Certificaten beheren op FindIT Network Manager

Doel

Een digitaal certificaat certificeert de eigendom van een openbare sleutel door het genoemde onderwerp van het certificaat. Dit stelt betrouwbare partijen in staat om afhankelijk te zijn van handtekeningen of beweringen van de privé-sleutel die overeenkomt met de openbare sleutel die gecertificeerd is. Na de installatie genereert de FindIT Network Manager een zichzelf ondertekend certificaat om web en andere communicatie met de server te beveiligen. U kunt ervoor kiezen dit certificaat te vervangen door het certificaat dat is ondertekend door een vertrouwde certificeringsinstantie (CA). Om dit te doen, zult u een certificaat het ondertekenen verzoek (CSR) moeten genereren voor het ondertekenen door CA.

U kunt ook ervoor kiezen om een certificaat en de bijbehorende privé-toets, volledig onafhankelijk van de Manager, te genereren. Als dat zo is, kunt u het certificaat en de privé-toets voor het uploaden combineren tot een PKCS (Public Key Cryptography Standards) #12.

De FindIT Network Manager ondersteunt alleen .pem-certificaten. Als u andere certificaatformaten krijgt, moet u het formaat of het verzoek om het .pem-formaat certificaat opnieuw converteren vanuit de CA.

Dit artikel bevat instructies hoe u certificaten op FindIT Network Manager kunt beheren.

Toepasselijke apparaten

- FindIT-netwerkbeheer

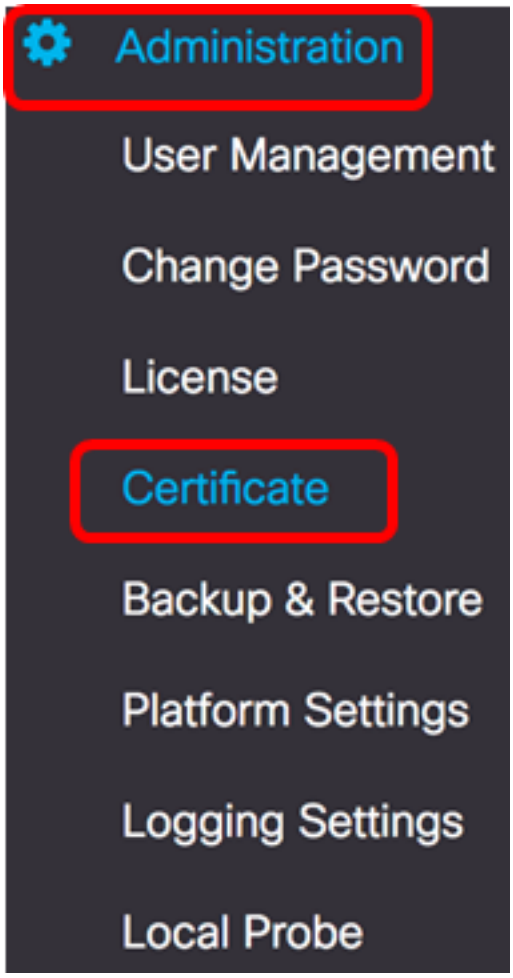
Softwareversie

- 1.1

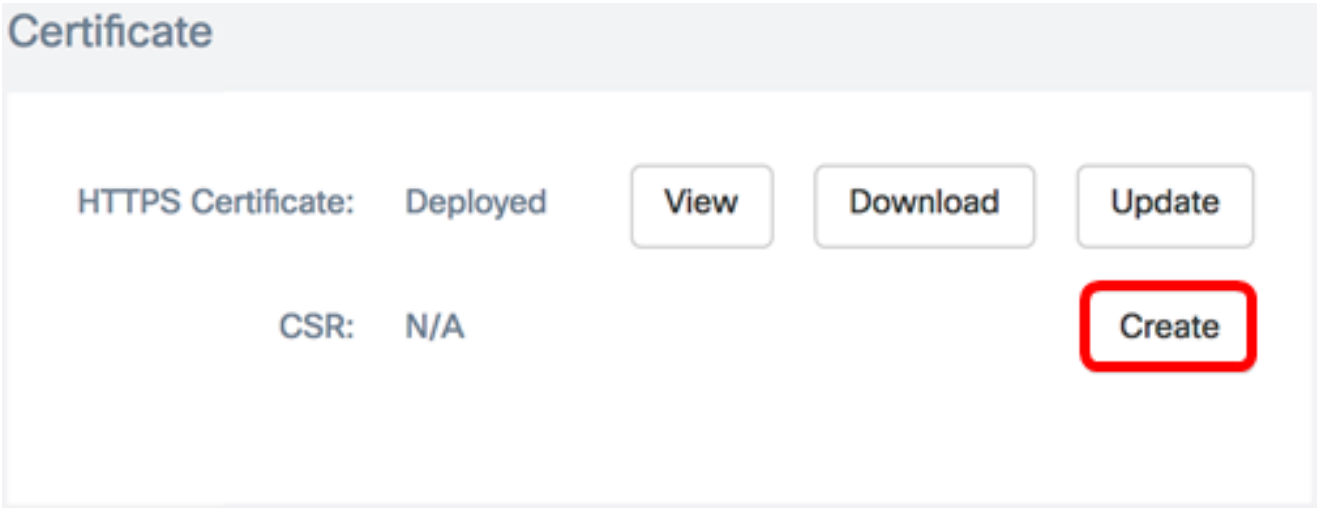
Certificaten beheren op FindIT Network Manager

Een CSR genereren

Stap 1. Meld u aan bij de Administration GUI van uw FindIT Network Manager en kies vervolgens **Administratie > Certificaat**.



