

Configurer mon certificat sur les routeurs VPN RV320 et RV325

Objectif

Les certificats sont utilisés pour vérifier l'identité d'une personne ou d'un périphérique, authentifier un service ou chiffrer des fichiers. Sur le routeur RV320, vous pouvez ajouter un maximum de 50 certificats en signant automatiquement ou avec une autorisation de tiers. Vous pouvez exporter un certificat pour un client ou un administrateur et l'enregistrer sur un PC ou un périphérique USB, puis l'importer.

L'objectif de ce document est de vous montrer comment sélectionner un certificat principal, exporter un certificat et importer un certificat sur les routeurs VPN de la gamme RV32x.

Périphériques pertinents

Routeur VPN double WAN · RV320

Routeur VPN double WAN Gigabit · RV325

Version du logiciel

•v 1.1.0.09

Mon certificat

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Gestion des certificats > Mon certificat**. La page *Mon certificat* s'ouvre :



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Buttons: Add, Delete, Select as Primary Certificate

Il existe deux types de certificats :

·Auto-Signed : certificat SSL (Secure Socket Layer) signé par son propre créateur. Ce type est moins sécurisé car il ne peut pas être annulé si la clé privée est compromise par un pirate.

·demande de signature de certificat — 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 puisque la clé privée est gardée secrète.

Étape 2. Cliquez sur la case d'option souhaitée dans la *table Mon certificat* pour choisir un certificat.

Étape 3. Cliquez sur **Sélectionner comme certificat principal** pour faire du certificat sélectionné le certificat principal.

Étape 4. (Facultatif) Pour afficher des informations détaillées sur le certificat, cliquez sur l'icône **Détails**.

My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

La fenêtre *Détails du certificat* s'ouvre :

Certificate Details

Certificate Information

Version: 3
 Serial Number: D8 AF 62 26 26 36 5D D1

Subject Information

Subject: CN=6c:20:56:c6:16:52
 OU=RV320
 O=Cisco Systems, Inc.
 L=Irvine
 C=US
 ST=California

Public Key Algorithm: rsaEncryption -
 Subject Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63

Issuer Information

Issuer: CN=6c:20:56:c6:16:52
 OU=RV320
 O=Cisco Systems, Inc.
 L=Irvine
 C=US
 ST=California

Valid From: Apr 8 19:12:48 2013 GMT
 Valid Through: Apr 6 19:12:48 2023 GMT
 Signature Algorithm: sha1WithRSAEncryption
 Authority Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
 Fingerprint: 33 C4 E6 40 7D DD 1F 44 32 57 18 A9 AA D1 66 FB 5A B2 CD 36

[Close](#)

Étape 5. (Facultatif) Pour supprimer un certificat, cliquez sur la case d'option du certificat à supprimer, puis cliquez sur **Supprimer**.

Étape 6. Cliquez sur **Save pour enregistrer les paramètres**.

Exporter un certificat auto-signé

Étape 1. Cliquez sur le bouton d'icône souhaité dans la colonne *Exporter* pour exporter un certificat auto-signé.

My Certificate

My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

[Add](#) [Delete](#) [Select as Primary Certificate](#)

Les boutons d'icône disponibles sont définis comme suit :

