Gestion des certificats sur le routeur de la gamme RV34x

Objectif

Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet aux parties de confiance de dépendre des signatures ou des assertions faites par la clé privée qui correspond à la clé publique qui est certifiée. Un routeur peut générer un certificat auto-signé, un certificat créé par un administrateur réseau. Il peut également envoyer des demandes aux autorités de certification (AC) pour demander un certificat d'identité numérique. Il est important d'avoir des certificats légitimes provenant de demandes tierces.

Parlons d'obtenir un certificat d'une autorité de certification (AC). Une autorité de certification est utilisée pour l'authentification. Les certificats sont achetés sur un certain nombre de sites tiers. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'AC est une source fiable qui vérifie que vous êtes une entreprise légitime et qu'elle peut être approuvée. Selon vos besoins, un certificat à un coût minime. Vous êtes extrait par l'autorité de certification, et une fois qu'ils vérifient vos informations, ils vous délivrent le certificat. Ce certificat peut être téléchargé sous forme de fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et le télécharger ici.

L'objectif de cet article est de vous montrer comment générer, exporter, importer et importer des certificats sur le routeur de la gamme RV34x.

Périphériques pertinents | Version du logiciel

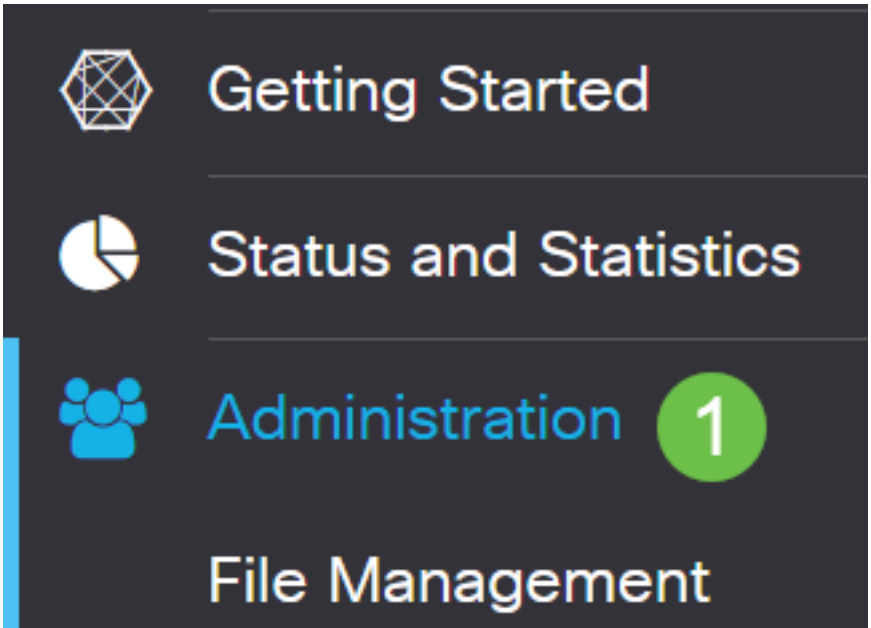
- Gamme RV34x |1.0.03.20

Gestion des certificats sur le routeur

Générer CSR/Certificat

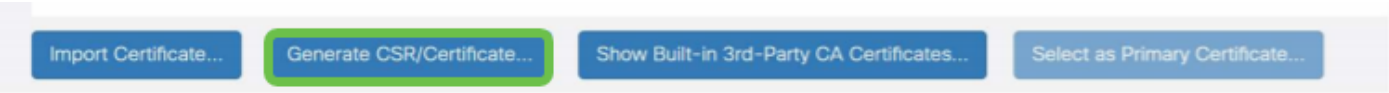
Étape 1

Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Administration > Certificate**.