Stap 2. Klik in het CSR-gebied op de knop **Maken**.



De waarden die in het certificaatformulier zijn ingevoerd, worden gebruikt om de CSR te construeren, en zullen vervat zijn in het ondertekende certificaat dat u van de CA ontvangt.

Stap 3. Voer het IP-adres of de domeinnaam in het veld *Volledig gekwalificeerde domeinnaam in*. In dit voorbeeld wordt hostname.cisco.com gebruikt.

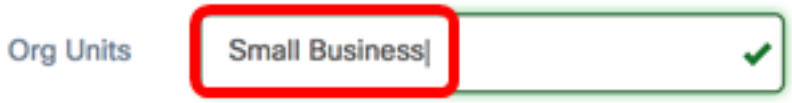
Stap 4. Voer de landencode in het veld *Land*. In dit voorbeeld worden de VS gebruikt.

Stap 5. Voer de staatscode in het veld *Staat in*. In dit voorbeeld wordt CA gebruikt.

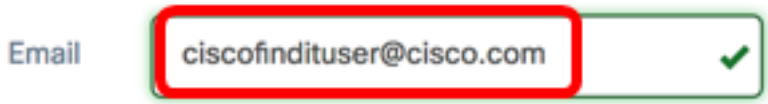
Stap 6. Voer de stad in het veld *Stad in*. In dit voorbeeld wordt Irvine gebruikt.

Stap 7. Voer de organisatienaam in het veld *Org in*. In dit voorbeeld wordt Cisco gebruikt.

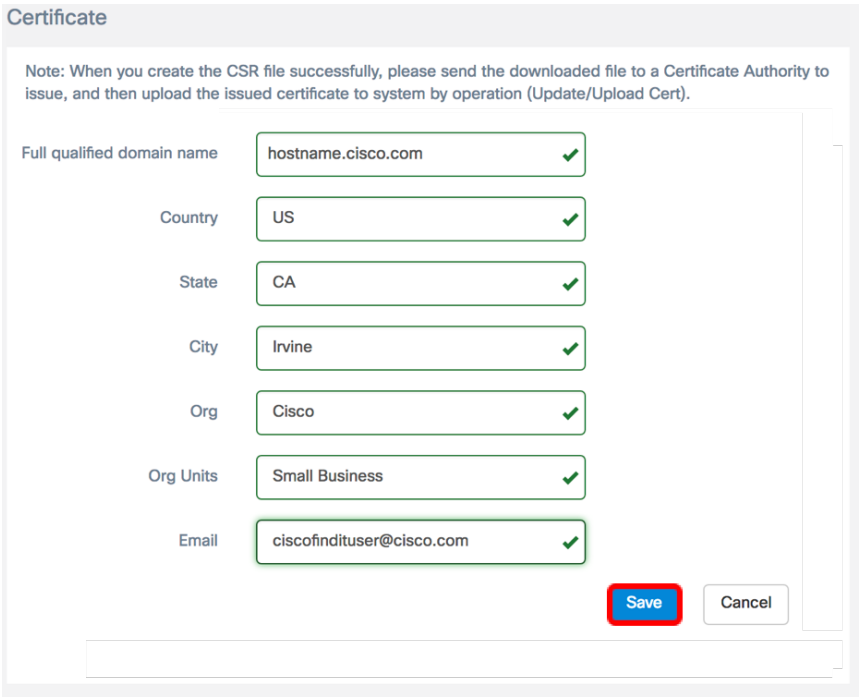
Stap 8. Voer de eenheden van de organisatie in het veld *Org Units in*. In dit voorbeeld wordt het MKB gebruikt.



