Gérer les certificats sur FindIT Network Manager

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. Lors de l'installation, FindIT Network Manager génère un certificat auto-signé pour sécuriser les communications Web et autres avec le serveur. Vous pouvez choisir de remplacer ce certificat par celui signé par une autorité de certification (CA) de confiance. Pour ce faire, vous devez générer une demande de signature de certificat (CSR) pour la signature par l'autorité de certification.

Vous pouvez également choisir de générer un certificat et la clé privée correspondante complètement indépendante du gestionnaire. Si c'est le cas, vous pouvez combiner le certificat et la clé privée dans un fichier au format PKCS (Public Key Cryptography Standards) n° 12 avant le téléchargement.

FindIT Network Manager ne prend en charge que les certificats au format .pem. Si vous obtenez d'autres formats de certificat, vous devez convertir à nouveau le format ou la demande du certificat au format .pem à partir de l'autorité de certification.

Cet article explique comment gérer les certificats sur FindIT Network Manager.

Périphériques pertinents

- FindIT Network Manager

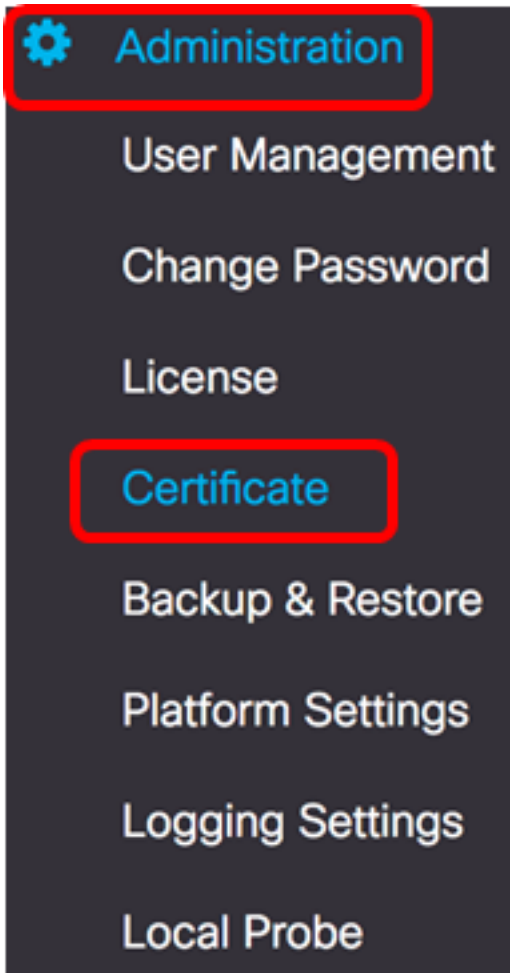
Version du logiciel

- 1.1

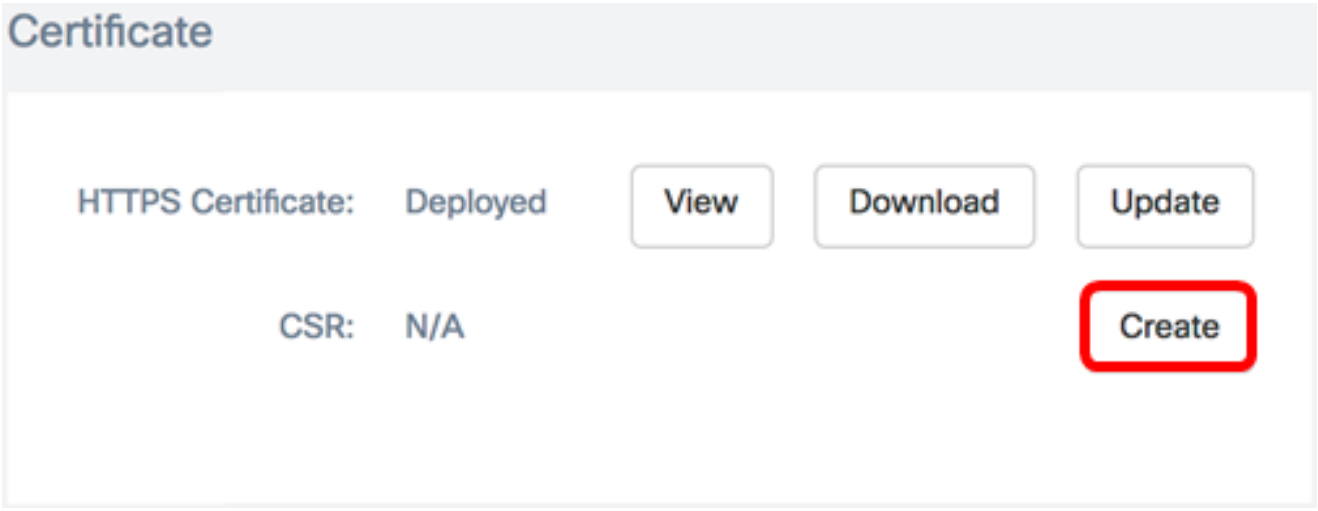
Gérer les certificats sur FindIT Network Manager

Générer une requête de signature de certificat (CSR)

Étape 1. Connectez-vous à l'interface utilisateur d'administration de FindIT Network Manager, puis sélectionnez **Administration > Certificate**.