Étape 2

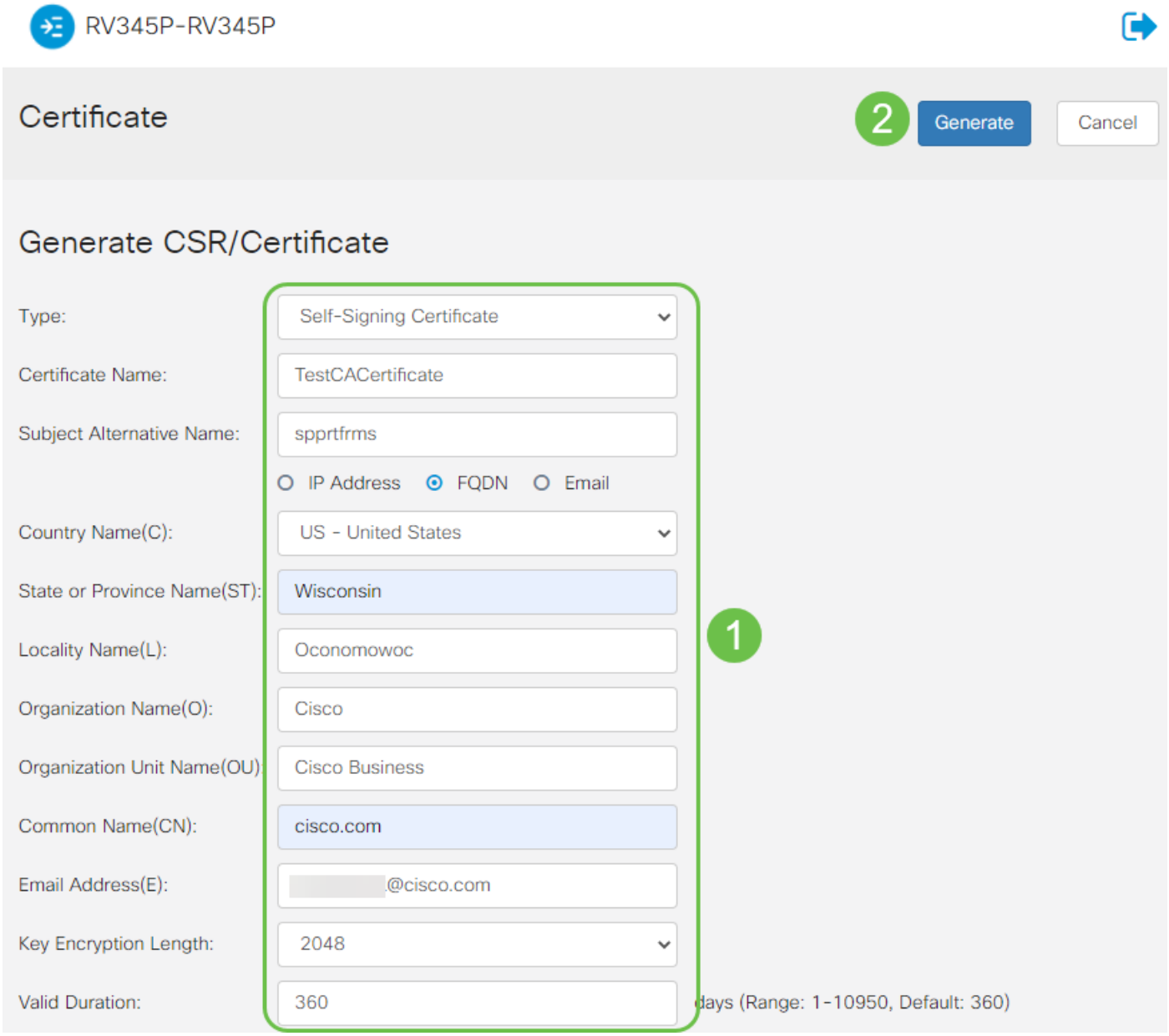
Cliquez sur **Générer CSR/Certificate**. Vous accéderez à la page Generate CSR/Certificate.



