Déployer une solution VPN rapide pour Mac OS sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Il n'existe pas de version Quick VPN adaptée à Mac OS. Cependant, de plus en plus d'utilisateurs souhaitent déployer une alternative Quick VPN pour Mac OS. Dans cet article, IP Securitas est utilisé comme une alternative pour un VPN rapide.

Remarque : vous devez télécharger et installer IP Securitas sur votre système d'exploitation MAC avant de commencer la configuration. Vous pouvez le télécharger à partir du lien suivant :

http://www.lobotomo.com/products/IPSecuritas/

Cet article explique comment déployer une alternative Quick VPN pour Mac OS sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

Version du logiciel

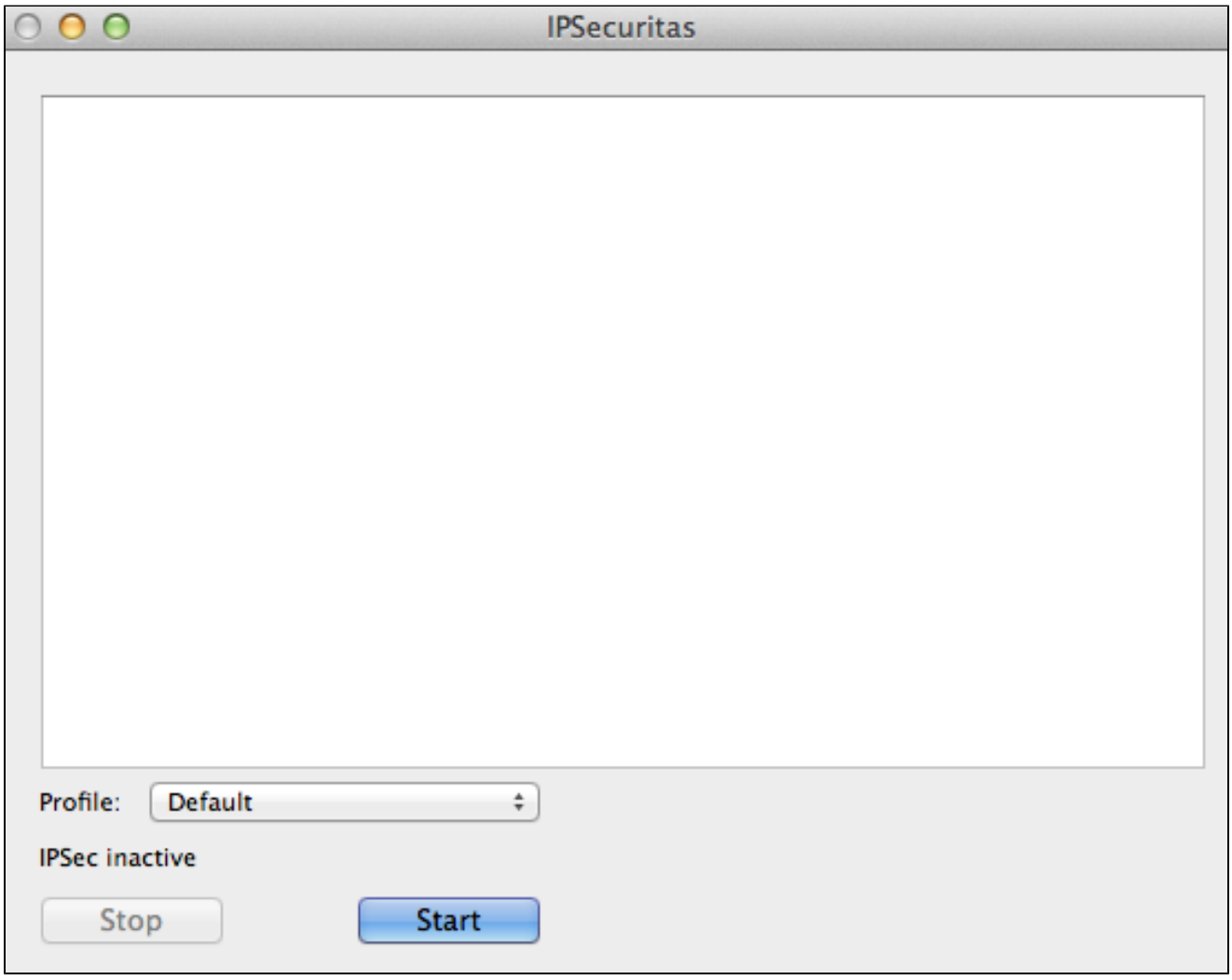
- v 4.2.2.08

Déployer une solution VPN rapide pour Mac OS

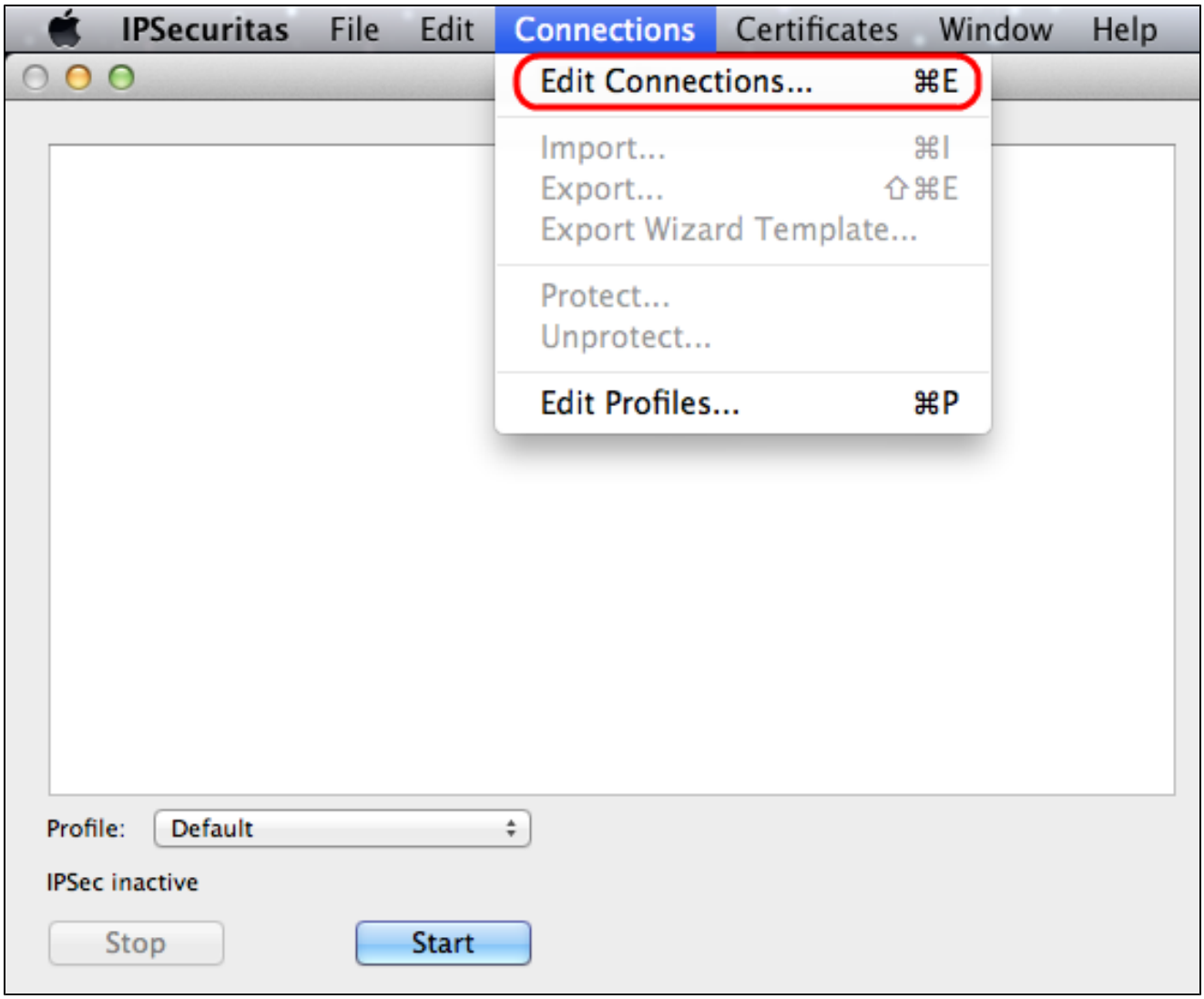
Remarque : la configuration VPN Client to Gateway du périphérique doit d'abord être effectuée. Pour en savoir plus sur la façon de configurer le client VPN vers la passerelle,

référez-vous à Configurer un tunnel d'accès à distance (client vers passerelle) pour les clients VPN sur les routeurs VPN RV016, RV042, RV042G et RV082.