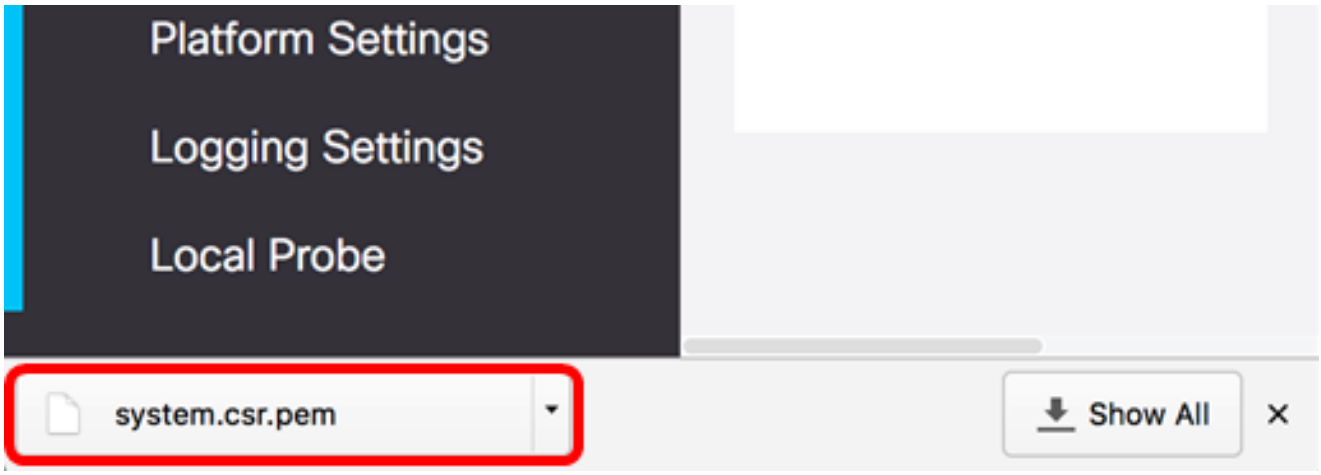
Stap 9. Voer uw e-mailadres in het veld *E-mail*. In dit voorbeeld wordt ciscofinduser@cisco.com ingevoerd.



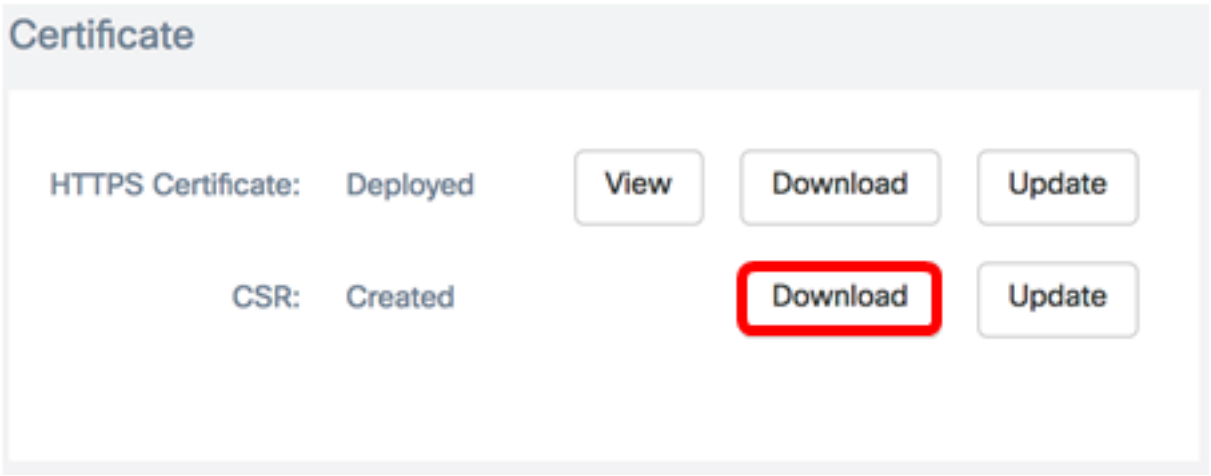
Stap 10. Klik op **Opslaan**.



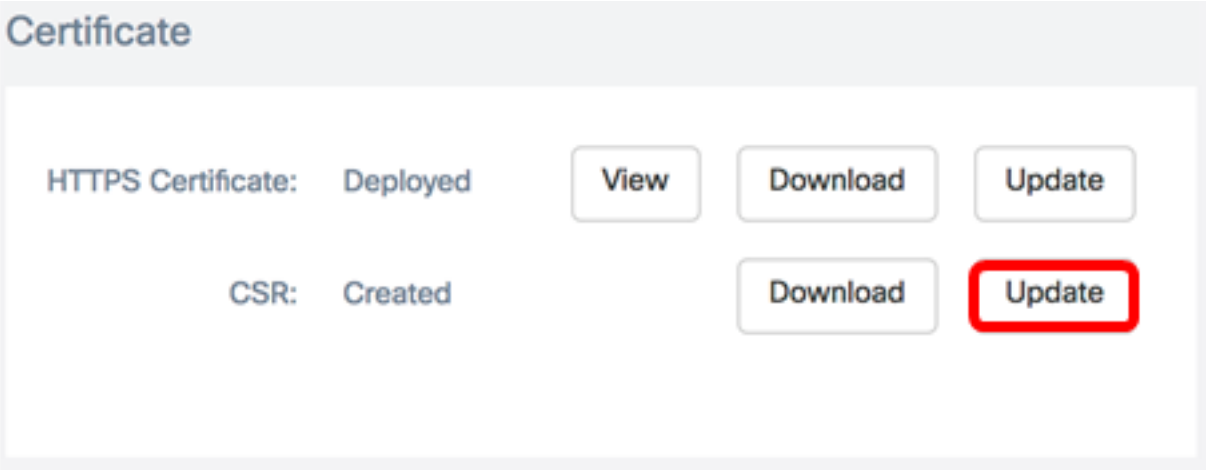
Het CSR-bestand wordt automatisch naar uw computer gedownload. In dit voorbeeld wordt het bestand system.csr.pem gegenereerd.



