Solution de contournement pour le téléchargement du certificat de routeur de la gamme RV32x

Résumé

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.

Il existe deux façons pour que CA signe les certificats :

1. L'autorité de certification signe le certificat avec des clés privées.

2. L'autorité de certification signe les certificats à l'aide de CSR généré par RV320/RV325.

Les modèles RV320 et RV325 prennent uniquement en charge les certificats au format .pem. Dans les deux cas, vous devez obtenir des certificats au format .pem auprès de l'autorité de certification. Si vous obtenez un autre certificat de format, vous devez convertir le format par vous-même ou demander de nouveau le certificat de format .pem à partir de l'autorité de certification.

La plupart des fournisseurs de certificats commerciaux utilisent des certificats intermédiaires. Lorsque le certificat intermédiaire est émis par l'autorité de certification racine de confiance, tout certificat émis par le certificat intermédiaire hérite de la confiance de la racine de confiance, comme une chaîne de certification de confiance.

Ce guide décrit comment importer un certificat émis par l'autorité de certification intermédiaire sur RV320/RV325.

Date d'identification

24 février 2017

Date de résolution

S/O

Produits affectés

RV320/RV325	1.1.1.06 et

	postérieures

Signature de certificat à l'aide de clés privées

Dans cet exemple, nous supposons que vous avez obtenu un RV320.pem de l'autorité de certification intermédiaire tierce. Le contenu du fichier est le suivant : clé privée, certificat, certificat d'autorité de certification racine, certificat d'autorité de certification intermédiaire.

Note: L'obtention de plusieurs fichiers de l'autorité de certification intermédiaire au lieu d'un seul fichier est facultative. Mais vous pouvez trouver au-dessus de quatre parties des différents fichiers.

Vérifiez si le fichier de certificat de l'autorité de certification contient à la fois le certificat de l'autorité de certification racine et le certificat intermédiaire. Le RV320/RV325 requiert le certificat intermédiaire et le certificat racine dans un certain ordre dans le bundle CA, le certificat racine d'abord, puis le certificat intermédiaire. Deuxièmement, vous devez combiner le certificat RV320/RV325 et la clé privée en un seul fichier.

