

# FindITネットワークマネージャでの証明書の管理

## 目的

デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによる署名やアサーションに依存できます。インストール時に、FindIT Network Managerは自己署名証明書を生成して、Webやその他のサーバとの通信を保護します。この証明書を、信頼できる認証局(CA)によって署名された証明書に置き換えることもできます。これを行うには、CAによる署名用の証明書署名要求(CSR)を生成する必要があります。

また、証明書と対応する秘密キーをマネージャから完全に独立して生成することもできます。その場合は、アップロードする前に、証明書と秘密キーを公開キー暗号規格(PKCS)#12形式ファイルに組み合わせることができます。

FindITネットワークマネージャは、.pem形式の証明書のみをサポートします。他の証明書形式を取得する場合は、形式を変換するか、CAから.pem形式の証明書を再度要求する必要があります。

この記事では、FindIT Network Managerで証明書を管理する方法について説明します。

## 該当するデバイス

- FindIT ネットワーク マネージャ

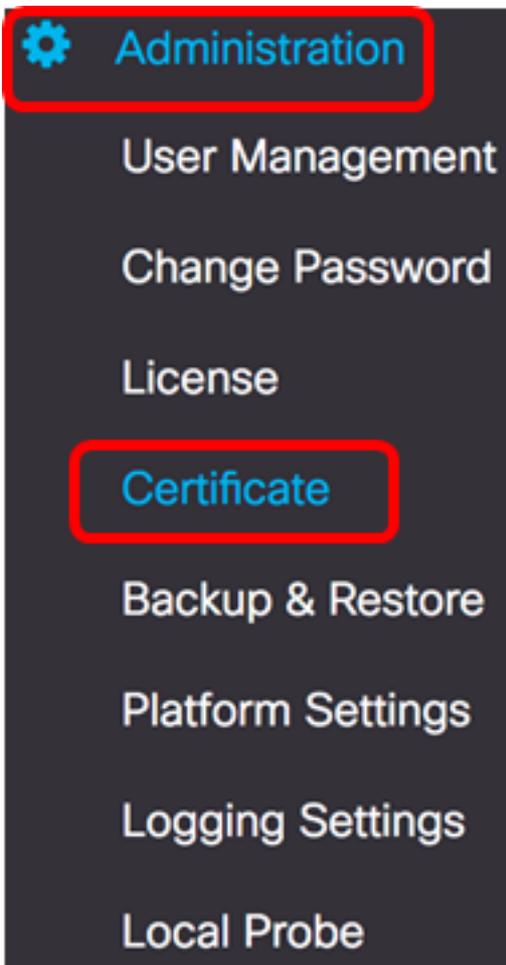
## [Software Version]