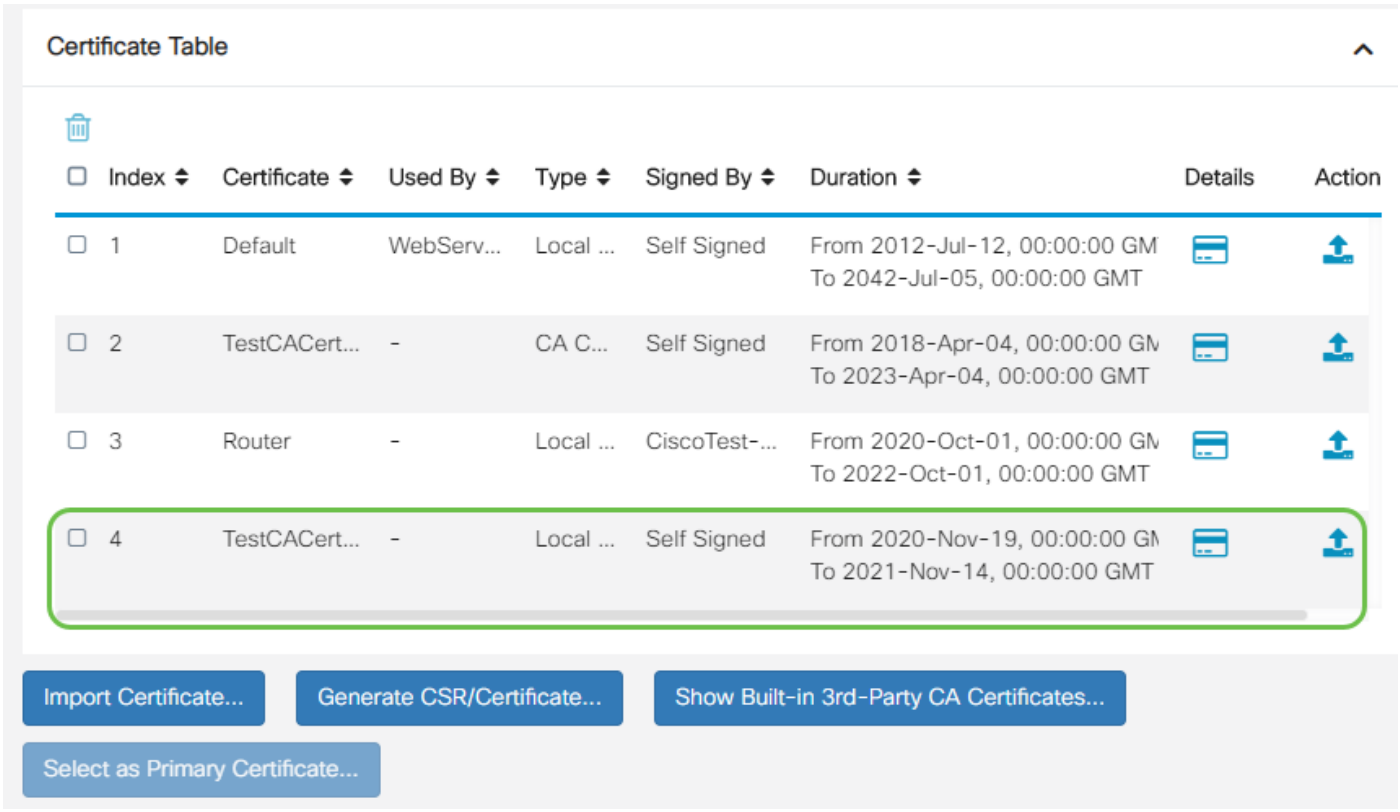
Étape 3

Remplissez les zones suivantes :