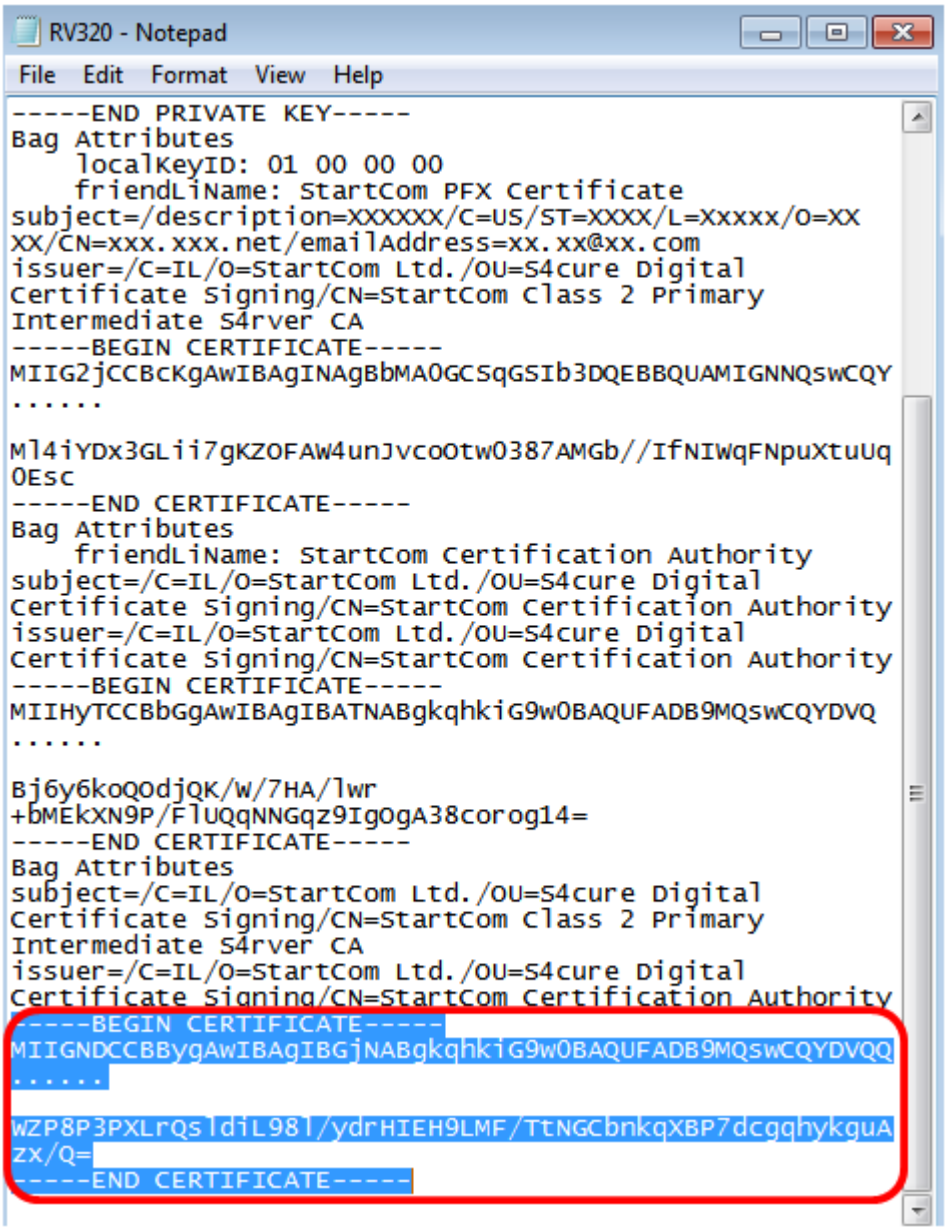
Note: N'importe quel éditeur de texte peut être utilisé pour ouvrir et modifier les fichiers. Il est important de s'assurer que les lignes vides, les espaces ou les retours de transport supplémentaires ne feront pas fonctionner le plan comme prévu.

Combinaison des certificats

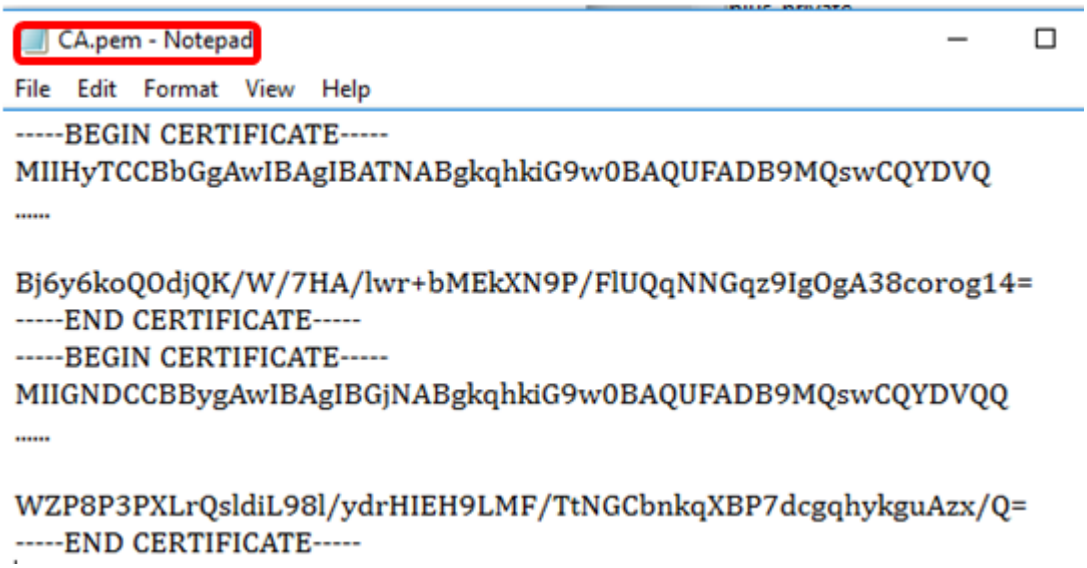
Étape 1. Ouvrez le RV320.pem, copiez le deuxième certificat (certificat racine) et le troisième certificat (certificat intermédiaire), y compris le message de début/fin.