- 1.1

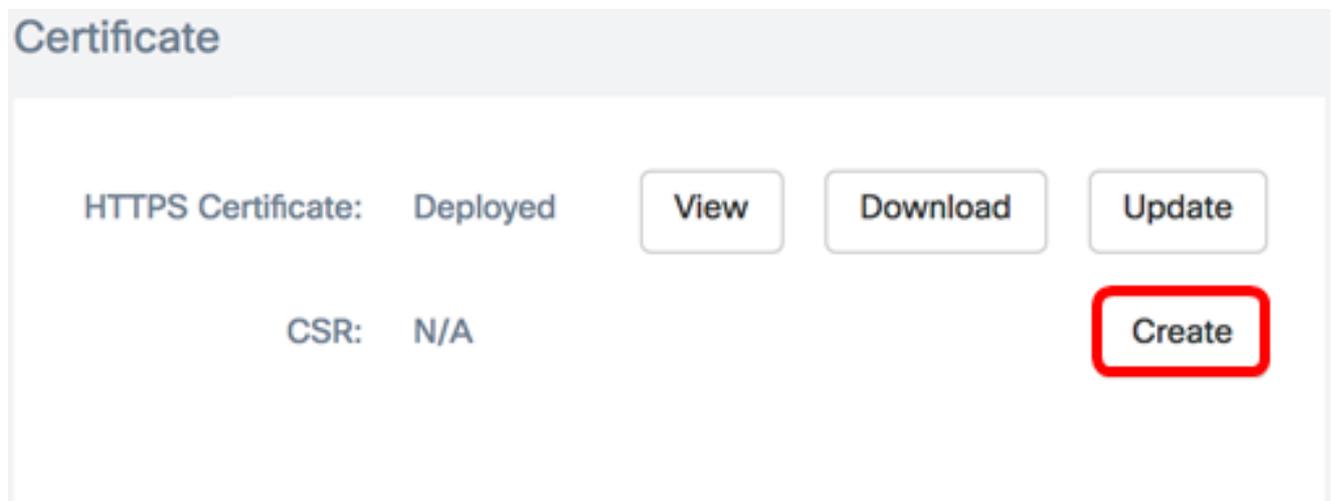
## FindITネットワークマネージャでの証明書の管理

### CSR の生成

ステップ1:FindITネットワークマネージャの管理GUIにログインし、[管理(Administration)] > [証明書(Certificate)]を選択します。



ステップ2:[CSR]領域で、[作成]ボタンをクリックします。



証明書フォームに入力した値はCSRの構築に使用され、CAから受け取った署名付き証明書に含まれます。

[ステップ3](#): [Full qualified domain name]フィールドにIPアドレスまたはドメイン名を入力します。この例では、hostname.cisco.comが使用されています。



ステップ4:[Country (国)]フィールドに国コードを入力します。この例では、USが使用されています。

Country  ✓

ステップ5:[State]フィールドに状態コードを入力します。この例では、CAが使用されています。

State  ✓

ステップ6:[City]フィールドに市を入力します。この例では、Irvineが使用されています。

City  ✓

ステップ7:[Org]フィールドに組織名を入力します。この例では、Ciscoが使用されています。

Org  ✓

ステップ8:「組織単位」フィールドに組織単位を入力します。この例では、Small Businessが使用されています。

Org Units  ✓

ステップ9:[Email (メール)]フィールドにメールアドレスを入力します。この例では、[ciscofindituser@cisco.com](mailto:ciscofindituser@cisco.com)と入力しています。

Email  ✓

ステップ10:[Save]をクリックします。

Certificate

Note: When you create the CSR file successfully, please send the downloaded file to a Certificate Authority to issue, and then upload the issued certificate to system by operation (Update/Upload Cert).

