **Démarrer / Observateur d'événements** ou en lançant la commande eventvwr.msc

Également en mode administré via EMM/GPO avec serveur distant AD pour la version Cybels VPN Premium.

Trois familles de logs sont disponibles : les logs d'audit, les logs techniques et les logs fonctionnels

Logs d'audits

Ci-dessous la liste des différents logs d'audit :

Type d'audit	Identifiant	Criticité	Qu'indique cet audit ?	Paramètres	Exemple	Remarques
App.Start	101	Info	Démarrage de l'application	La version logicielle (softwareVersion), Mode administré ou non (Managed)	App.Start softwareVersion: 0.5.99.16 Managed: no	
App.Stop	102	Info	Arrêt de l'application		App.Stop	Cet audit peut ne pas être enregistré en cas d'arrêt inattendu de l'application
Tunnel.Start	201	Info	Lancement d'un tunnel	Nom du tunnel (tunnelName)	Tunnel.Start tunnelName: Official_Ercom	Cet audit indique qu'un tunnel a été lancé, mais n'indique pas si la connexion a réussi ou a échoué
Tunnel.Stop	202	Info	Arrêt d'un tunnel	Nom du tunnel (tunnelName)	Tunnel.Stop tunnelName: Official_Ercom	
Config.CreateTunnel	301	Info	Création d'un tunnel	Nom du tunnel (tunnelName), Mode du tunnel (DR ou pas DR)	Config.CreateTunnel tunnelName: valid_standard_cert isDr: no	

Type d'audit	Identifiant	Criticité	Qu'indique cet audit ?	Paramètres	Exemple	Remarques
Config.ModifyTunnel	302	Info	Modification d'un tunnel	Nom du tunnel (tunnelName)	Config.ModifyTunnel tunnelName: valid_standard_cert	
Config.DeleteTunnel	303	Info	Suppression d'un tunnel	Nom du tunnel (tunnelName)	Config.DeleteTunnel tunnelName: valid_standard_cert	
Config.TunnelChange	304	Info	Nouvelle configuration pour un tunnel	Nom du tunnel (tunnelName), les paramètres impactés sous format clé valeur	Config.TunnelChange tunnelName: valid_standard_cert fieldName: IkeKeyExchange fieldValue: Group 14	Voir note ci-dessous
Config.ExportConfig	305	Info	Export d'une configuration		Config.ExportConfig	
Config.ImportConfig	306	Info	Import d'une configuration		Config.ImportConfig	

NOTES

- Config.TunnelChange s'affiche lors de l'ajout d'un tunnel mais aussi lors de la modification d'un tunnel
- Dans le cas de l'ajout, les paramètres du nouveau tunnel sont affichés => un événement pour chaque paramètre
- Dans le cas de modification, seuls les paramètres modifiés sont affichés (la nouvelle valeur) => un événement pour chaque paramètre modifié
- Certains paramètres ne sont pas affichables: PSK (pour raison de sécurité), les certificats (pour raisons techniques)

Logs techniques

A venir ultérieurement

Menu « Paramètres généraux »

Ce menu regroupe les options globales qui s'appliquent à l'ensemble des connexions VPN et des tunnels paramétrés.

Notamment les paramètres de configuration globale pour exporter et importer une configuration, les paramètres liés à la PKI ainsi qu'à la configuration et statut de la licence à activer (ou déjà activée) sur le poste de l'utilisateur. Cette licence permet de savoir quel type de produit Essential ou Premium a été configuré sur le poste et sa période de validité.

Menu « A propos de »

Ce menu affiche les informations relatives à la version du logiciel (SDK, client multiplateforme, build) et les licences tierces utilisées.

Informations de version standard

L'écran principal affiche les informations d'identité du produit :

- Version du client : Version majeure de l'application (ex: 0.4.0)
- Copyright : Mentions légales et propriété intellectuelle (Ercom)
- Licences tierces : Un lien dédié permet de consulter la liste des composants open-source intégrés à la solution, garantissant la transparence logicielle

Informations détaillées (Expert / Debug)

En cliquant sur le bouton « Plus d'informations sur la version », un volet latéral s'ouvre pour afficher des données techniques approfondies :

- SDK : Version du kit de développement utilisé
- StrongSwan : Version du moteur de cryptographie IPsec pilotant les tunnels
- Numéro de build : Identifiant unique de la compilation du logiciel (ex: 20260130...)
- Version du serveur de licence d'activation du client VPN

NOTE
Ces informations détaillées sont destinées à un usage de diagnostic avancé. Elles ne sont généralement pas nécessaires au quotidien, mais doivent être transmises sur demande des équipes de Support Technique en cas d'ouverture d'un ticket d'incident. Elles permettent une analyse précise du comportement du client selon son environnement de compilation.

STORMSHIELD

documentation@stormshield.eu