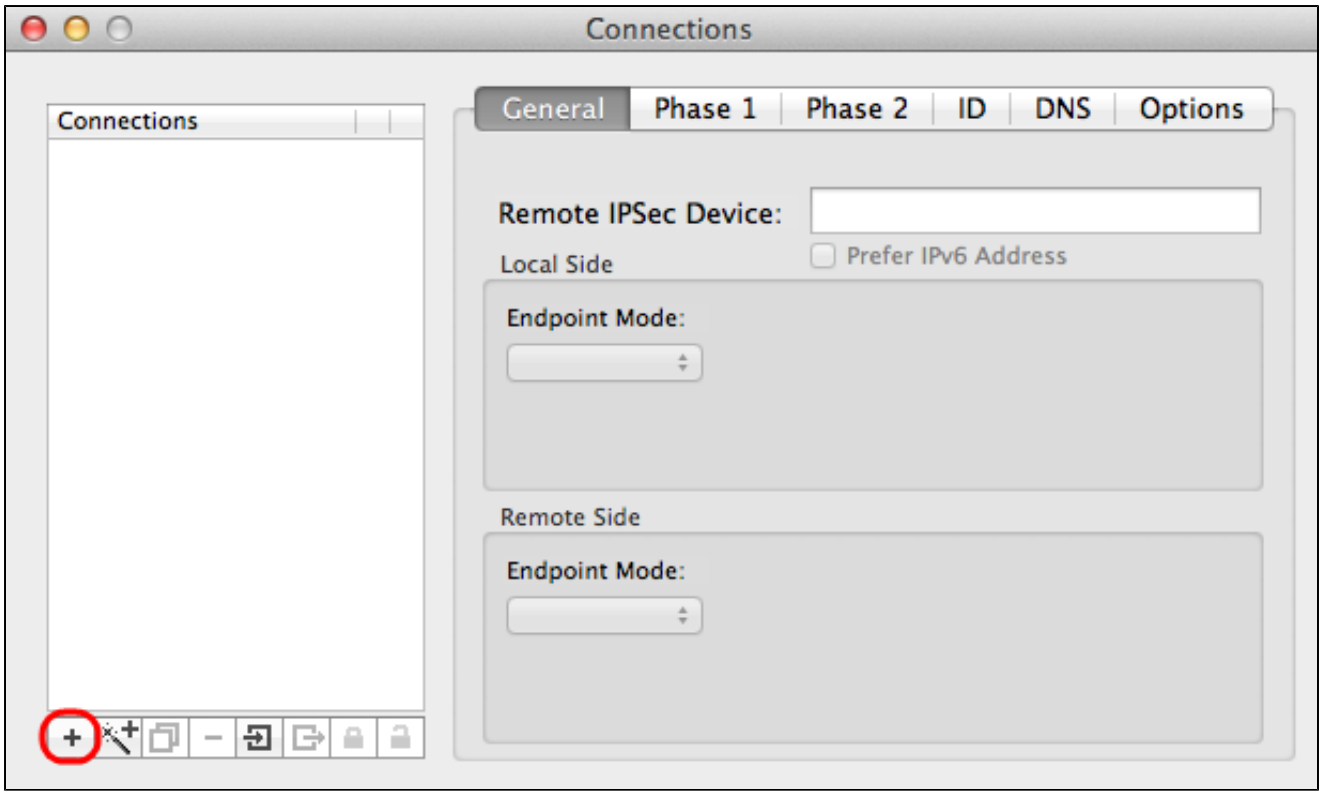
Étape 1. Exécutez IP Securitas sur Mac OS. La fenêtre IPSecuritas apparaît :



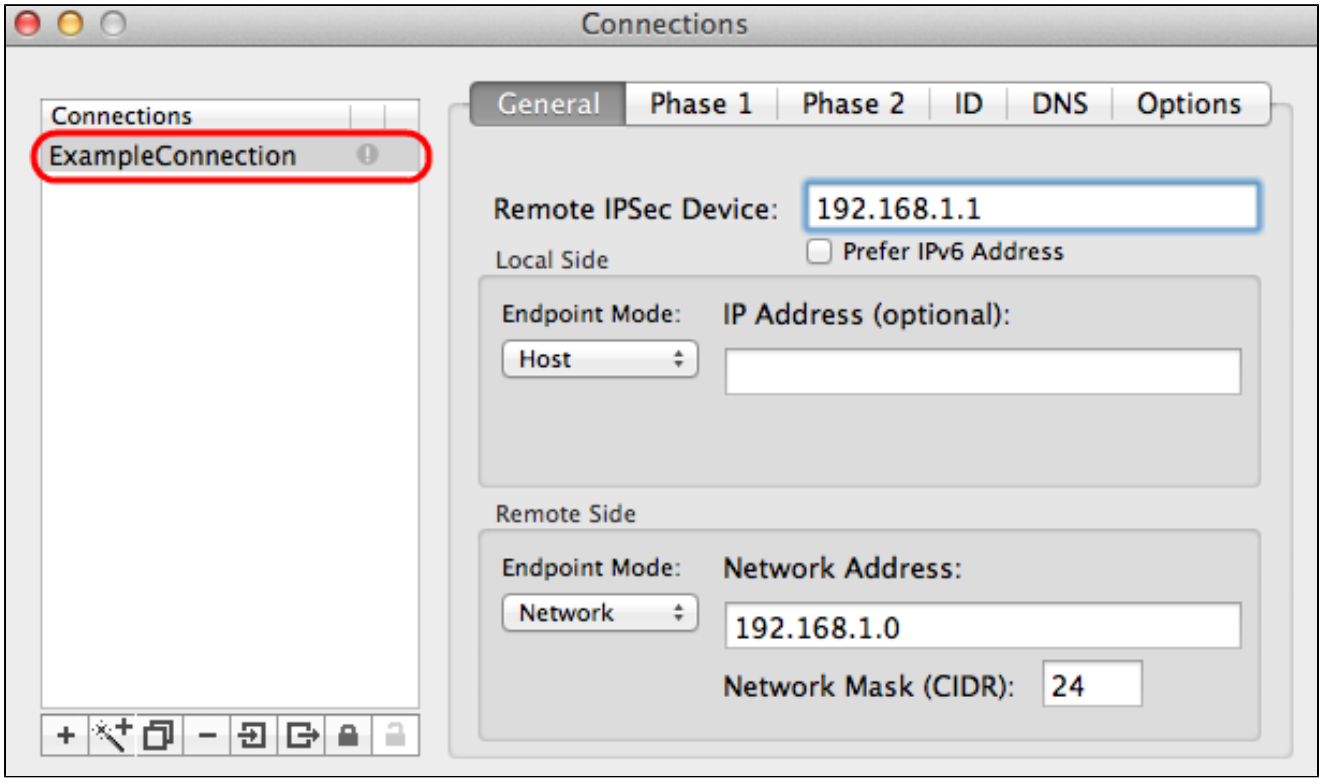
Étape 2. Cliquez sur Démarrer.