Stap 11. (Optioneel) In het CSR-gebied wordt de status bijgewerkt vanaf N/A naar gemaakt. Klik op de knop **Downloaden** om de gemaakte CSR te downloaden.



Stap 12. (Optioneel) Klik om de gemaakte CSR bij te werken op de knop **Update** en ga vervolgens terug naar Stap 3.

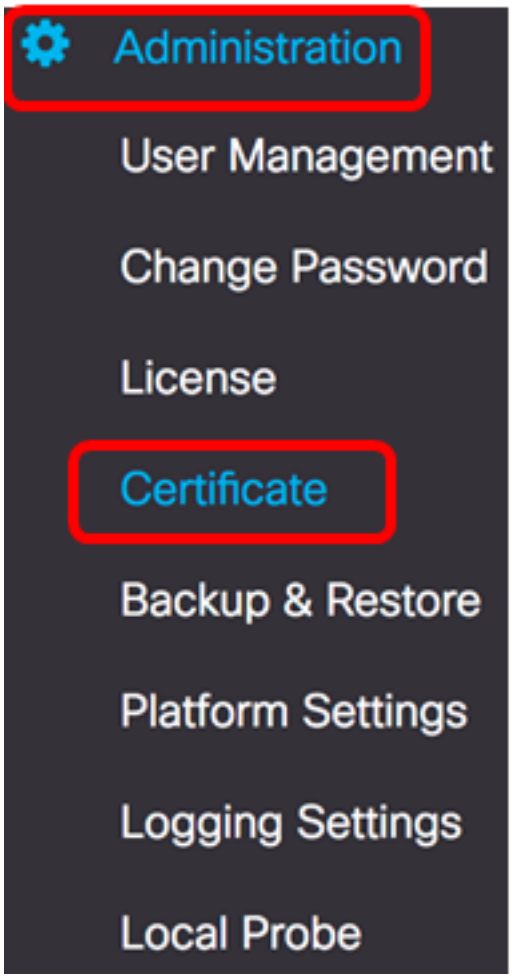


U hebt nu een CSR-bestand gegenereerd op uw FindIT-netwerkbeheer. U kunt het gedownload CSR-bestand nu naar de CA sturen.

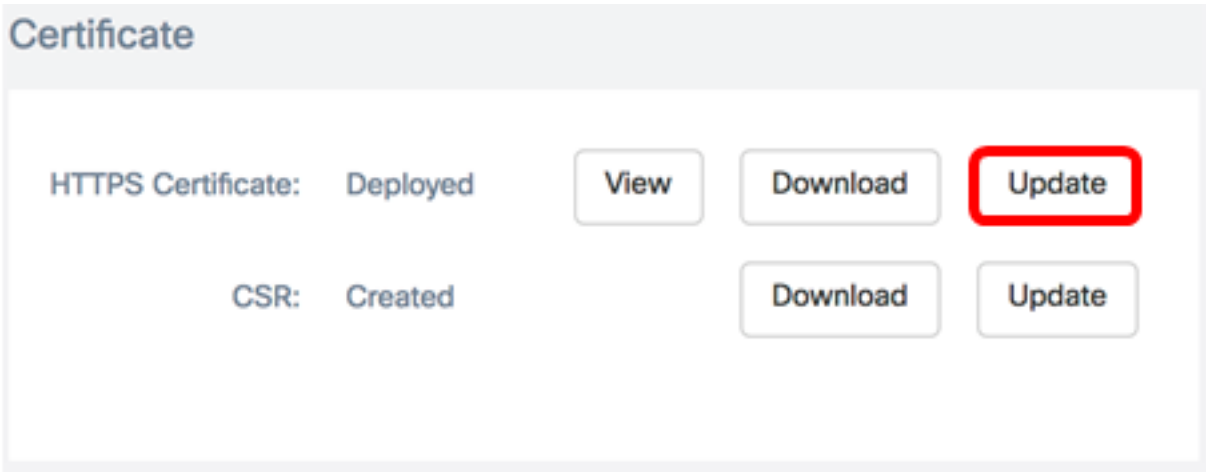
Een ondertekend certificaat vanuit de CA uploaden

Nadat u de ondertekende CSR van CA hebt ontvangen, kunt u deze nu uploaden naar de Manager.