- Choisissez le type de certificat approprié
  - Certificat auto-signant : certificat SSL (Secure Socket Layer) signé par son créateur. Ce certificat est moins fiable, car il ne peut pas être annulé si la clé privée est compromise d'une manière ou d'une autre par un pirate.
  - Demande de signature certifiée — Il s'agit d'une infrastructure à clé publique (ICP) qui est envoyée à l'autorité de certification pour demander un certificat d'identité numérique. Il est plus sécurisé que autosigné car la clé privée est gardée secrète.
- Entrez un nom pour votre certificat dans le champ *Nom du certificat* pour identifier la demande. Ce champ ne peut pas être vide ni contenir d'espaces et de caractères spéciaux.
- (Facultatif) Sous la zone Nom alternatif de l'objet, cliquez sur une case d'option. Les options sont les suivantes :
  - IP Address : saisissez une adresse IP (Internet Protocol).
  - FQDN : saisissez un nom de domaine complet (FQDN)
  - E-mail : saisissez une adresse e-mail
- Dans le champ *Subject Alternative Name*, saisissez le nom de domaine complet (FQDN).
- Choisissez un nom de pays dans lequel votre organisation est légalement enregistrée dans la liste déroulante Nom du pays.
- Entrez un nom ou une abréviation de l'État, de la province, de la région ou du territoire où se trouve votre organisation dans le champ *Nom* de l'*État ou de la province(ST)*.
- Entrez le nom de la localité ou de la ville dans laquelle votre organisation est enregistrée ou se trouve dans le champ *Nom de la localité*.
- Entrez un nom sous lequel votre entreprise est légalement enregistrée. Si vous vous inscrivez en tant que petite entreprise ou propriétaire unique, saisissez le nom du demandeur de certificat dans le champ *Nom de l'organisation*. Les caractères spéciaux ne peuvent pas être utilisés.
- Entrez un nom dans le champ *Nom de l'unité d'organisation* pour différencier les divisions d'une organisation.
- Entrez un nom dans le champ *Nom commun*. Ce nom doit être le nom de domaine complet du site Web pour lequel vous utilisez le certificat.
- Saisissez l'adresse e-mail de la personne qui souhaite générer le certificat.
- Dans la liste déroulante Key Encryption Length, sélectionnez une longueur de clé. Les options sont 512, 1024 et 2048. Plus la longueur de la clé est grande, plus le certificat est sécurisé.
- Dans le champ *Durée valide*, saisissez le nombre de jours pendant lesquels le certificat sera valide. Il est défini par défaut à 360.
- Cliquez sur **Generate**.



Note: Le certificat généré doit maintenant apparaître dans la table de certificats.

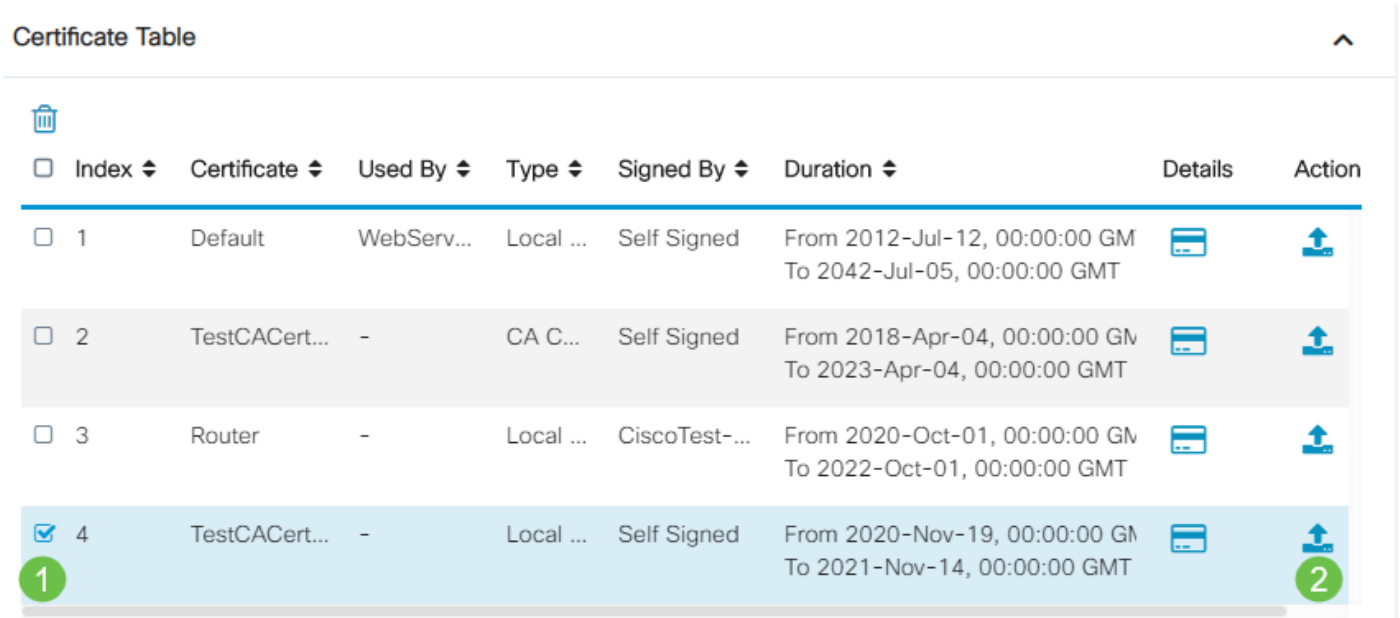


Vous devez maintenant avoir créé un certificat sur le routeur RV345P.