Étape 3. Dans la barre de menus, choisissez Connexions > Modifier les connexions. La fenêtre Connexions s'affiche.

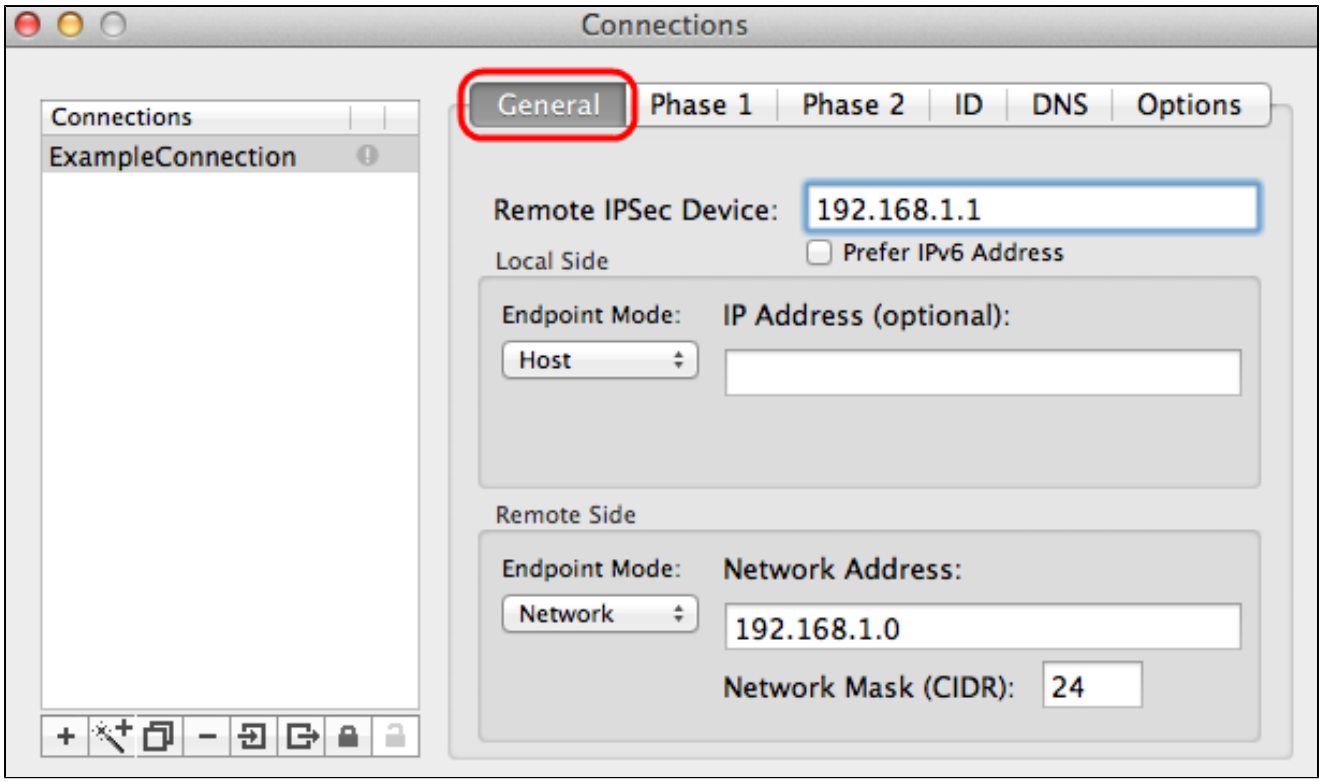


Étape 4. Cliquez sur l'icône + pour ajouter une nouvelle connexion.