Note: Dans cet exemple, la chaîne de texte en surbrillance est le certificat racine.

Note: Dans cet exemple, la chaîne de texte mise en surbrillance est le certificat intermédiaire.

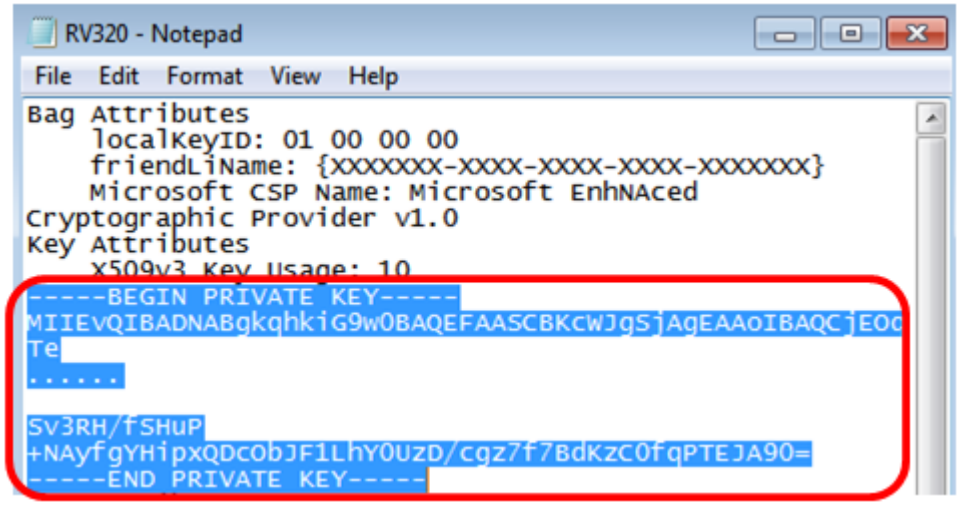


Étape 2. Collez le contenu dans un nouveau fichier et enregistrez-le en tant que CA.pem.