Exporter un certificat

Étape 1

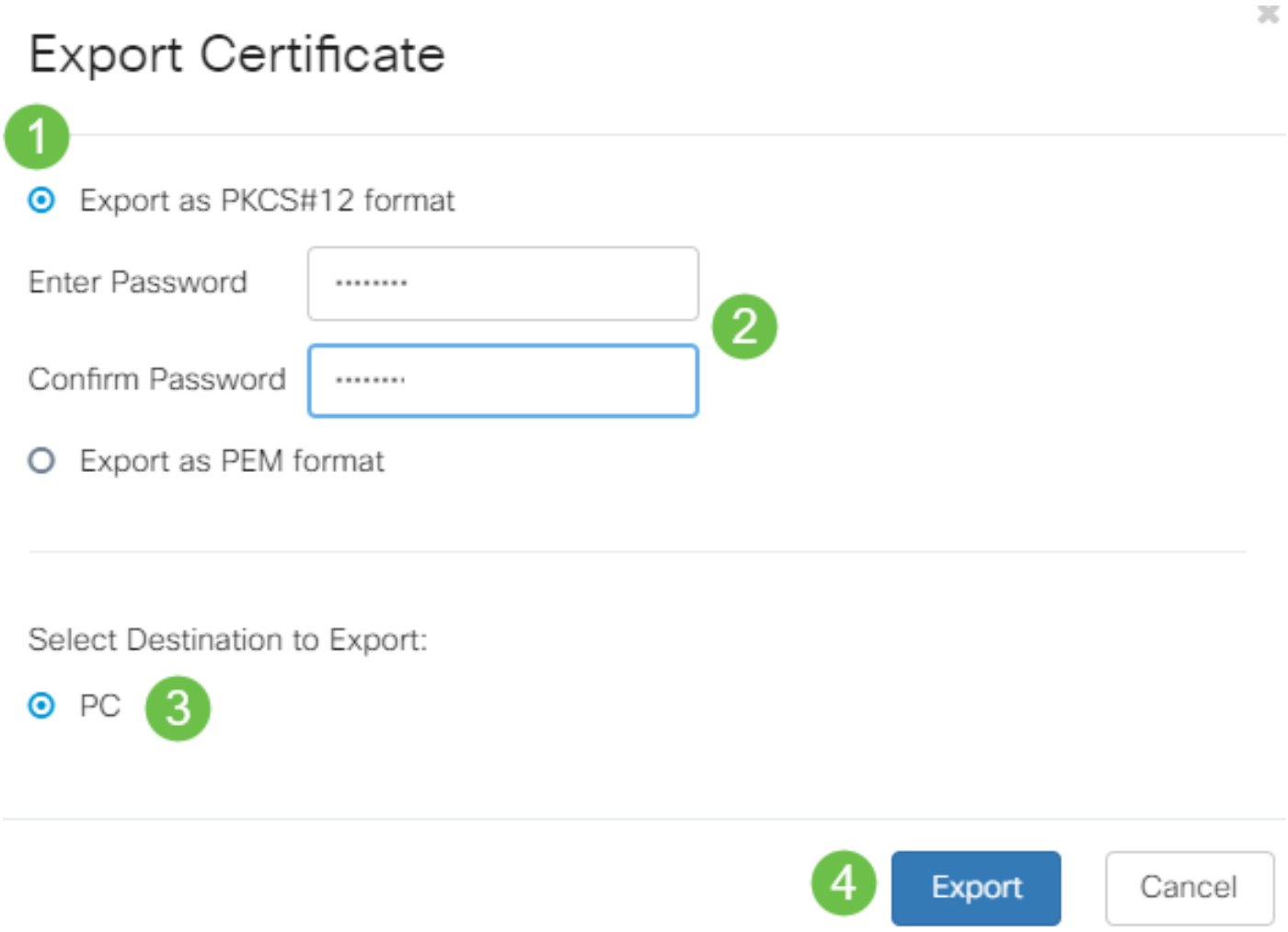
Dans la table des certificats, cochez la case du certificat à exporter et cliquez sur l'**icône d'exportation**.