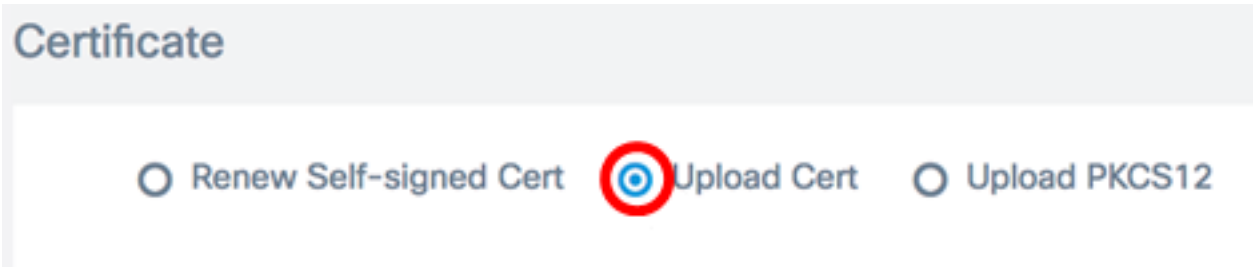
Stap 1. Meld u aan bij de Administration GUI van uw FindIT Network Manager en kies vervolgens **Administratie > Certificaat**.



Stap 2. Klik in het gebied HTTPS-certificaat op de knop **Update**.

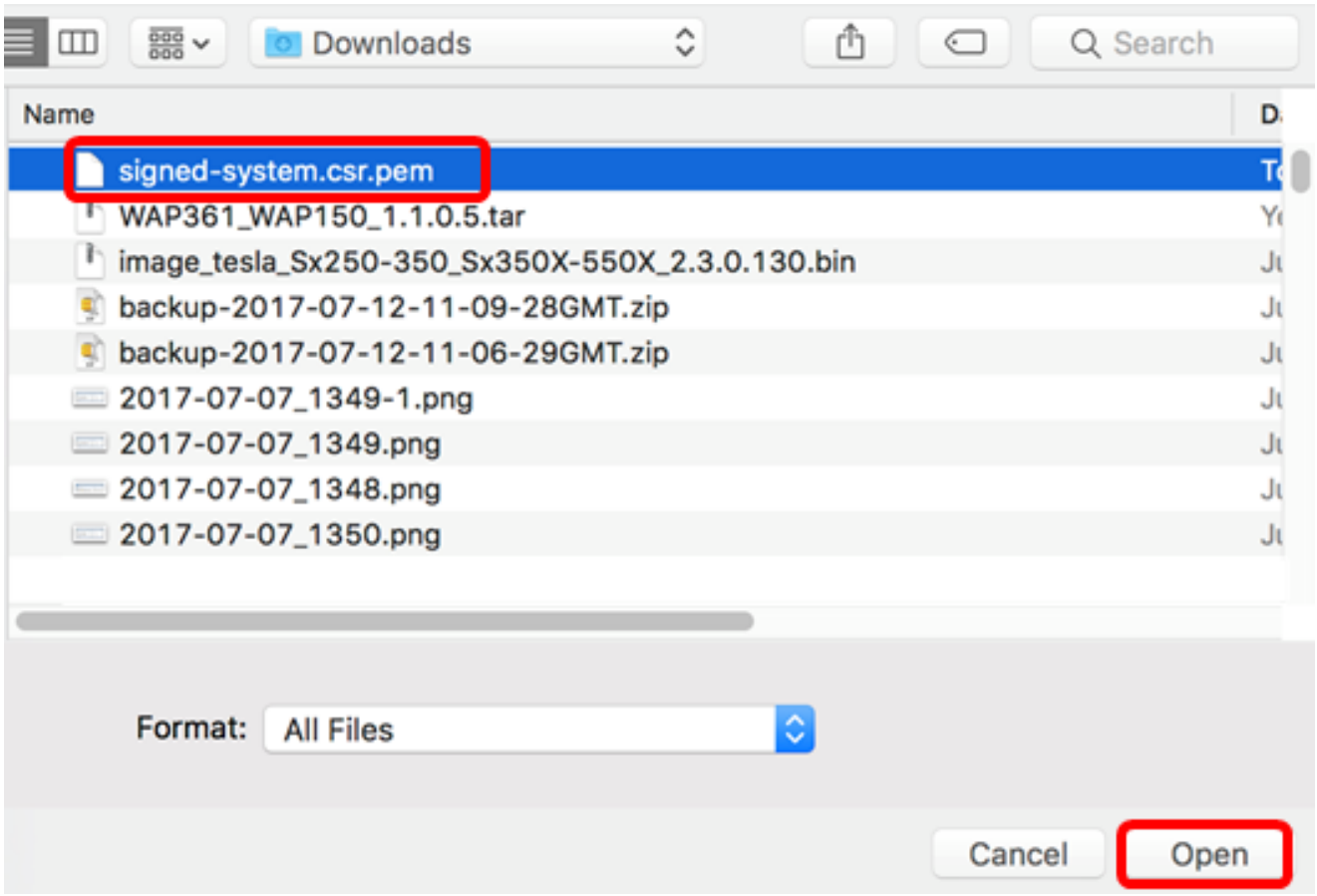


Stap 3. Klik op de radioknop **UploadCert**.



