# Visualisez/ajoutez a fait confiance au certificat d'IPSec sur les routeurs VPN RV320 et RV325

## Objectif

Des Certificats sont utilisés pour vérifier l'identité de l'utilisateur sur un ordinateur ou un Internet et pour améliorer une conversation privée ou sécurisée. Dans RV320, vous pouvez ajouter un maximum de 50 Certificats par l'auto-signature ou la tiers autorisation. Vous pouvez exporter un certificat pour un client ou pour un administrateur, sauf que dans un PC ou un USB et puis importez cela. IPsec est utilisé dans l'échange des données de génération de clés et d'authentification, du protocole principal d'établissement, de l'algorithme de chiffrement, ou du mécanisme d'authentification de l'authentification et de la validation sécurisées des transactions en ligne avec des Certificats SSL.

Cet article explique comment visualiser et ajouter a fait confiance au certificat d'IPSec sur la gamme de routeur VPN RV32x.

## Périphériques applicables

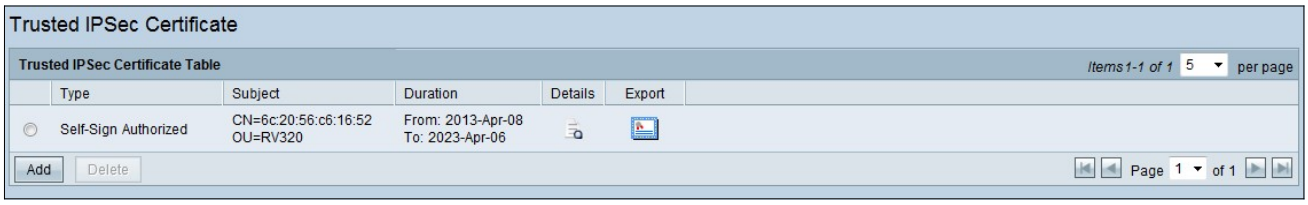
- RV320 conjuguent routeur VPN BLÊME
- Double routeur VPN BLÊME du gigabit RV325

## Version de logiciel

- v1.1.0.09

## Certificat de confiance d'IPSec

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Gestion de certificat > a fait confiance au certificat d'IPSec**. La page *de confiance de certificat d'IPSec* s'ouvre :




La page *de confiance de certificat d'IPSec* contient les champs suivants :

- Les types de type deux de Certificats sont disponibles

  – Auto-signé — C'est un certificat de Protocole SSL (Secure Socket Layer) qui est signé par son propre créateur. Il est moins digne de confiance car il ne peut pas être annulé si la clé privée est compromise d'une certaine manière par l'attaquant.

  – Demande de signature certifiée — C'est un Infrastructure à clés publiques (PKI) qui est envoyé à l'autorité de certification pour s'appliquer pour un certificat d'identité numérique. Il est plus sécurisé qu'auto-signé car la clé privée est maintenue secrète.

• Sujet — Il affiche à qui le certificat est émis.

• Durée — Elle affiche que la date le certificat expire. La Sécurité du site Web ne peut pas être garantie si cette date a été dépassée.

• Détails — Il affiche tous les détails au sujet de l'émetteur de certificat, numéro de série de certificat, et la date d'expiration sont générées par le service CA. Les informations sont utilisées quand une demande de signature de certificat de générer est créée et envoyée à votre service CA pour la validation.