Étape 2. Dans la zone CSR, cliquez sur le bouton **Créer**.



Les valeurs entrées dans le formulaire de certificat seront utilisées pour construire le CSR et seront contenues dans le certificat signé que vous recevez de l'AC.

Étape 3. Entrez l'adresse IP ou le nom de domaine dans le champ *Nom de domaine complet qualifié*. Dans cet exemple, hostname.cisco.com est utilisé.

Étape 4. Entrez le code pays dans le champ *Pays*. Dans cet exemple, US est utilisé.

Étape 5. Entrez le code d'état dans le champ *État*. Dans cet exemple, l'autorité de certification est utilisée.

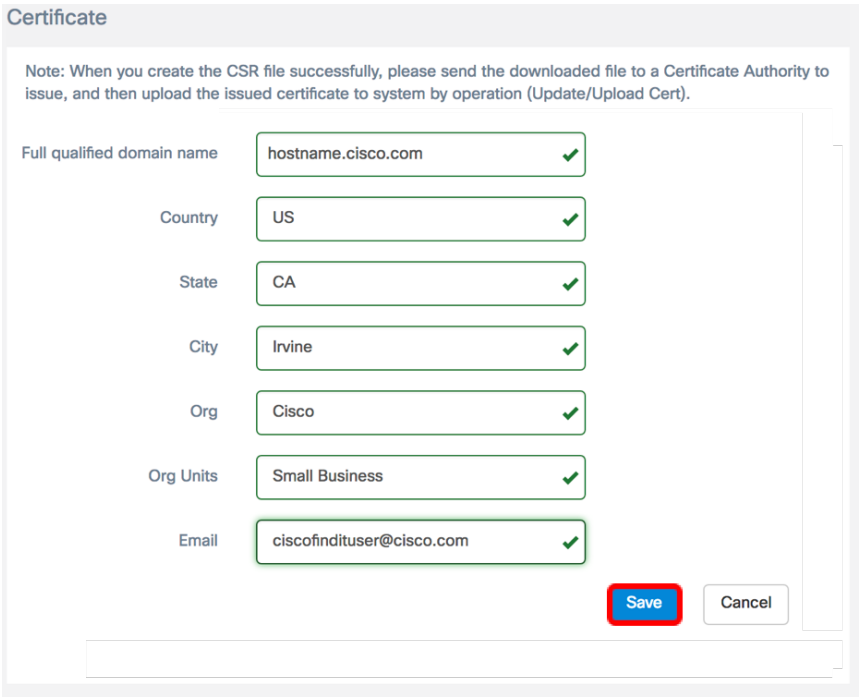
Étape 6. Entrez la ville dans le champ *Ville*. Dans cet exemple, Irvine est utilisé.

Étape 7. Entrez le nom de l'organisation dans le champ *Organisation*. Dans cet exemple, Cisco est utilisé.

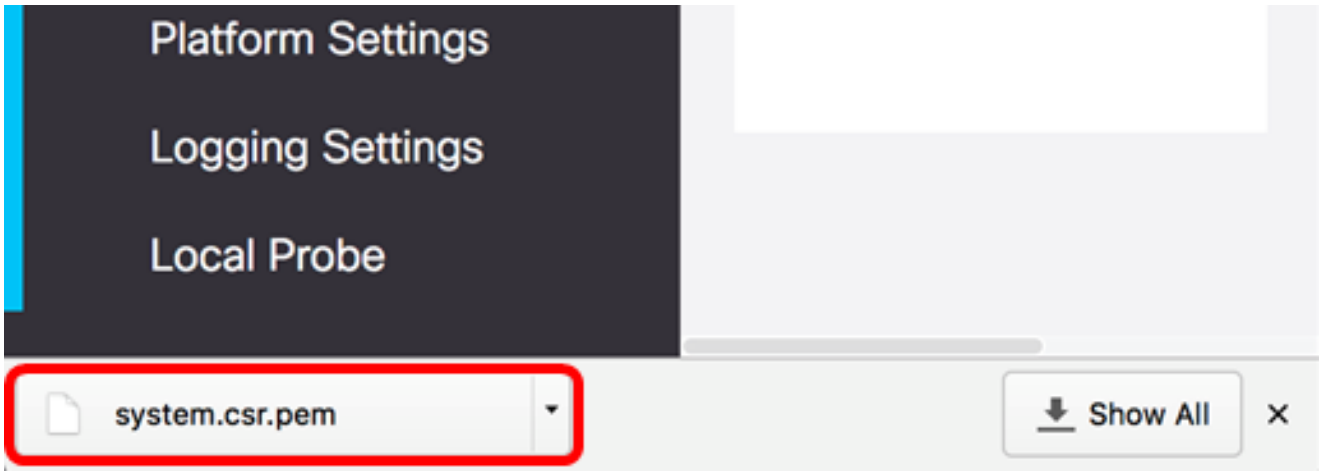
Étape 8. Entrez les unités d'organisation dans le champ *Unités d'organisation*. Dans cet exemple, Small Business est utilisé.