Full qualified domain name  ✓

Country  ✓

State  ✓

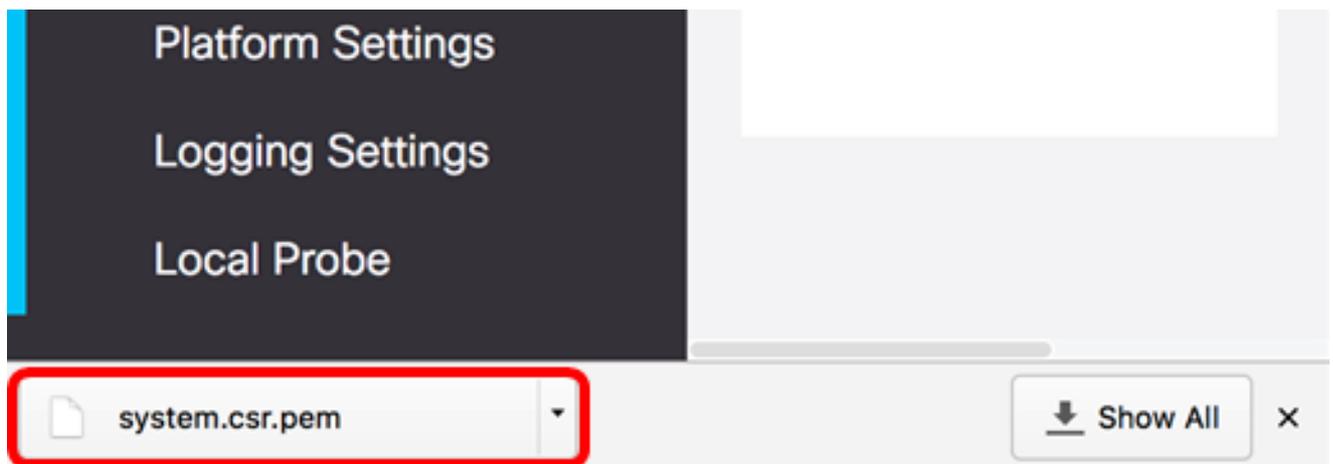
City  ✓

Org  ✓

Org Units  ✓

Email  ✓

CSRファイルが自動的にコンピュータにダウンロードされます。この例では、system.csr.pemファイルが生成されます。

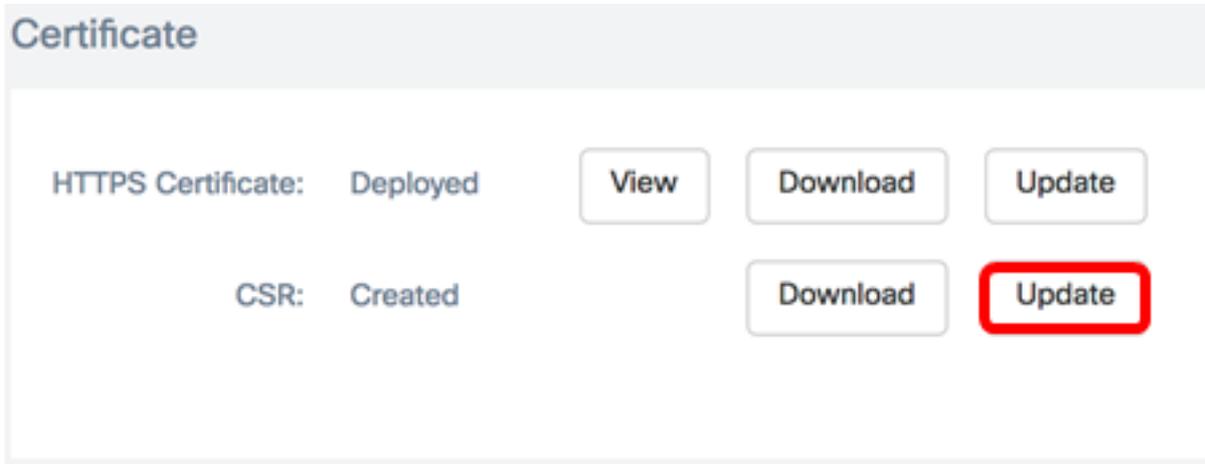


ステップ11: ( オプション ) [CSR]領域で、ステータスが[N/A]から[Created]に更新されます。作成したCSRをダウンロードするには、[ダウンロード]ボタンをクリックします。

Certificate

HTTPS Certificate:	Deployed	<input type="button" value="View"/>	<input type="button" value="Download"/>	<input type="button" value="Update"/>
CSR:	Created		<input type="button" value="Download"/>	<input type="button" value="Update"/>