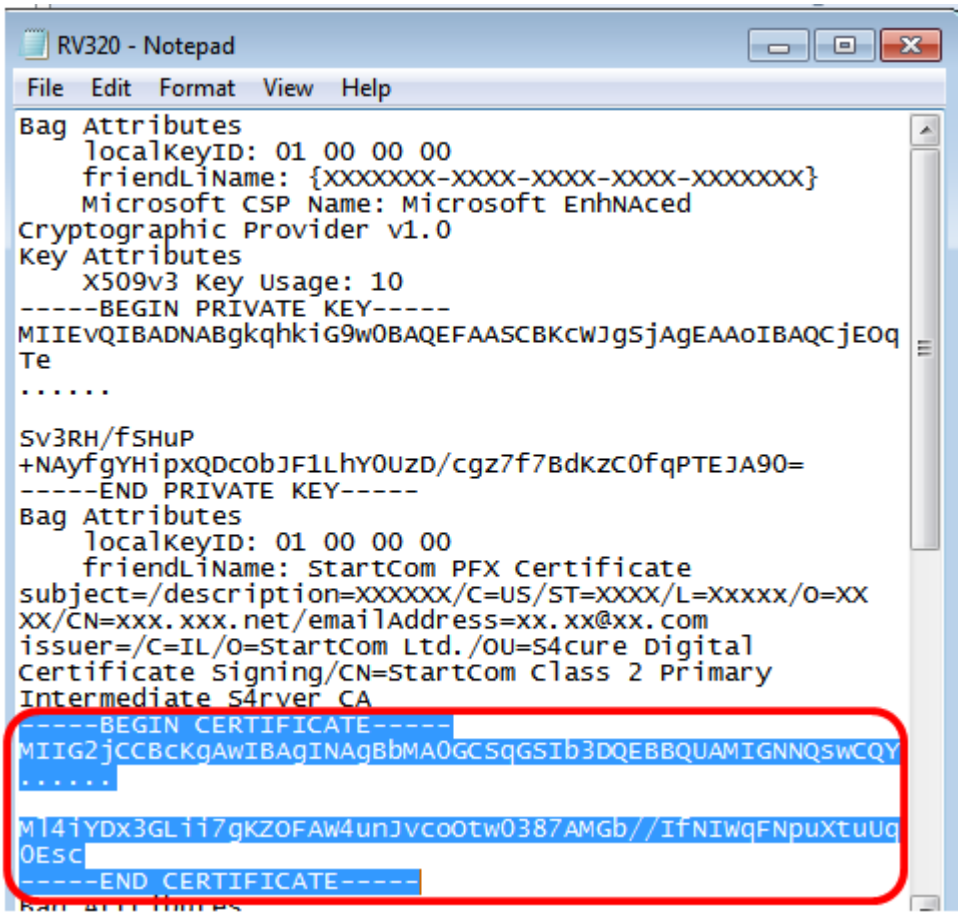


Étape 3. Ouvrez le fichier RV320.pem, puis copiez la section clé privée et le premier certificat, y compris le message de début/fin.

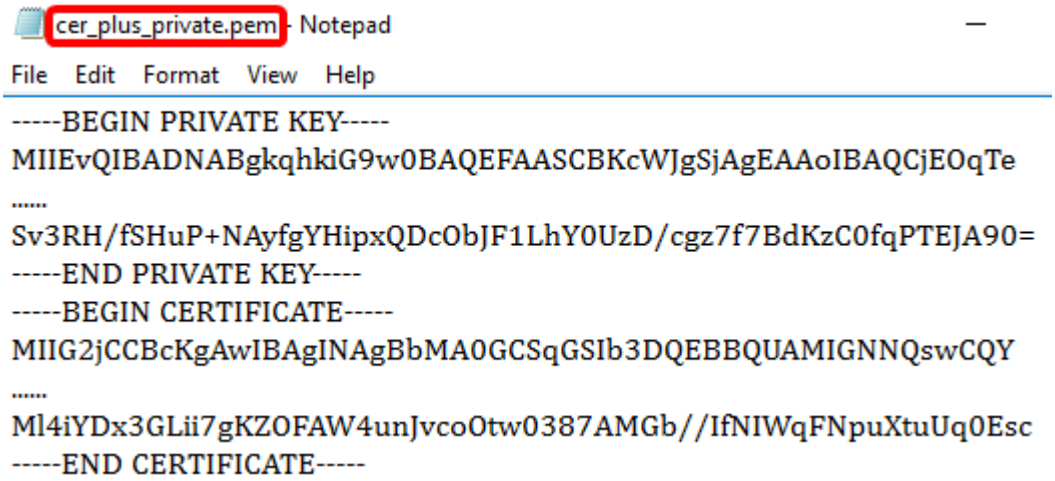
Note: Dans l'exemple ci-dessous, la chaîne de texte mise en surbrillance est la section clé privée.



Note: Dans l'exemple ci-dessous, la chaîne de texte mise en surbrillance est le premier certificat.