Étape 2

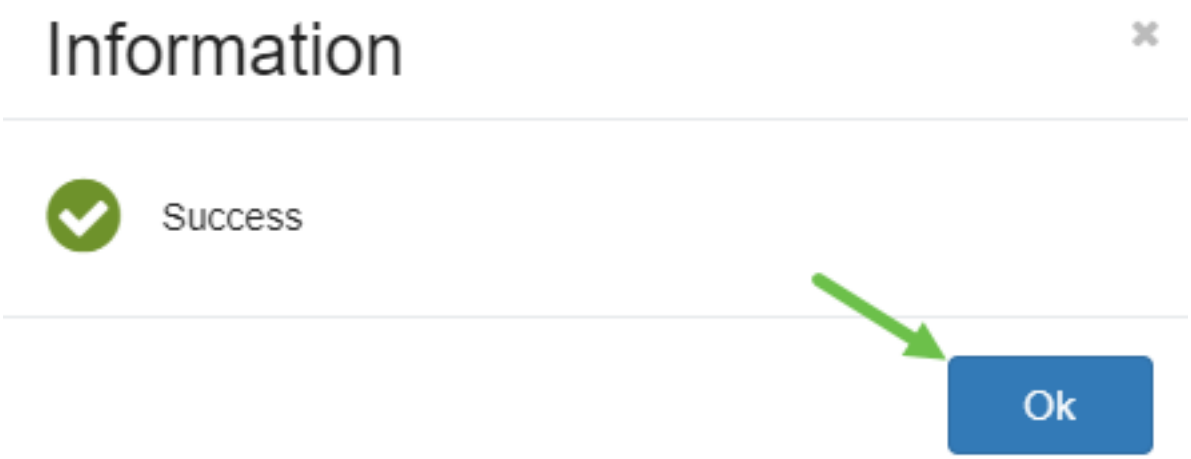
- Cliquez sur un format pour exporter le certificat. Les options sont les suivantes :
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 est un certificat exporté qui vient dans une extension .p12. Un mot de passe est nécessaire pour chiffrer le fichier afin de le protéger lors de son exportation, de son importation et de sa suppression.

    - PEM - La fonction PEM (Privacy Enhanced Mail) est souvent utilisée pour les serveurs Web afin qu'ils puissent être facilement traduits en données lisibles à l'aide d'un éditeur de texte simple tel que le bloc-notes.
- Si vous avez choisi PEM, cliquez simplement sur **Exporter**.
- Entrez un mot de passe pour sécuriser le fichier à exporter dans le champ *Enter Password*.
- Saisissez à nouveau le mot de passe dans le champ *Confirmer le mot de passe*.
- Dans la zone Sélectionner la destination, PC a été choisi et est la seule option actuellement disponible.
- Cliquez sur **Exporter**.



Étape 3

Un message indiquant le succès du téléchargement apparaît sous le bouton Télécharger. Un fichier commence à être téléchargé dans votre navigateur. Cliquez sur **OK**.

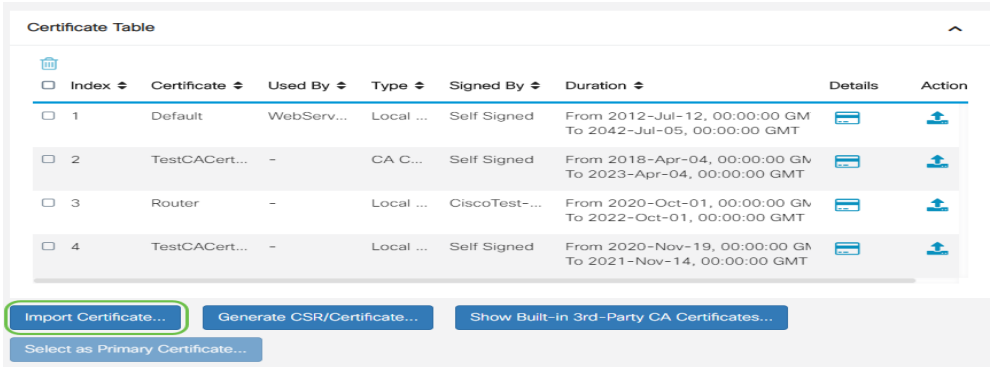


Vous devez maintenant avoir exporté un certificat sur le routeur de la gamme Rv34x.