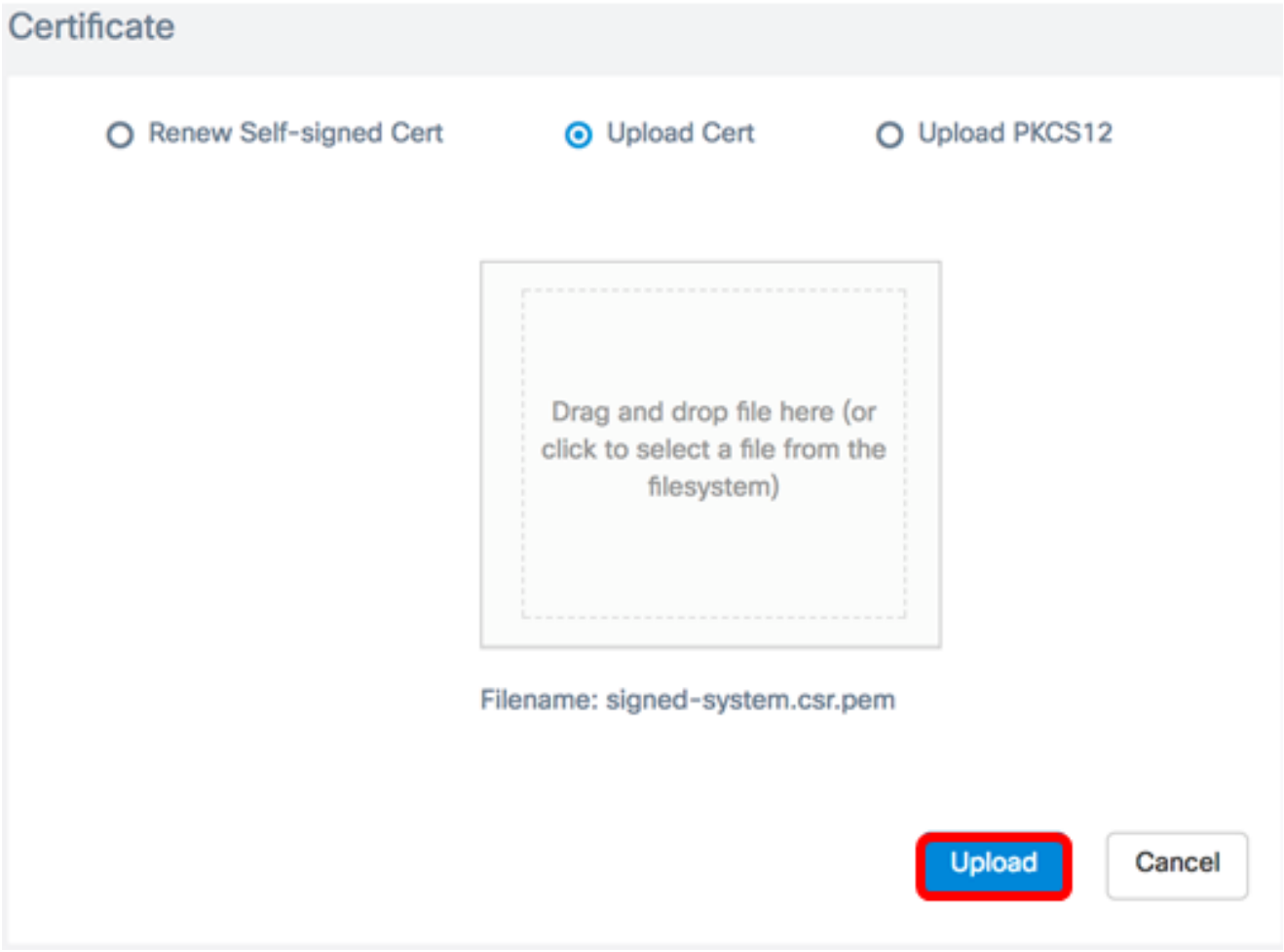
Opmerking: U kunt ook een certificaat met de bijbehorende privé-toets in het PKCS#12-formaat uploaden door de radioknop **Upload PKCS12** te kiezen. Het wachtwoord om het bestand te ontgrendelen, dient in het veld *Wachtwoord* te worden gespecificeerd.

Stap 4. Laat het ondertekende certificaat op het doelgebied vallen of klik op het doelgebied om door het bestandssysteem te bladeren en klik vervolgens op **Openen**. Het bestand moet in .pem-formaat zijn.



Opmerking: In dit voorbeeld wordt getekend-system.csr.pem gebruikt.