Étape 9. Saisissez votre adresse e-mail dans le champ *E-mail*. Dans cet exemple, ciscofinduser@cisco.com est entré.

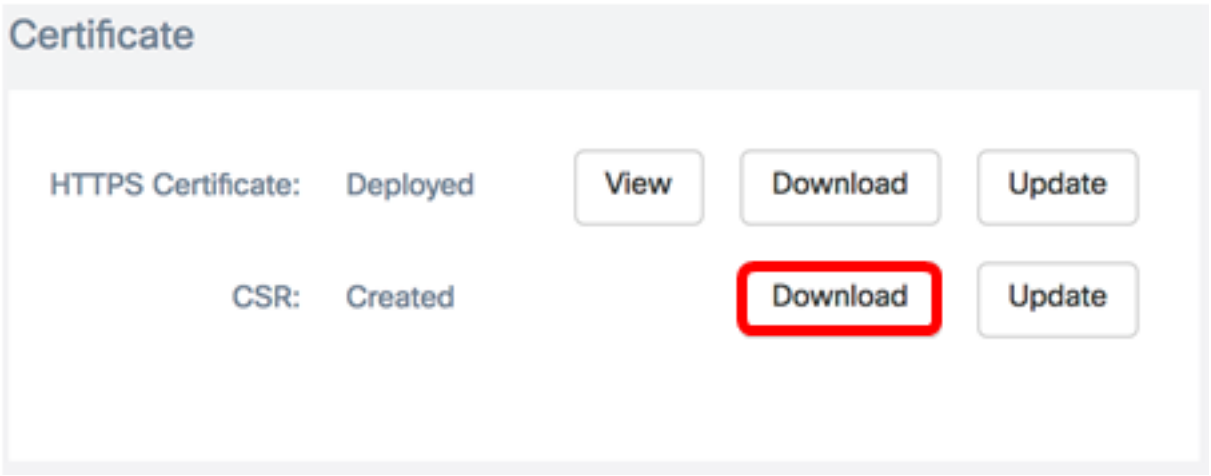
Étape 10. Click **Save**.



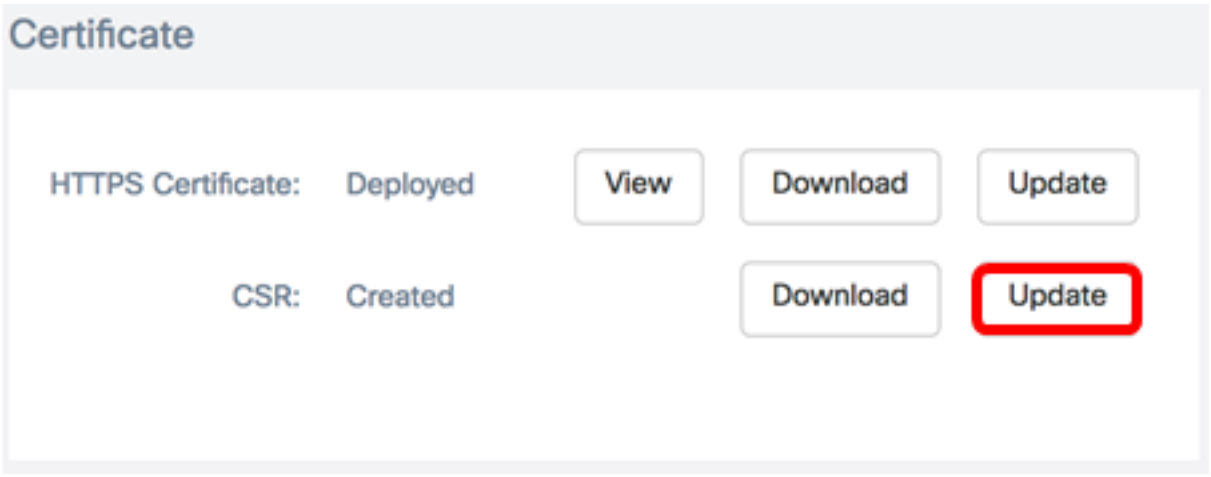
Le fichier CSR sera automatiquement téléchargé sur votre ordinateur. Dans cet exemple, le fichier system.csr.pem est généré.