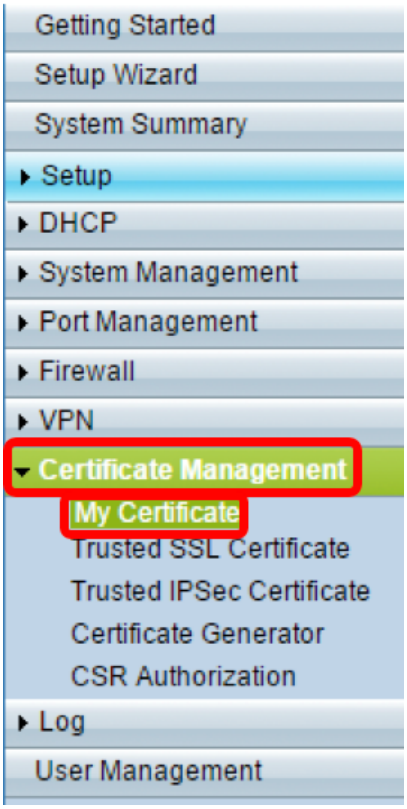
Étape 4. Collez le contenu dans un nouveau fichier et enregistrez-le en tant que cer_plus_private.pem



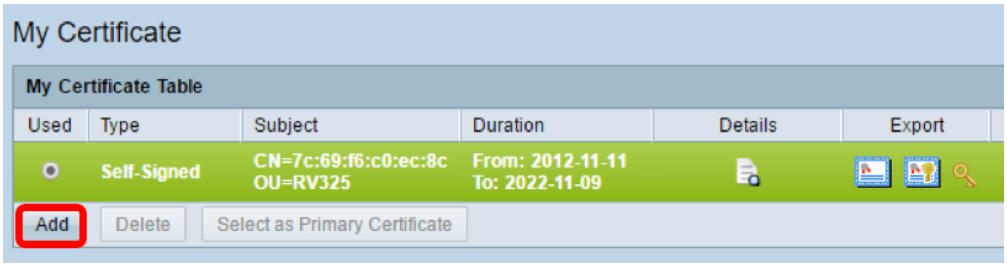
Note: Si la version du microprogramme RV320/RV325 est inférieure à 1.1.1.06, assurez-vous qu'il y a deux flux de ligne à la fin du fichier (cer_plus_private.pem). Dans le micrologiciel après 1.1.1.06, vous n'avez pas besoin d'ajouter deux flux de ligne supplémentaires. Dans cet exemple, une version abrégée du certificat est affichée à des fins de démonstration uniquement.

Importer CA.pem et cer_plus_private.pem RV320/RV325

Étape 1. Connectez-vous à l'utilitaire Web du routeur RV320 ou RV325 et choisissez **Certificate Management > My Certificate**.



Étape 2. Cliquez sur **Ajouter** pour importer le certificat.



Étape 3. Cliquez sur la case d'option *Autorisé tiers* pour importer le certificat.

Étape 4. Dans la zone *Importer un jeu de certificats complet*, cliquez sur une case d'option pour choisir la source des certificats enregistrés. Les options sont les suivantes :

- *Import from PC* - Sélectionnez cette option si les fichiers sont trouvés sur l'ordinateur.
- *Import from USB* - Sélectionnez cette option pour importer les fichiers à partir d'un lecteur flash.

Note: Dans cet exemple, **Importer à partir du PC** est choisi.

Étape 5. Dans la zone *Certificat CA*, cliquez sur **Parcourir...** et localisez le fichier CA.pem. fichier.

Note: Si vous exécutez le micrologiciel après la version 1.1.0.6, cliquez sur le bouton Choisir et localisez le fichier nécessaire.

Étape 6. Dans la zone *Certificate + Private Key*, cliquez sur **Browse...**et localisez le fichier er_plus_private.pem.