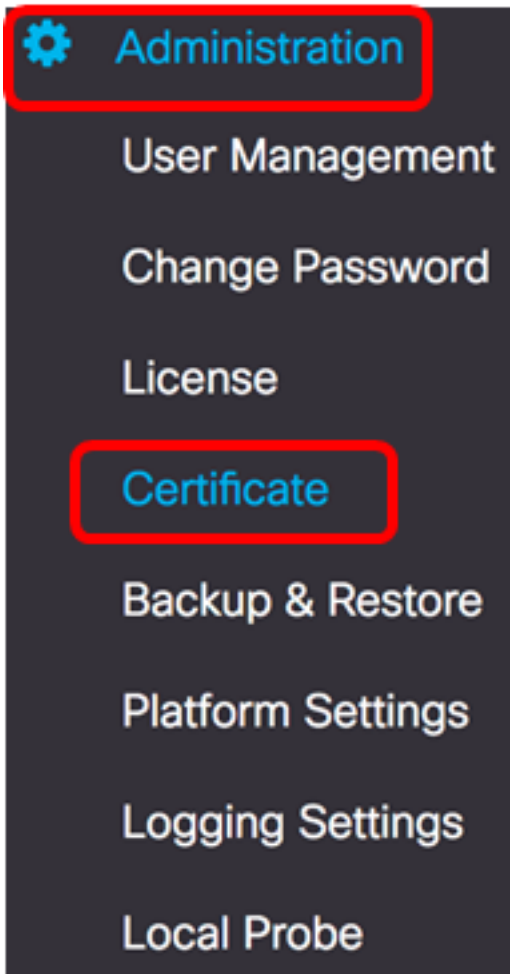
Stap 5. Klik op **Upload**.



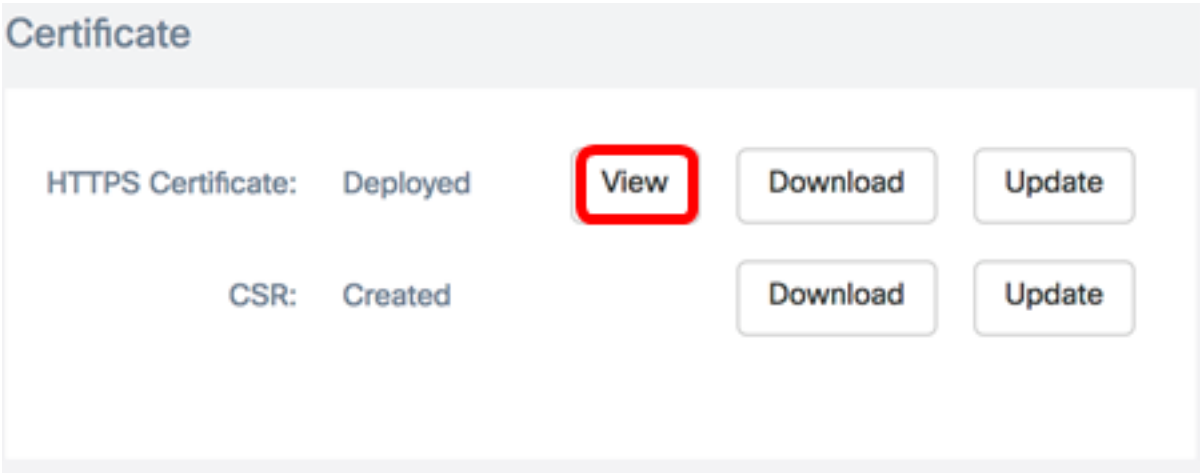
U hebt nu met succes een ondertekend certificaat geüpload naar de FindIT Network Manager.