ステップ12: ( オプション ) 作成したCSRを更新するには、[更新]ボタンをクリックし、ステップ3に[戻ります](#)。

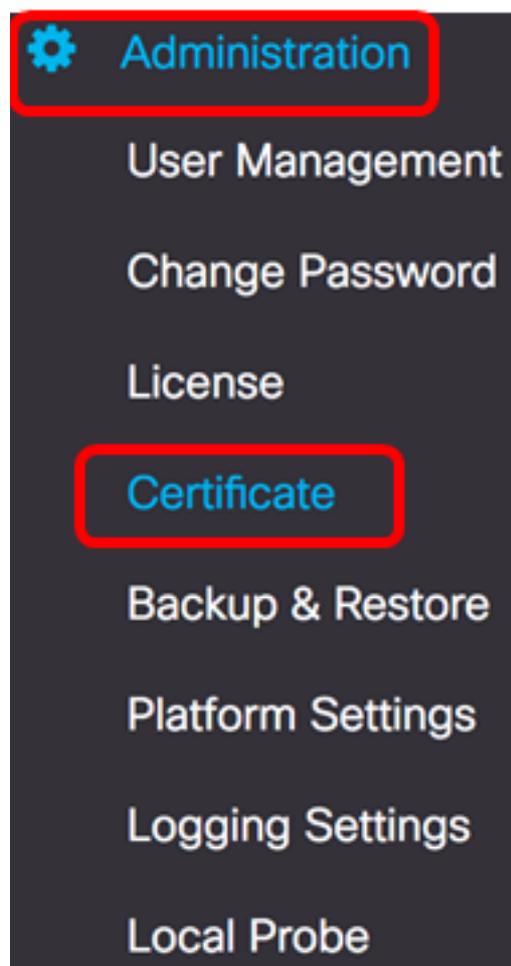


これで、FindITネットワークマネージャでCSRが正常に生成されました。ダウンロードしたCSRファイルをCAに送信できるようになりました。

## CAからの署名付き証明書のアップロード

署名付きCSRをCAから受け取ったら、マネージャにアップロードできます。

ステップ1: FindITネットワークマネージャの管理GUIにログインし、[管理(Administration)] > [証明書(Certificate)]を選択します。



ステップ2: [HTTPS Certificate]領域で、[Update]ボタンをクリックします。

## Certificate

HTTPS Certificate: Deployed

View

Download

Update

CSR: Created

Download

Update

ステップ3:[UploadCert]ラジオボタンをクリックします。

## Certificate

Renew Self-signed Cert



Upload Cert

Upload PKCS12

注：または、[PKCS12のアップロード]オプションボタンを選択して、PKCS#12形式で関連付けられた秘密キーを使用して証明書をアップロードできます。ファイルのロックを解除するパスワードは、指定された[パスワード]フィールドで指定する必要があります。