Étape 5. Entrez un nom pour la nouvelle connexion sous connexions.

Généralités



Étape 1. Cliquez sur l’onglet General (Général).

Étape 2. Saisissez l'adresse IP du routeur distant dans le champ Remote IPSec Device.

Remarque : vous n'avez pas besoin de configurer le côté local, car cette configuration est destinée au client distant. Il vous suffit de configurer le mode distant.

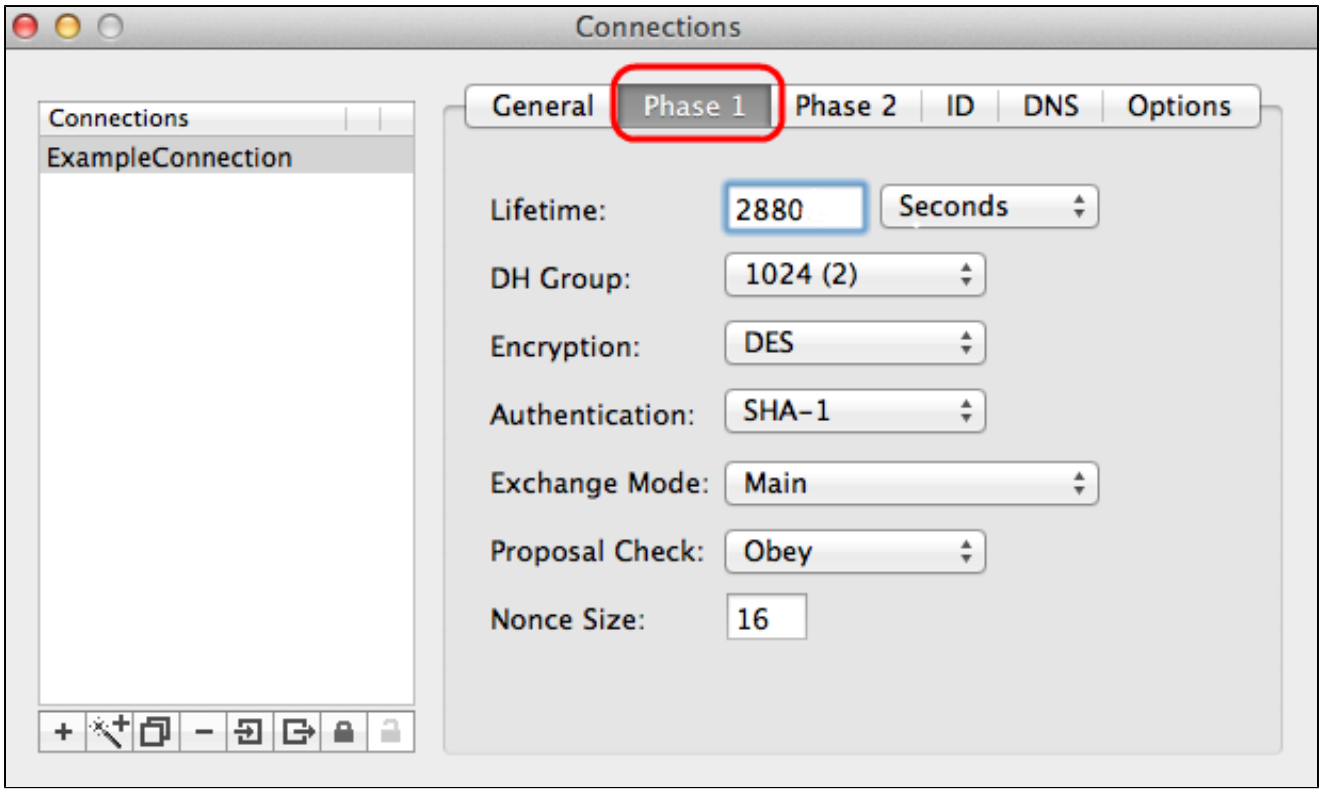
Étape 3. Dans la zone Remote Side, choisissez Network dans la liste déroulante Endpoint Mode.

Étape 4. Saisissez le masque de sous-réseau dans le champ Network Mask (CIDR).

Étape 5. Saisissez l'adresse du réseau distant dans le champ Network Address.

Phase 1

La phase 1 est l'association de sécurité logique (SA) simplex entre les deux extrémités du tunnel pour prendre en charge les communications authentifiées sécurisées.



Étape 1. Cliquez sur l'onglet Phase 1.