Étape 11. (Facultatif) Dans la zone CSR, l'état sera mis à jour de N/A à Créé. Pour télécharger le CSR créé, cliquez sur le bouton **Télécharger**.



Étape 12. (Facultatif) Pour mettre à jour le CSR créé, cliquez sur le bouton **Mettre à jour**, puis revenez à l'étape 3.

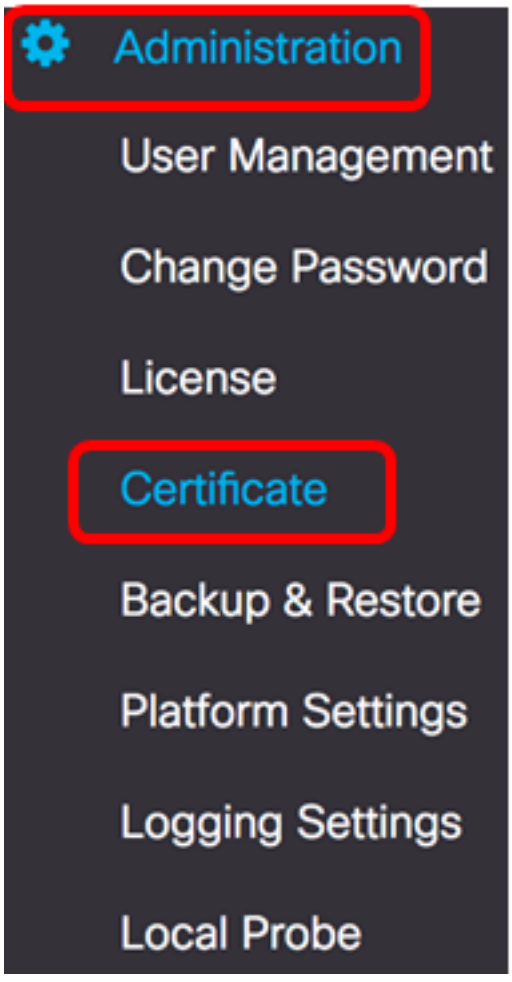


Vous devez maintenant avoir généré une demande de service de contact sur votre FindIT Network Manager. Vous pouvez maintenant envoyer le fichier CSR téléchargé à l'autorité de certification.

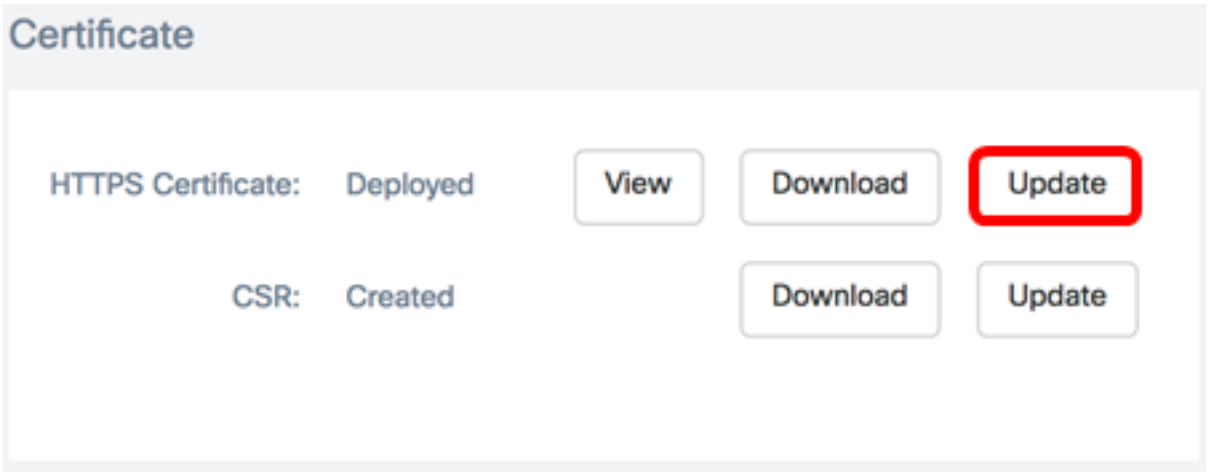
Télécharger un certificat signé de l'autorité de certification

Une fois que vous avez reçu le CSR signé de la CA, vous pouvez le télécharger vers le gestionnaire.

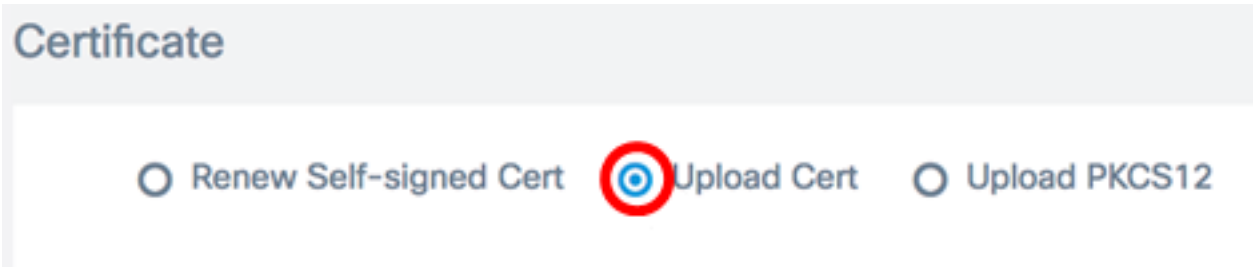
Étape 1. Connectez-vous à l'interface utilisateur d'administration de FindIT Network Manager, puis sélectionnez **Administration > Certificate**.