Upload Cert

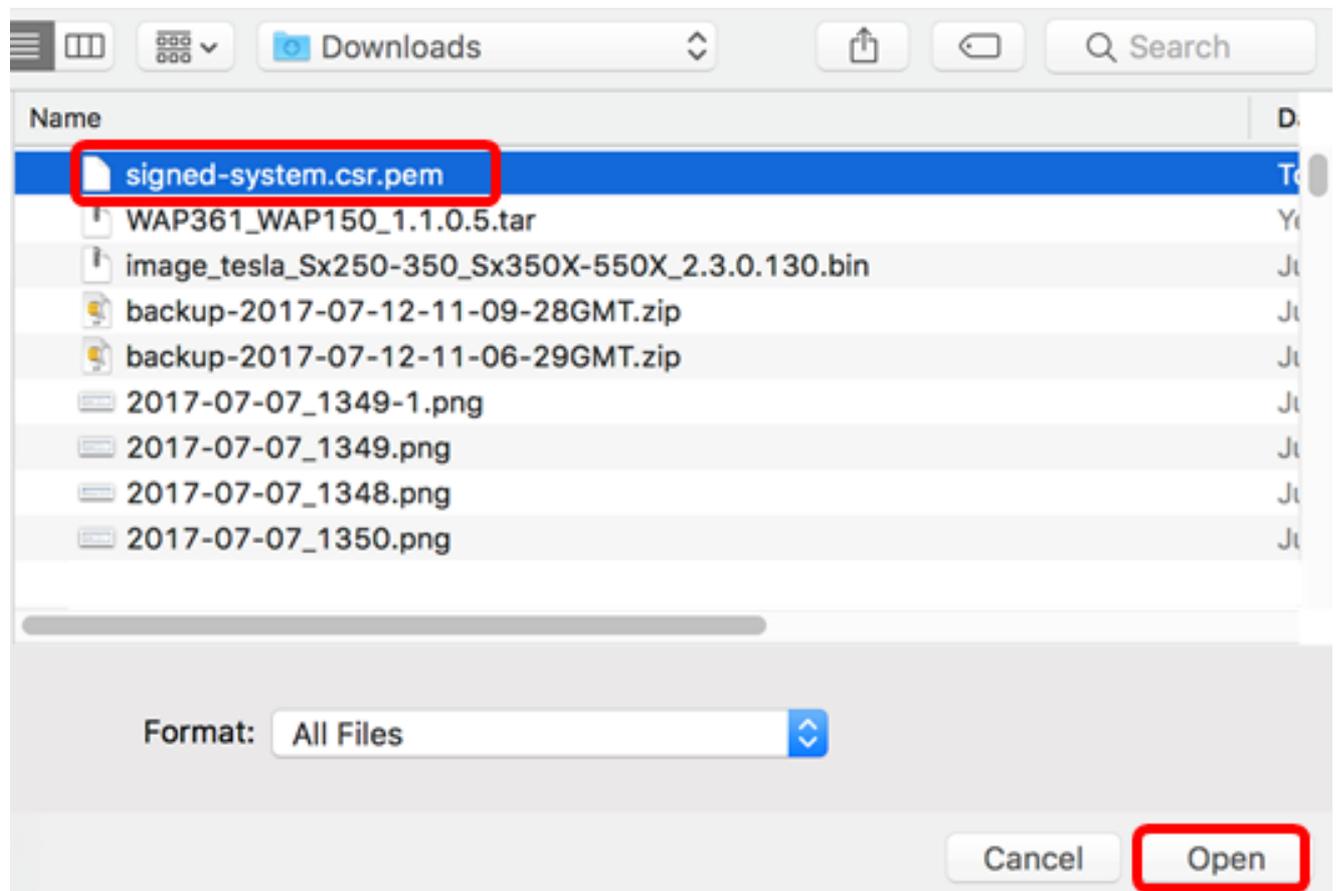


Upload PKCS12

Password:

.....|

ステップ4：ターゲット領域に署名付き証明書をドロップするか、ターゲット領域をクリックしてファイルシステムを参照し、[開く]をクリックします。ファイルは.pem形式である必要があります。



注：この例では、signed-system.csr.pemが使用されています。

ステップ5:[Upload]をクリックします。

Certificate

Renew Self-signed Cert     Upload Cert     Upload PKCS12

Drag and drop file here (or  
click to select a file from the  
filesystem)