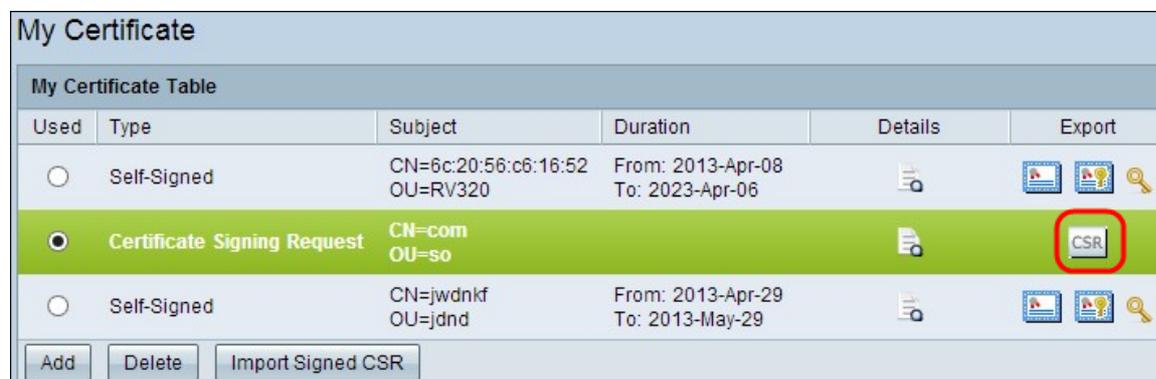
- Export Certificate for Client : exporte un certificat client utilisé pour connecter le client au réseau privé virtuel (VPN).
- Export Certificate for Administrator : exporte un certificat administrateur. Une clé privée est générée et une copie est conservée pour sauvegarde.
- Export Private Key : exporte une clé privée pour le logiciel client VPN, qui nécessite des informations d'identification distinctes pour une connexion VPN.

Étape 2. Cliquez sur **Ouvrir** pour afficher la clé.

Étape 3. Cliquez sur **Enregistrer** pour enregistrer la clé.

Exporter une demande de signature de certificat

Étape 1. Cliquez sur **CSR** (Export Certificate Signing Request).



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Étape 2. Cliquez sur **Ouvrir** pour afficher.

Étape 3. Cliquez sur **Save** pour enregistrer la clé sur votre ordinateur ou USB.

Importer un certificat

Étape 1. Cliquez sur **Ajouter** pour importer un certificat.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

La fenêtre suivante s'affiche :

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: No file chosen (PEM format)

Certificate + Private Key: No file chosen (PEM format)

Import from USB Device

USB Device Status: No Device Attached

Étape 2. Cliquez sur la case d'option souhaitée pour définir le type de certificat que vous importez.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: No file chosen (PEM format)

Certificate + Private Key: No file chosen (PEM format)

Import from USB Device

USB Device Status: No Device Attached

· tierce partie autorisée - une infrastructure à clé publique (PKI) dans laquelle l'autorité de certification fournit la signature numérique.

· Auto-Signed : certificat SSL (Secure Socket Layer) signé par son propre créateur.

Étape 3. Cliquez sur la case d'option souhaitée pour choisir le mode d'importation du certificat.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC
 CA Certificate: No file chosen (PEM format)
 Certificate + Private Key: No file chosen (PEM format)
 Import from USB Device

· Importer à partir du PC : le certificat est importé à partir du PC sur lequel vous l'avez enregistré.

· Import from USB : le certificat est importé à partir de votre lecteur USB.

Importer le certificat à partir du PC

Étape 1. Si vous importez un certificat agréé tiers, cliquez sur **Choisir un fichier** en regard de *certificat CA* pour rechercher l'emplacement du fichier et le sélectionner.

Étape 2. Cliquez sur **Choose File** en regard de *Certificate + Private Key* pour rechercher l'emplacement du fichier et le sélectionner.

Étape 3. Cliquez sur **Save pour enregistrer les paramètres**. Le certificat importé apparaît dans la *table Mon certificat*.