Importer un certificat

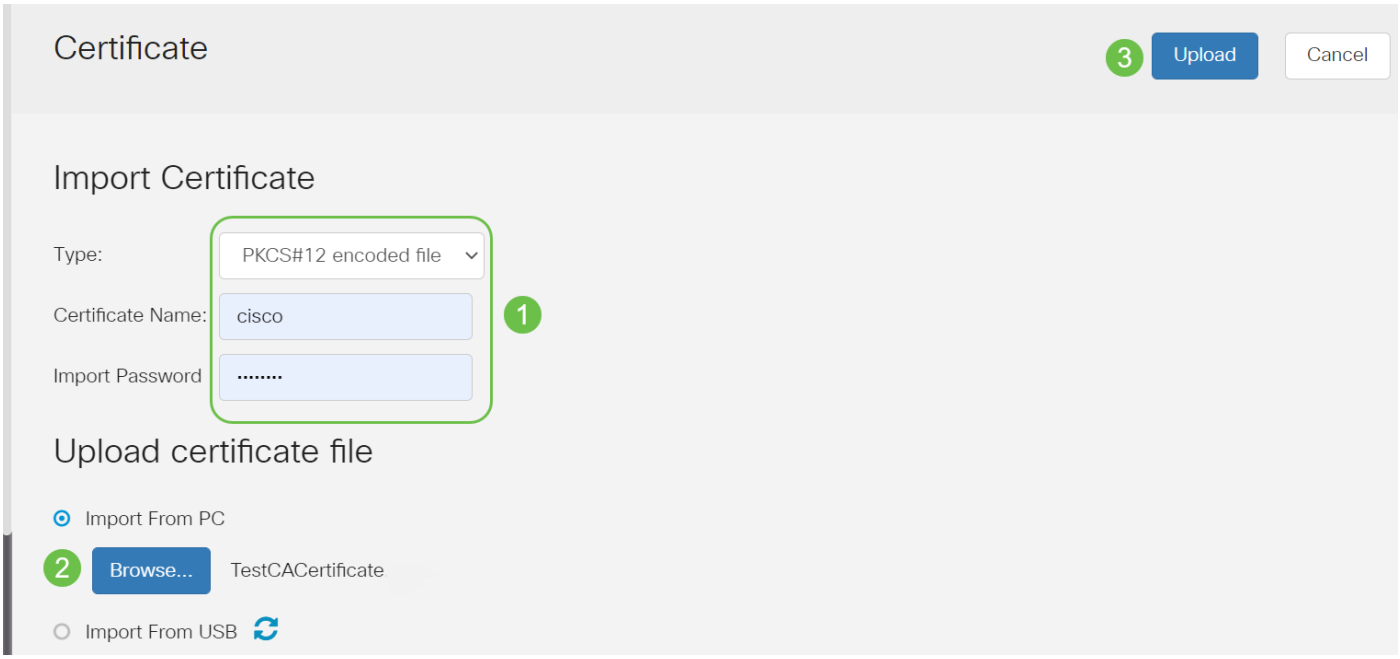
Étape 1

Cliquez sur **Importer un certificat...**.