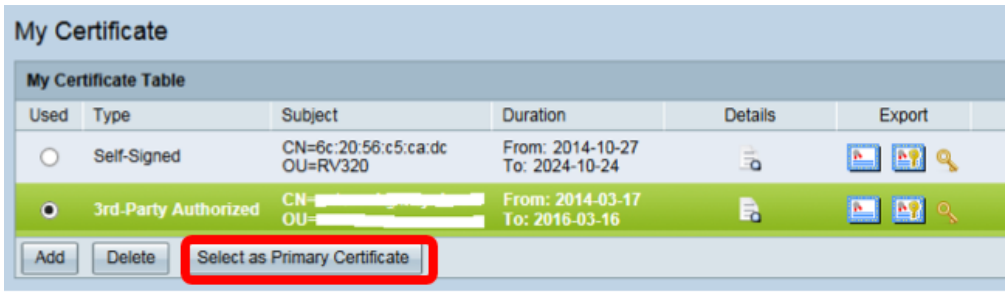
Note: Si vous exécutez le micrologiciel après la version 1.1.0.6, cliquez sur le bouton Choisir et localisez le fichier nécessaire.

Étape 7. Click **Save**.

Les certificats sont importés avec succès. Il peut désormais être utilisé pour l'accès HTTPS,

VPN SSL ou VPN IPSec.

Étape 8. (Facultatif) Pour utiliser le certificat pour HTTPS ou SSL VPN, cliquez sur la case d'option du certificat et cliquez sur le bouton **Sélectionner comme certificat principal**.

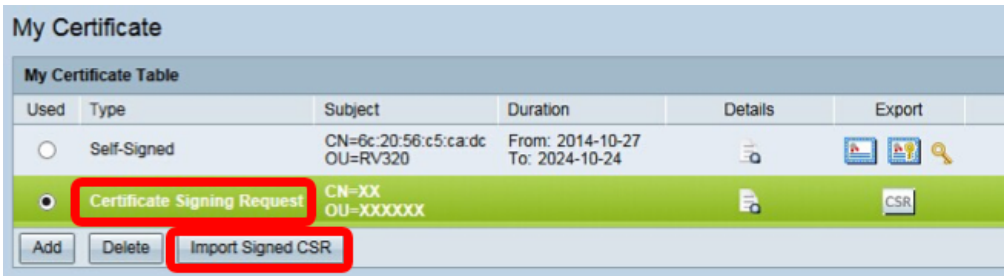


Vous devez avoir importé un certificat avec succès.

Signature de certificat à l'aide de CSR

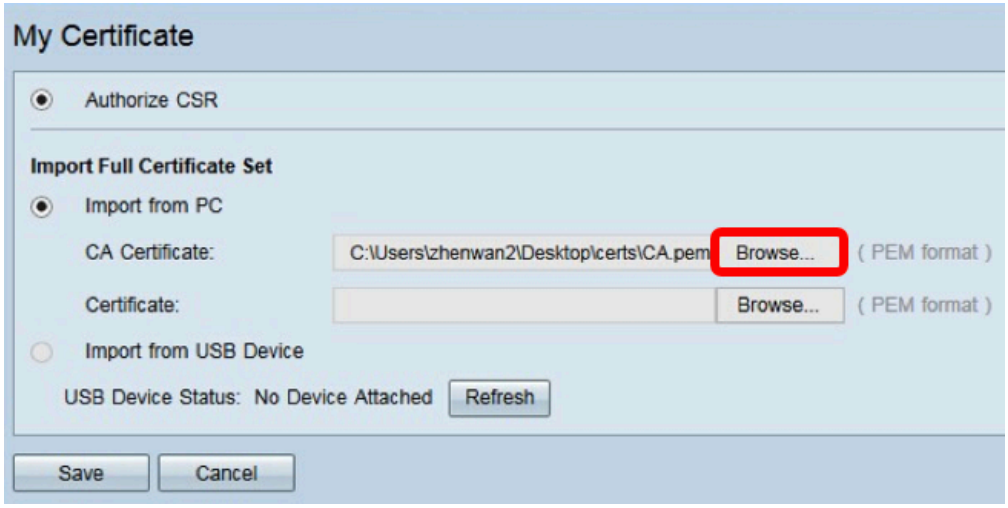
Étape 1. Générer une demande de signature de certificat (CSR) sur RV320/RV325. Pour savoir comment générer une CSR, cliquez ici.