Étape 2. Dans la zone HTTPS Certificate, cliquez sur le bouton **Update**.

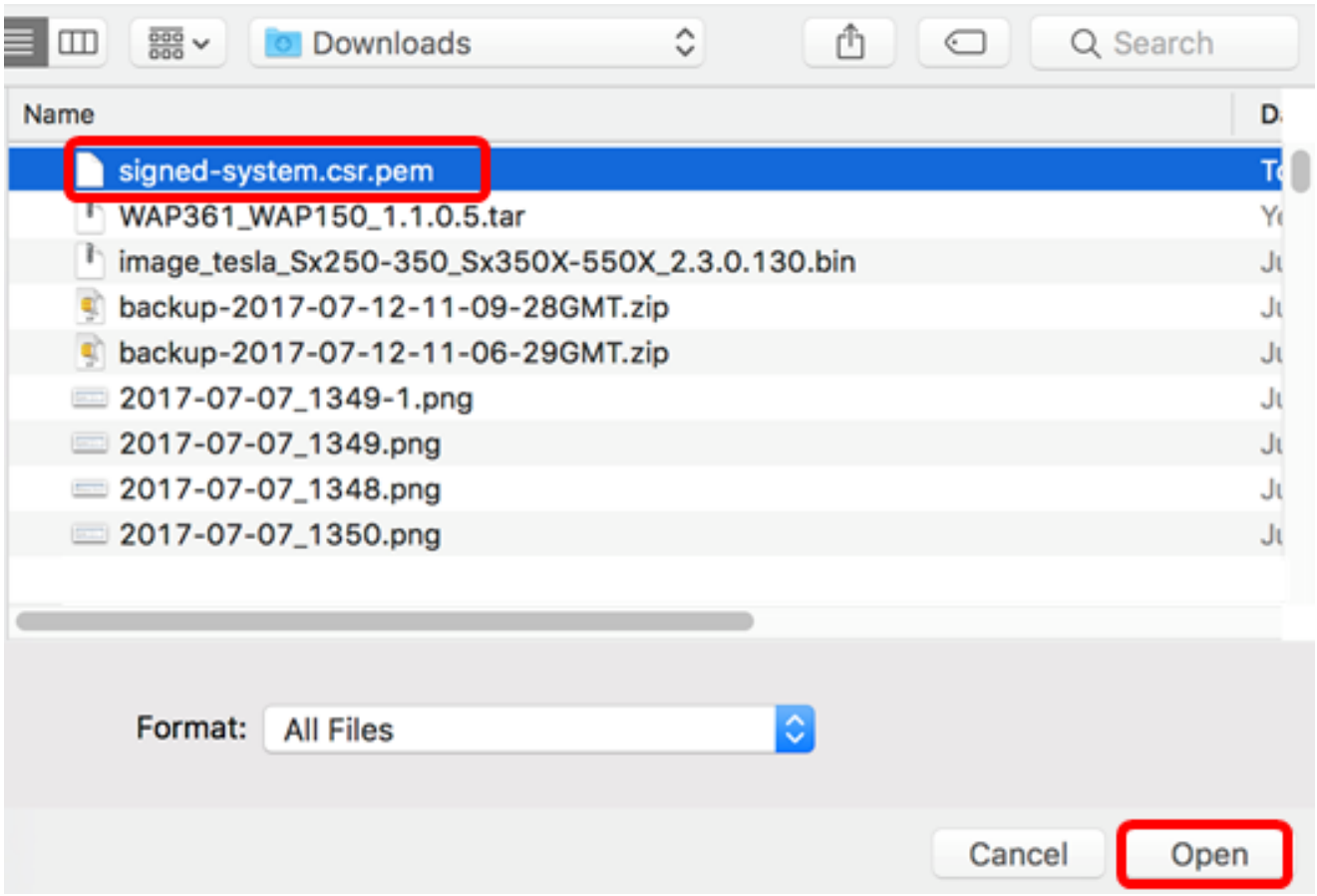


Étape 3. Cliquez sur la case d'option **UploadCert**.