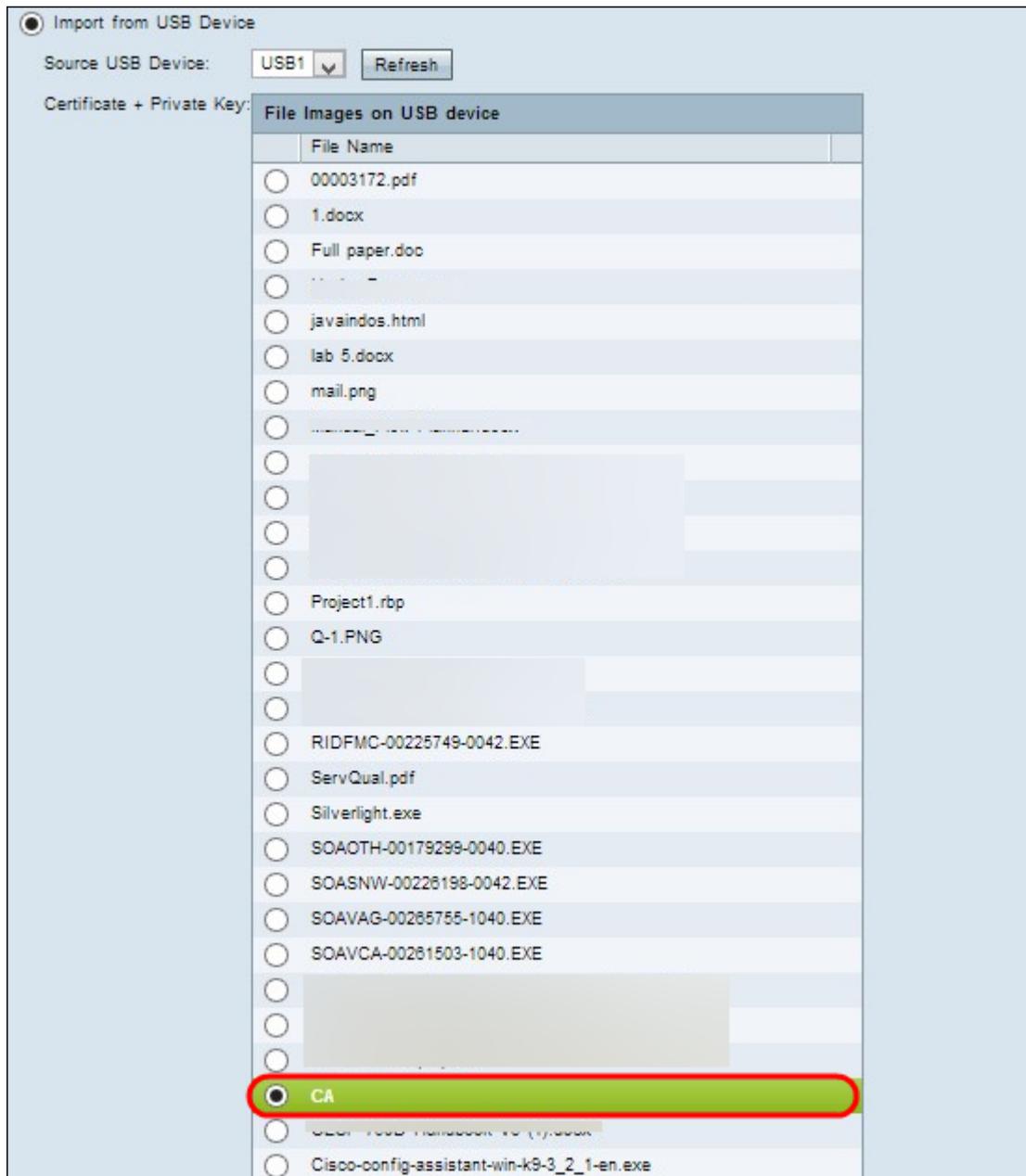
My Certificate

My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		
<input type="radio"/>	Self-Signed	CN= OU=			

Importer le certificat à partir d'USB

Étape 1. Choisissez le périphérique USB approprié dans la liste déroulante *Périphérique USB source*.



Étape 2. Si vous importez un certificat agréé tiers, cliquez sur la case d'option appropriée pour importer le certificat CA que vous avez enregistré sur votre USB.

Étape 3. Sélectionnez la case d'option appropriée pour importer le certificat + clé privée que vous avez enregistré sur votre USB.

Étape 4. Cliquez sur Save pour enregistrer les paramètres. Le certificat importé apparaît dans la *table Mon certificat*.

My Certificate

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		  
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		  
<input type="radio"/>	Self-Signed	CN= OU=			  