Étape 2. Pour importer le certificat, sélectionnez **Demande de signature de certificat** et cliquez sur **Importer la CSR signée**.

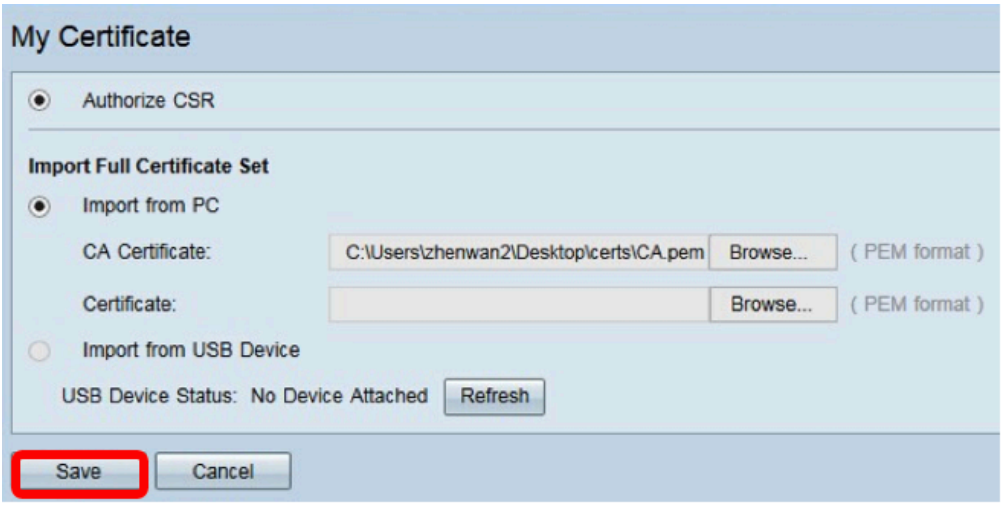


Étape 3. Cliquez sur **Parcourir...** et choisissez le fichier de certificat CA. Il contient le certificat CA racine + CA intermédiaire.

Note: Dans cet exemple, la clé privée n'est pas requise car le certificat est généré à l'aide de CSR.



Étape 4. Click **Save**.



Vous devez maintenant avoir téléchargé un certificat à l'aide du CSR.

Annexe::

Contenu de RV320.pem

Attributs du sac

localKeyID : 01 00 00 00

friendLiName : {{XXXXXXX-XXXX-XXXX-XXXX-XXXXXXX}}

Nom CSP Microsoft : Fournisseur de chiffrement Microsoft EnhNAced v1.0

Attributs clés

Utilisation de clé X509v3 : 10

—COMMENCER LA CLÉ PRIVÉE—

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—CLÉ PRIVÉE DE FIN—

Attributs du sac

localKeyID : 01 00 00 00

friendLiName : Certificat StartCom PFX

subject=/description=XXXX/C=US/ST=XXXX/L=Xxxxx/O=XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

émetteur=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signation/CN=StartCom Class 2 Primary Intermediate S4rver CA

—CERTIFICAT DE DÉBUT—

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY

.....

Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

—CERTIFICAT DE FIN—

Attributs du sac

friendLiName : Autorité de certification StartCom

subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signation/CN=StartCom Certification Authority

émetteur=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signation/CN=StartCom Certification Authority

—CERTIFICAT DE DÉBUT—

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=

—CERTIFICAT DE FIN—

Attributs du sac

subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signation/CN=StartCom Class 2 Primary Intermediate S4rver CA

émetteur=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signation/CN=StartCom Certification Authority

—CERTIFICAT DE DÉBUT—

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

—CERTIFICAT DE FIN—