Étape 2. Saisissez la durée de vie que vous avez entrée lors de la configuration du tunnel dans le champ Lifetime. Si le délai expire, une nouvelle clé est renégociée automatiquement. La durée de vie de la clé peut être comprise entre 1081 et 86400 secondes. La valeur par défaut de la phase 1 est 28800 secondes.

Étape 3. Sélectionnez l'unité de temps appropriée pour la durée de vie dans la liste déroulante Durée de vie. La valeur par défaut est secondes.

Étape 4. Dans la liste déroulante Groupe DH, sélectionnez le groupe DH que vous avez entré pour la configuration du tunnel. Le groupe Diffie-Hellman (DH) est utilisé pour l'échange de clés.

Étape 5. Choisissez le type de cryptage dans la liste déroulante Encryption (Cryptage) que vous avez entrée pour la configuration du tunnel. La méthode Encryption détermine la longueur de la clé utilisée pour chiffrer/déchiffrer les paquets ESP (Encapsulating Security Payload).

Étape 6. Choisissez la méthode d'authentification que vous avez entrée pour la configuration du tunnel dans la liste déroulante Authentication. Le type d’authentification détermine la méthode d’authentification des paquets ESP.

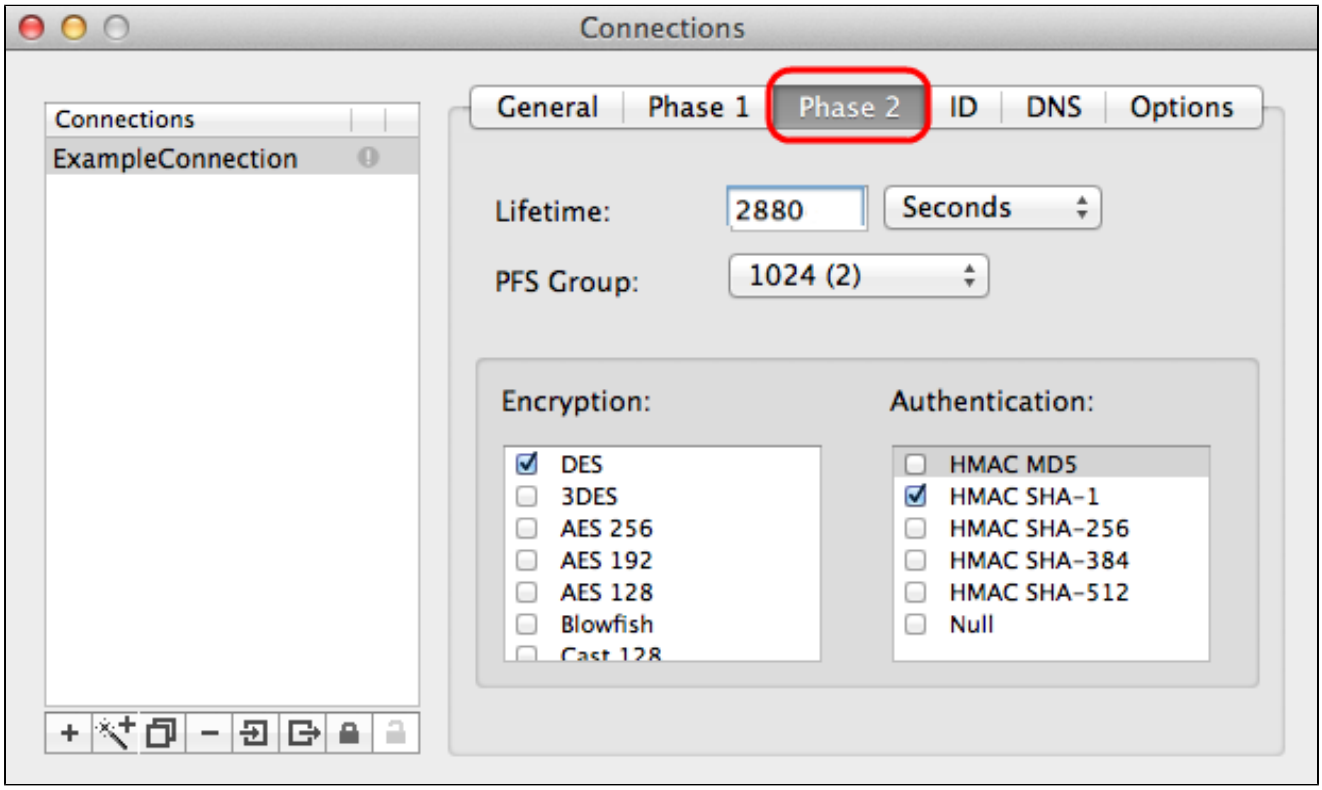
Étape 7. Sélectionnez le mode d'échange approprié dans la liste déroulante Mode d'échange.