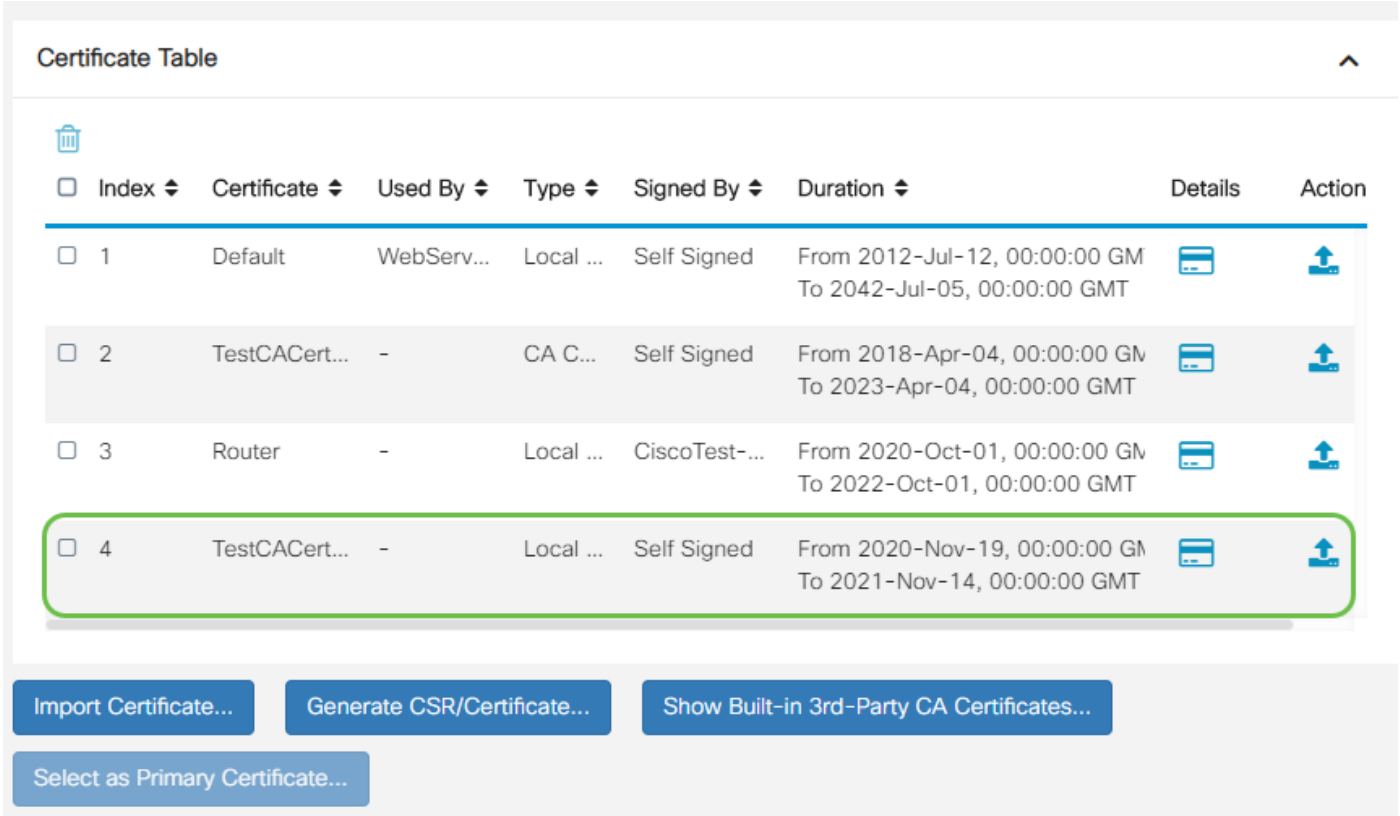


Étape 2

- Sélectionnez le type de certificat à importer dans la liste déroulante. Les options sont les suivantes :
  - Local Certificate : certificat généré sur le routeur.
  - Certificat CA — Certificat certifié par une autorité tierce de confiance qui a confirmé que les informations contenues dans le certificat sont exactes.
  - Fichier codé PKCS #12 — Les normes de cryptographie à clé publique (PKCS) #12 sont un format de stockage d'un certificat de serveur.
- Entrez un nom pour le certificat dans le champ *Nom du certificat*.
- Si PKCS #12 a été sélectionné, saisissez un mot de passe pour le fichier dans le champ *Importer le mot de passe*. Sinon, passez à l'étape 3.
- Cliquez sur une source pour importer le certificat. Les options sont les suivantes :
  - Importer à partir du PC
  - Importer depuis USB
- Si le routeur ne détecte pas de lecteur USB, l'option Import from USB est grisée.
- Si vous avez choisi Import From USB et que votre port USB n'est pas reconnu par le routeur, cliquez sur Refresh.
- Cliquez sur le bouton Choisir un fichier et choisissez le fichier approprié.
- Cliquez sur **Upload** (charger).



Une fois que vous avez réussi, vous accédez automatiquement à la page principale du certificat. La table de certificats contient le certificat récemment importé.



Vous devez maintenant avoir importé un certificat sur votre routeur de la gamme RV34x.