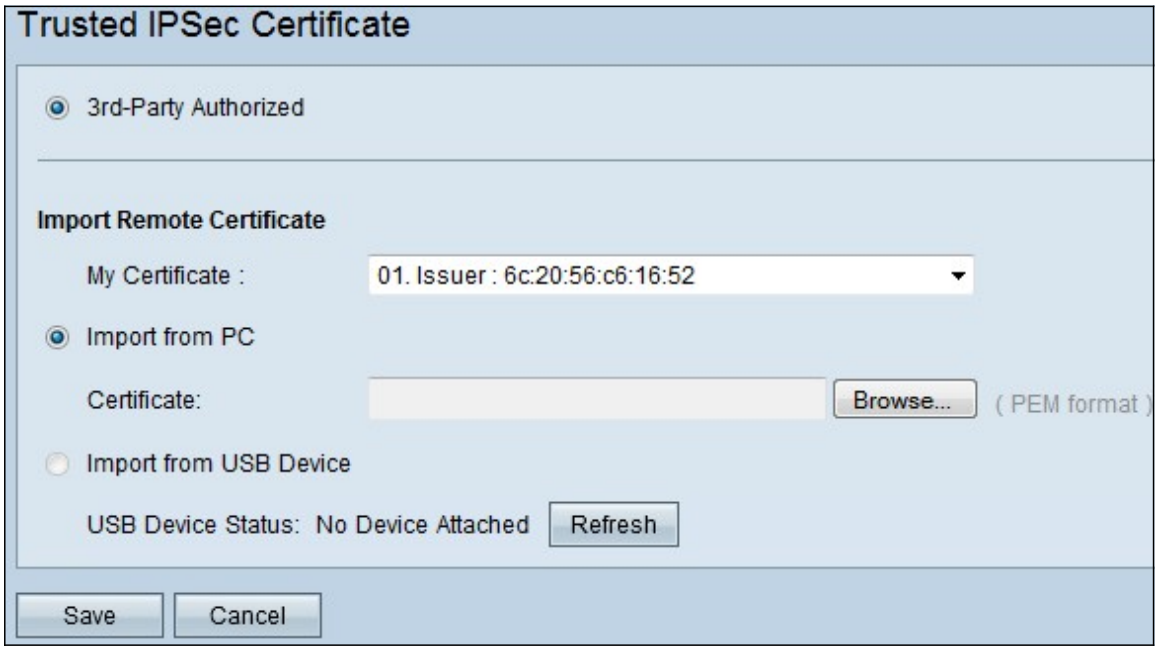
• Exportation — Pour exporter ou afficher un certificat, cliquez sur l'icône de certificat d'exportation. Affichages d'une fenêtre externe où vous pouvez ouvrir le certificat pour l'inspection ou sauvegarder le certificat à un PC.

Étape 2. Cliquez sur la case d'**enable** pour activer un certificat particulier d'IPSec.

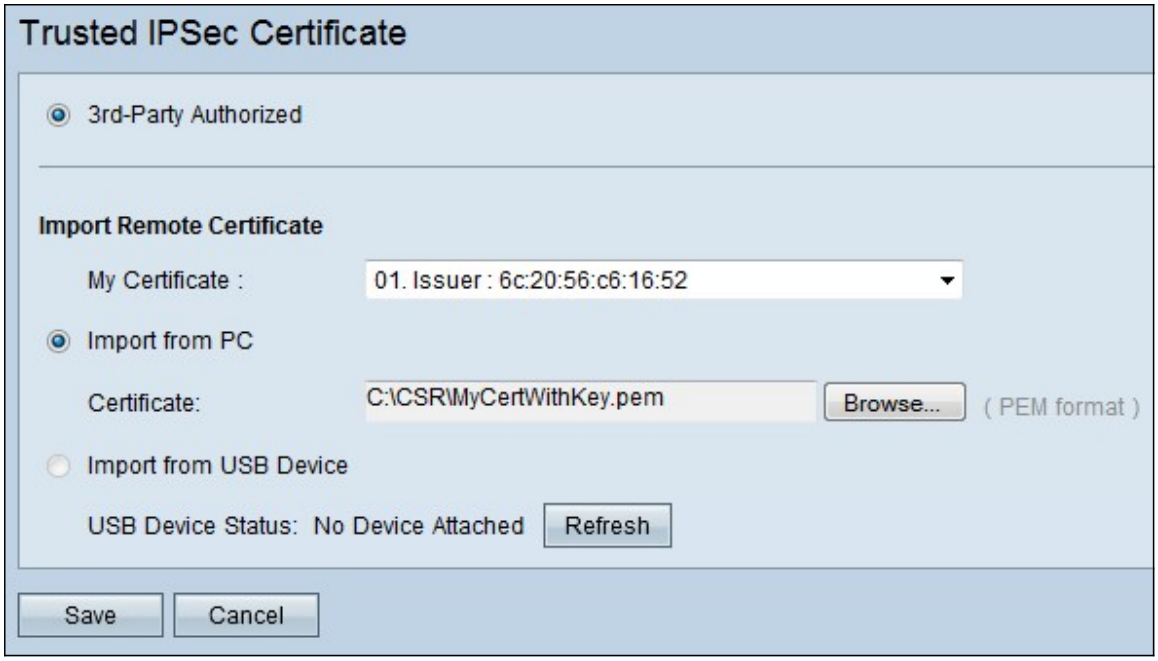
Étape 3. Cliquez sur Add pour obtenir un nouveau certificat du PC ou d'USB.

• Importation en provenance de PC — Du PC vous pouvez localiser le certificat et l'importation au périphérique

• Importation en provenance d'USB — De l'USB qui est relié au périphérique vous pouvez également importer le certificat.




Étape 3. Cliquez sur en fonction **Browse** pour localiser le certificat de CA du PC.




Étape 4. **Sauvegarde de** clic pour ajouter le certificat au Tableau de confiance de certificat d'IPSec.