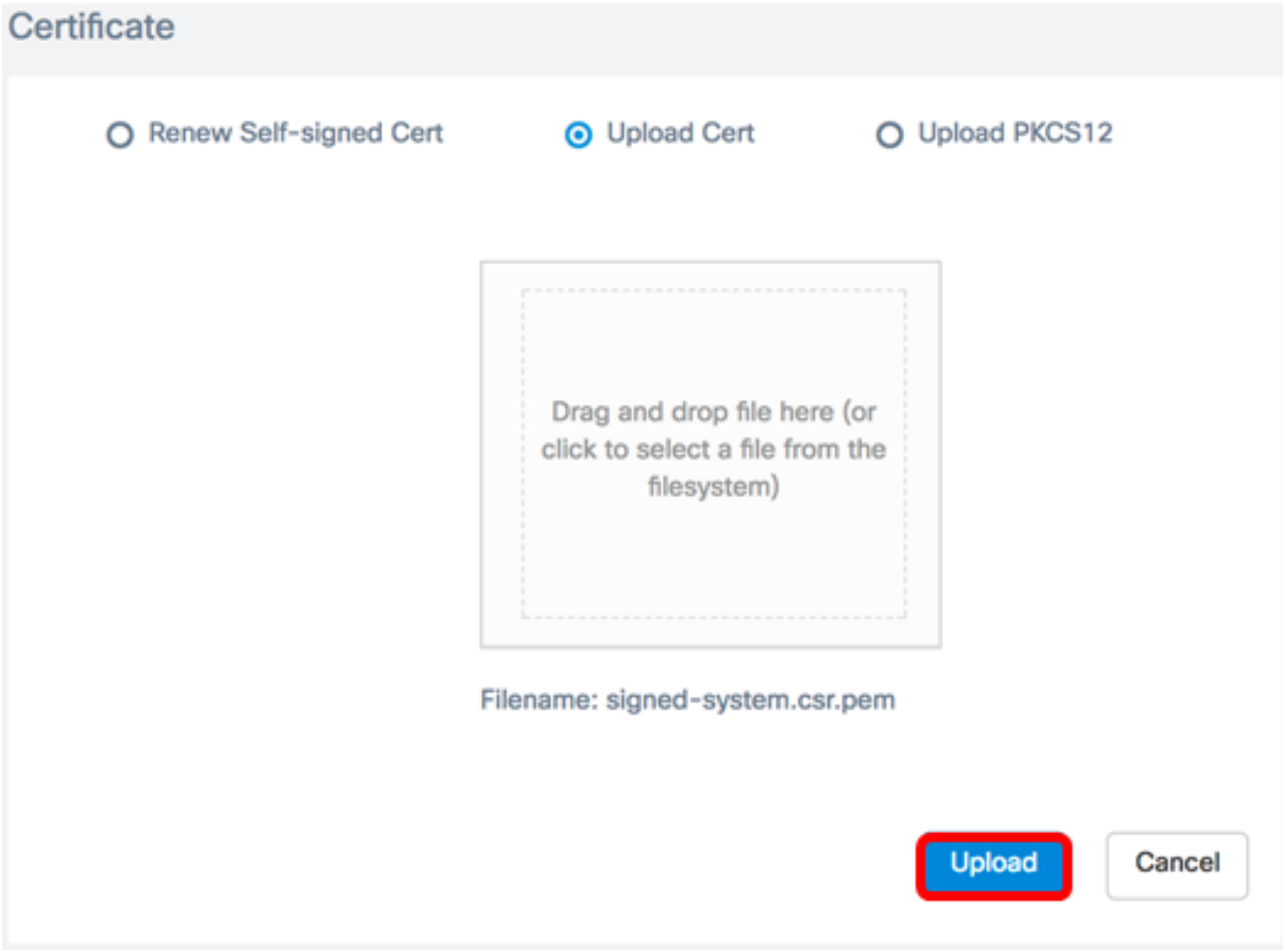
Note: Vous pouvez également télécharger un certificat avec la clé privée associée au format PKCS#12 en sélectionnant la case d'option **Upload PKCS12**. Le mot de passe pour déverrouiller le fichier doit être spécifié dans le champ *Mot de passe* fourni.

Étape 4. Supprimez le certificat signé dans la zone cible ou cliquez sur la zone cible pour parcourir le système de fichiers, puis cliquez sur **Ouvrir**. Le fichier doit être au format .pem.



Note: Dans cet exemple, signed-system.csr.pem est utilisé.