· Main : représente le mode d'échange pour tous les types de passerelle, à l'exception du nom de domaine complet (FQDN).

· Aggressive : représente le mode d'échange pour la passerelle FQDN (Full Qualified Domain Name).

Phase 2

La phase 2 est l'association de sécurité qui permet de déterminer la sécurité du paquet de données pendant le passage des paquets de données à travers les deux points d'extrémité.



Étape 1. Cliquez sur l'onglet Phase 2.

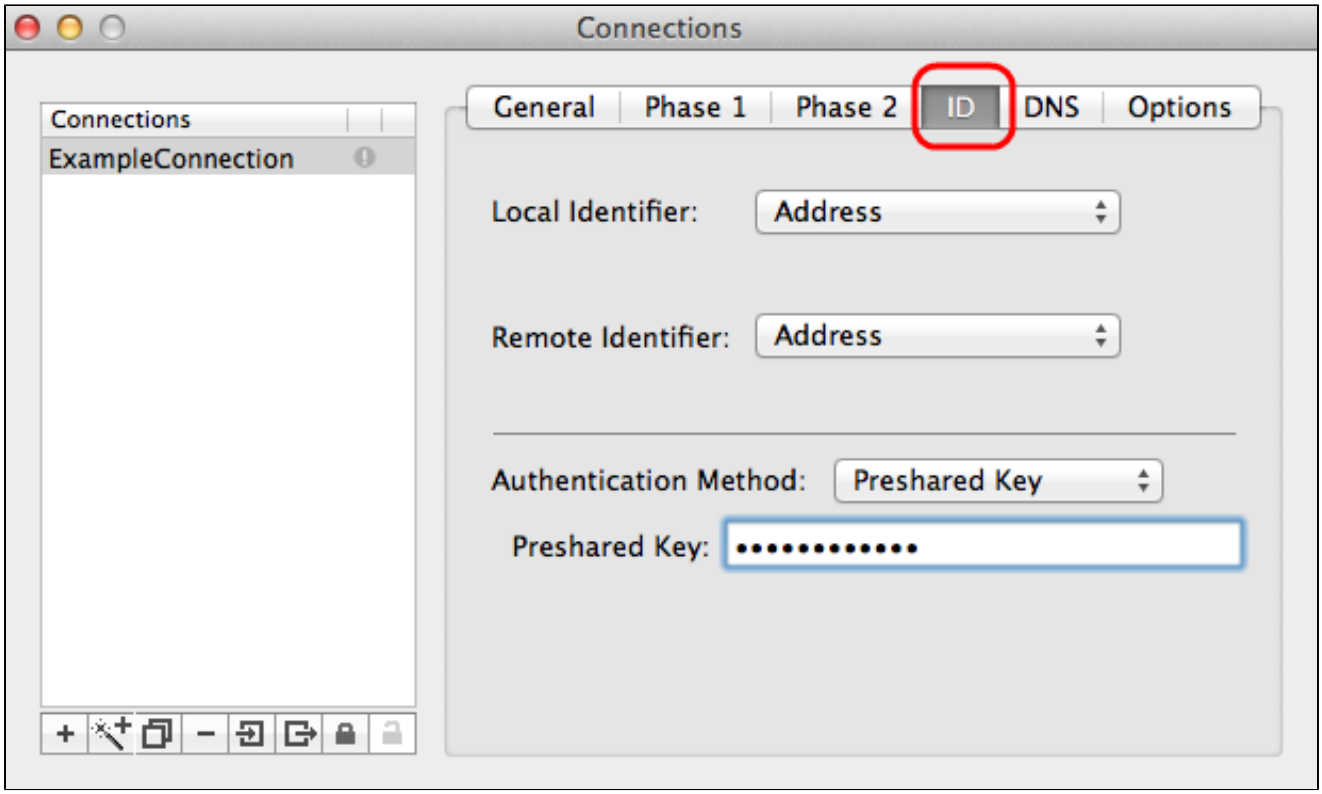
Étape 2. Saisissez la même durée de vie dans le champ Lifetime (Durée de vie) que celle que vous avez saisie pour la configuration du tunnel et pour la phase 1.

Étape 3. Choisissez la même unité de temps de la durée de vie dans la liste déroulante Durée de vie que vous avez entrée pour la configuration du tunnel et de la Phase 1.

Étape 4. Choisissez le même groupe DH dans la liste déroulante Groupe PFS (Perfect Forwarding Secrecy) que vous avez entré pour la configuration du tunnel.

Étape 5. Désactivez toutes les méthodes de chiffrement et d'authentification inutilisées. Cochez uniquement celles définies sous l'onglet Phase 1.

ID



Étape 1. Cliquez sur l'onglet ID.