Huidig certificaat beheren

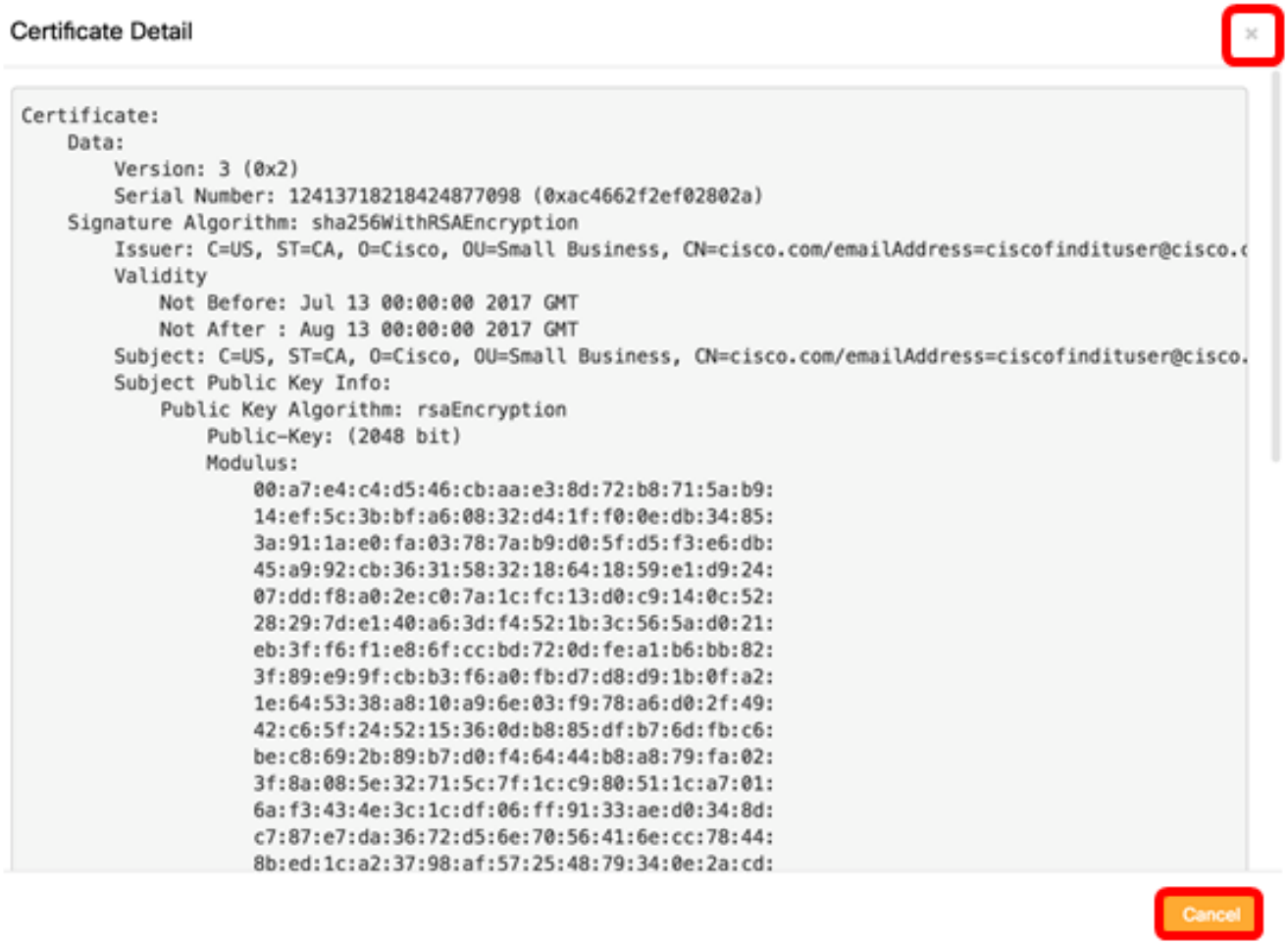
Stap 1. Meld u aan bij de Administration GUI van uw FindIT Network Manager en kies vervolgens **Administratie > Certificaat**.



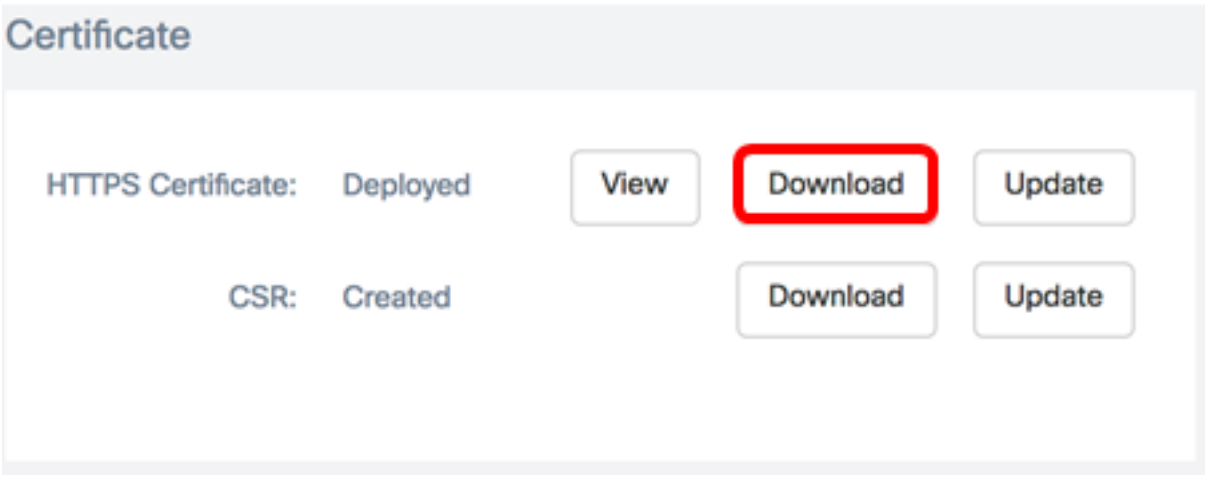
Stap 2. Klik in het gebied HTTPS-certificaat op de knop **Bekijken**.



Stap 3. Het huidige certificaat wordt in onbewerkte tekstindeling weergegeven in een nieuw browser-venster. Klik op de knop **x** of **Annuleren** om het venster te sluiten.



Stap 4. (Optioneel) Klik om een kopie van het huidige certificaat te downloaden op de knop **Downloaden** in het veld HTTPS-certificaat.



U dient nu het huidige certificaat met succes te beheren op uw FindIT Network Manager.