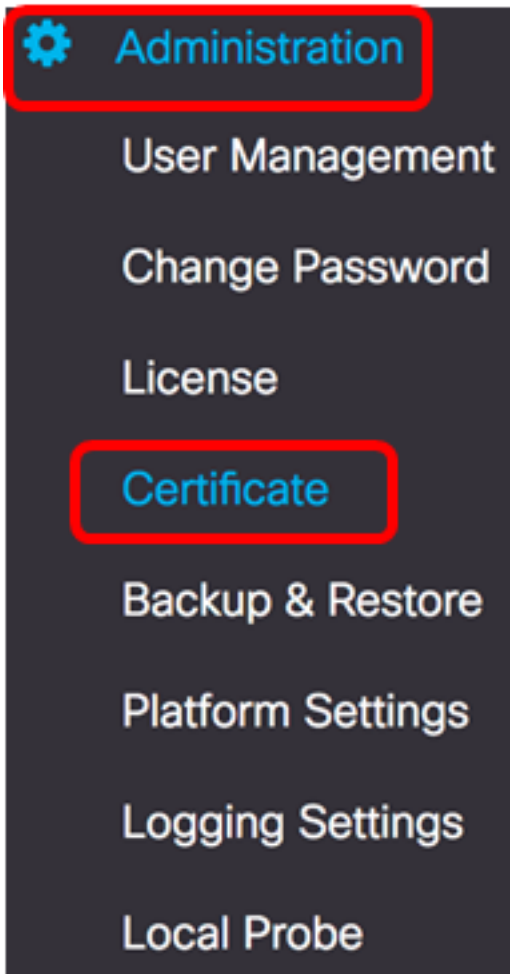
Étape 5. Cliquez sur **Upload** (charger).



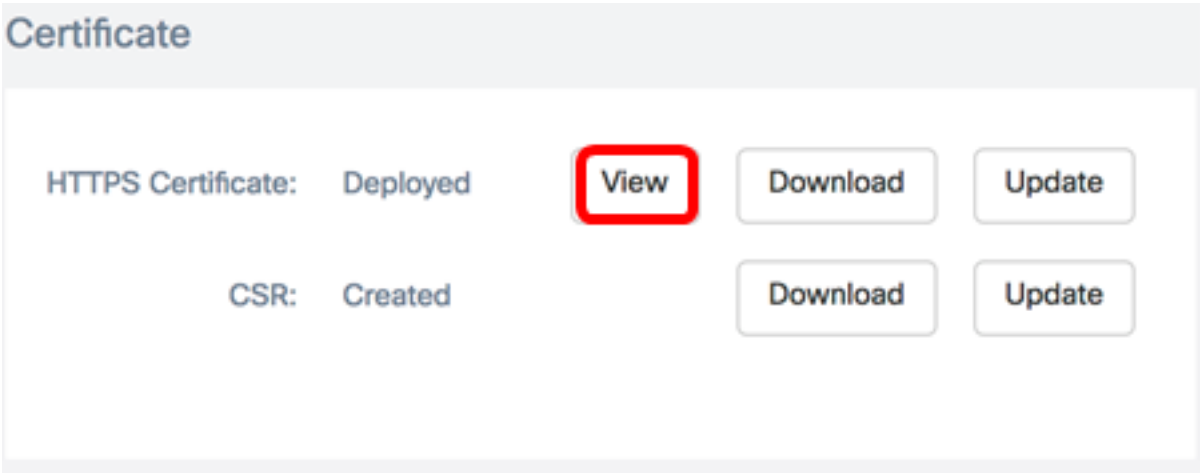
Vous devez maintenant avoir téléchargé un certificat signé dans FindIT Network Manager.