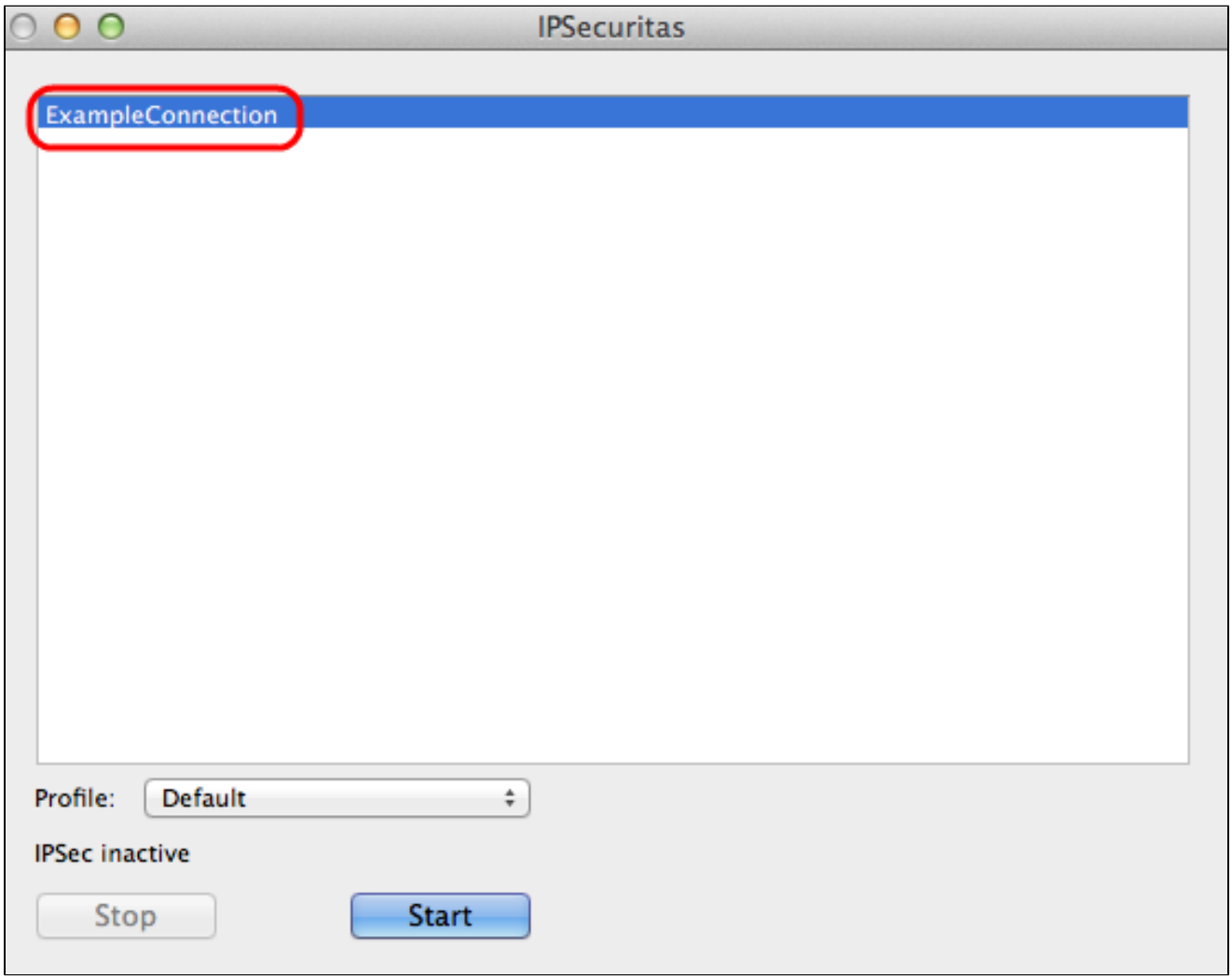
Étape 2. Choisissez la même méthode d'identificateur local que le tunnel dans la liste déroulante Identificateur local. Saisissez la valeur appropriée en fonction du type d'identificateur local, le cas échéant.

Étape 3. Choisissez la même méthode d'identificateur distant que le tunnel dans la liste déroulante Identificateur distant. Saisissez la valeur appropriée en fonction du type d'identificateur distant, si nécessaire.

Étape 4. Choisissez la même méthode d'authentification que le tunnel dans la liste déroulante Authentication Method. Saisissez la valeur d'authentification appropriée en fonction du type de méthode d'authentification, le cas échéant.

Étape 5. Cliquez sur l'icône x (cercle rouge) pour fermer la fenêtre de connexion. Les paramètres sont automatiquement enregistrés. La fenêtre IPSecuritas s'affiche.

Connexion



Étape 1. Dans la fenêtre IPSecuritas, cliquez sur Démarrer. L'utilisateur est alors connecté pour accéder au VPN.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.