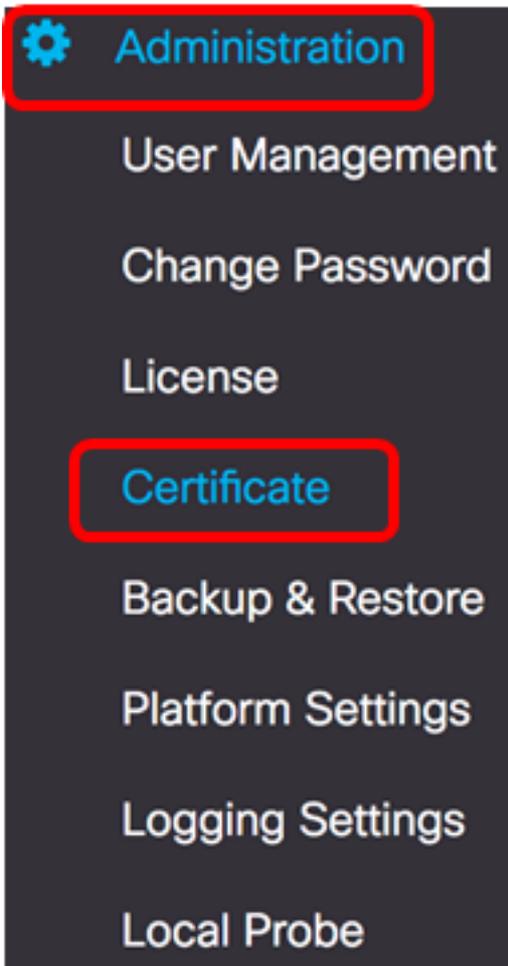
Filename: signed-system.csr.pem

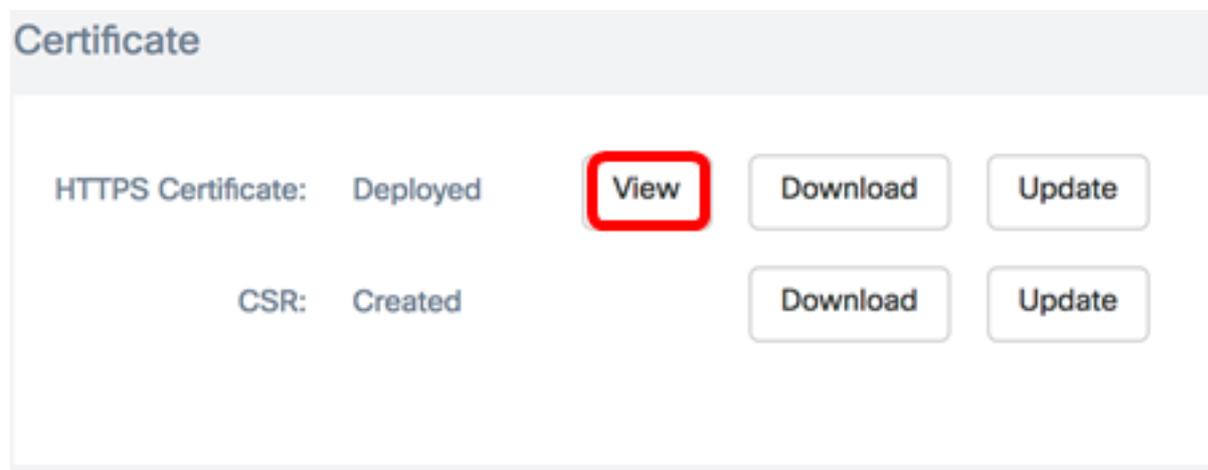
これで、署名付き証明書がFindITネットワークマネージャに正常にアップロードされました。

## 現在の証明書の管理

ステップ1: FindITネットワークマネージャの管理GUIにログインし、[管理(Administration)] > [証明書(Certificate)]を選択します。



ステップ2:[HTTPS Certificate]領域で、[View]ボタンをクリックします。



ステップ3：現在の証明書がプレーンテキスト形式で新しいブラウザウィンドウに表示されます。xボタンまたはCancelボタンをクリックして、ウィンドウを閉じます。

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 12413718218424877098 (0xac4662f2ef02802a)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=CA, O=Cisco, OU=Small Business, CN=cisco.com/emailAddress=cisconfindituser@cisco.c
Validity
  Not Before: Jul 13 00:00:00 2017 GMT
  Not After : Aug 13 00:00:00 2017 GMT
Subject: C=US, ST=CA, O=Cisco, OU=Small Business, CN=cisco.com/emailAddress=cisconfindituser@cisco.
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
  Modulus:
    00:a7:e4:c4:d5:46:cb:aa:e3:8d:72:b8:71:5a:b9:
    14:ef:5c:3b:bf:a6:08:32:d4:1f:f0:0e:db:34:85:
    3a:91:1a:e0:fa:03:78:7a:b9:d0:5f:d5:f3:e6:db:
    45:a9:92:cb:36:31:58:32:18:64:18:59:e1:d9:24:
    07:dd:f8:a0:2e:c0:7a:1c:fc:13:d0:c9:14:0c:52:
    28:29:7d:e1:40:a6:3d:f4:52:1b:3c:56:5a:d0:21:
    eb:3f:f6:f1:e8:6f:cc:bd:72:0d:fe:a1:b6:bb:82:
    3f:89:e9:9f:cb:b3:f6:a0:fb:d7:d8:d9:1b:0f:a2:
    1e:64:53:38:a8:10:a9:6e:03:f9:78:a6:d0:2f:49:
    42:c6:5f:24:52:15:36:0d:b8:85:df:b7:6d:fb:c6:
    be:c8:69:2b:89:b7:d0:f4:64:44:b8:a8:79:fa:02:
    3f:8a:08:5e:32:71:5c:7f:1c:c9:00:51:1c:a7:01:
    6a:f3:43:4e:3c:1c:df:06:ff:91:33:ae:d0:34:8d:
    c7:87:e7:da:36:72:d5:6e:70:56:41:6e:cc:78:44:
    8b:ed:1c:a2:37:98:af:57:25:48:79:34:0e:2a:cd:
```

Cancel

ステップ4: ( オプション ) 現在の証明書のコピーをダウンロードするには、[HTTPS Certificate]領域の[Download]ボタンをクリックします。

### Certificate

HTTPS Certificate:	Deployed	View	<b>Download</b>	Update
CSR:	Created		Download	Update

これで、FindITネットワークマネージャで現在の証明書を正常に管理できました。