Gérer le certificat actuel

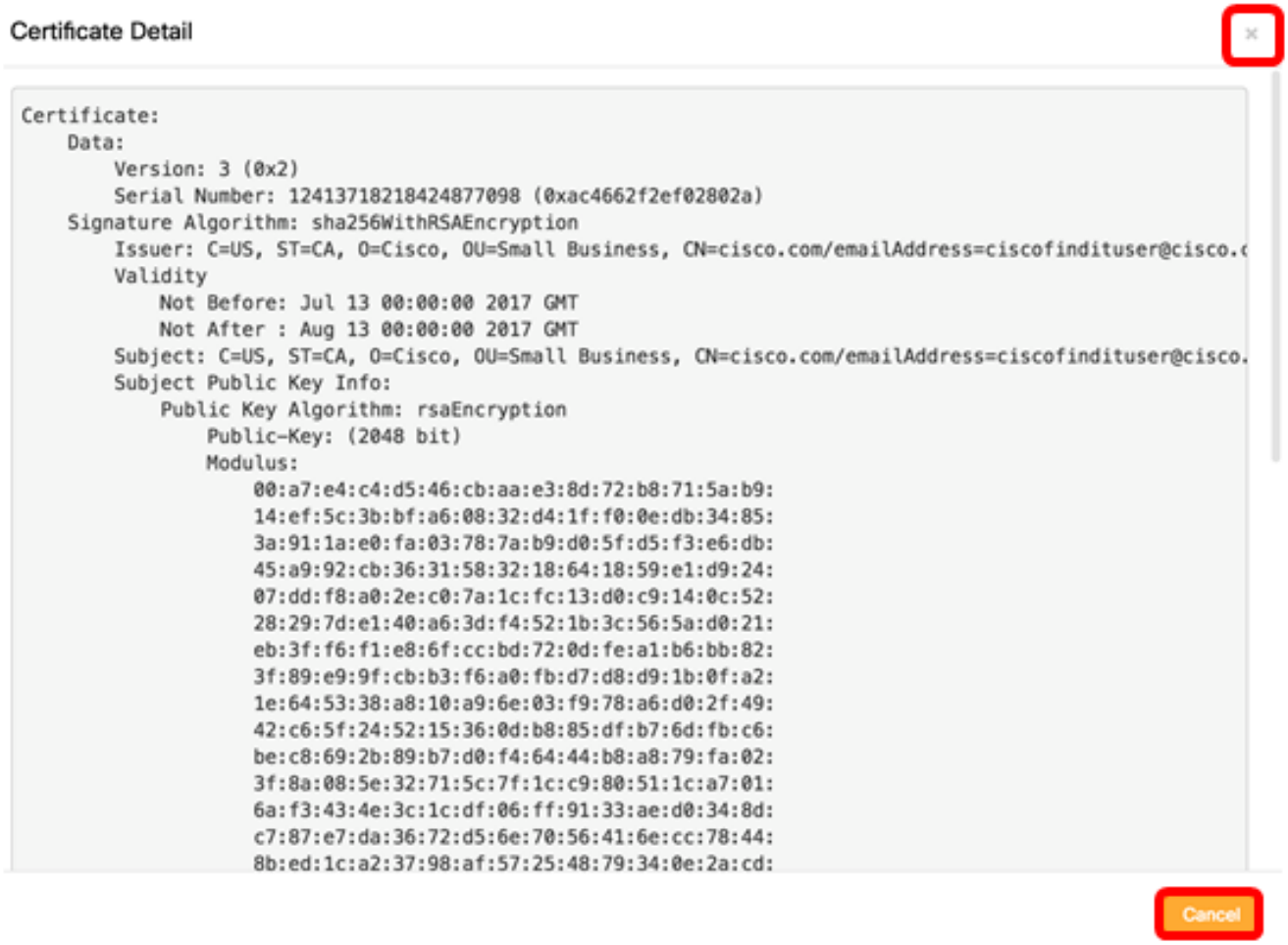
Étape 1. Connectez-vous à l'interface utilisateur d'administration de FindIT Network Manager, puis sélectionnez **Administration > Certificate**.



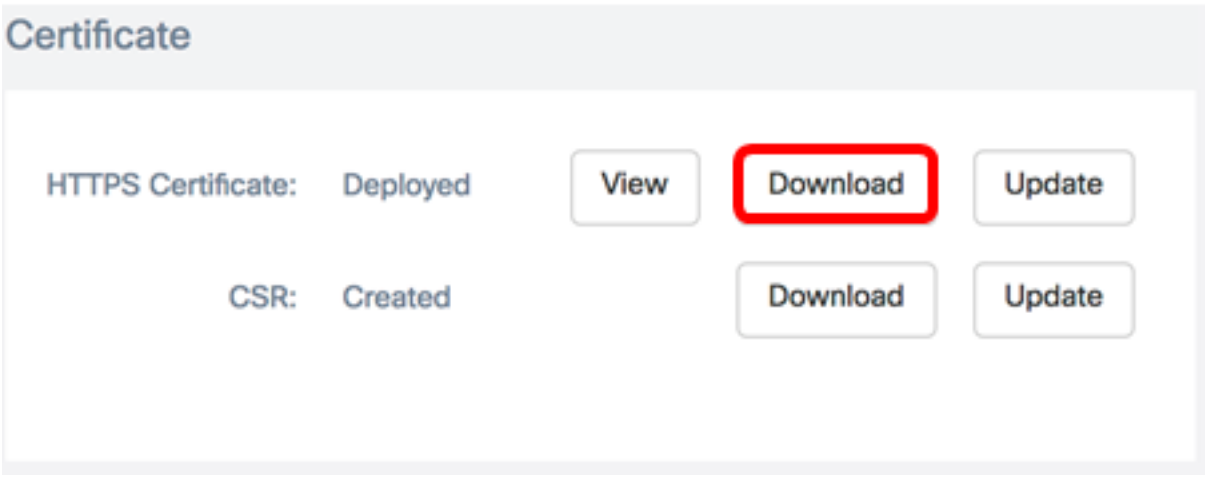
Étape 2. Dans la zone HTTPS Certificate, cliquez sur le bouton **View**.



Étape 3. Le certificat actuel s'affiche en texte brut dans une nouvelle fenêtre de navigateur. Cliquez sur le bouton **x** ou **Cancel** pour fermer la fenêtre.



Étape 4. (Facultatif) Pour télécharger une copie du certificat actuel, cliquez sur le bouton **Télécharger** dans la zone Certificat HTTPS.



Vous devez maintenant avoir géré correctement le certificat actuel sur votre FindIT Network Manager.