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

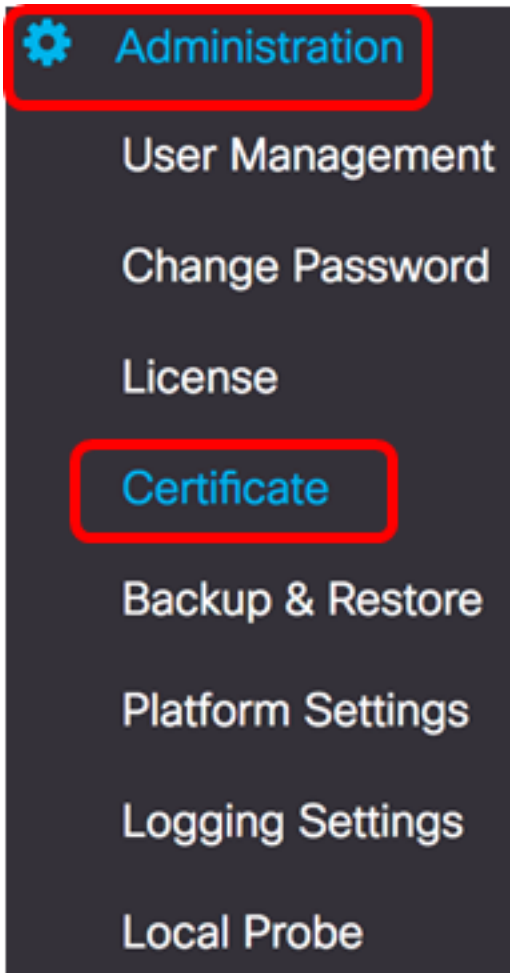
[Software Version]

- 1.1

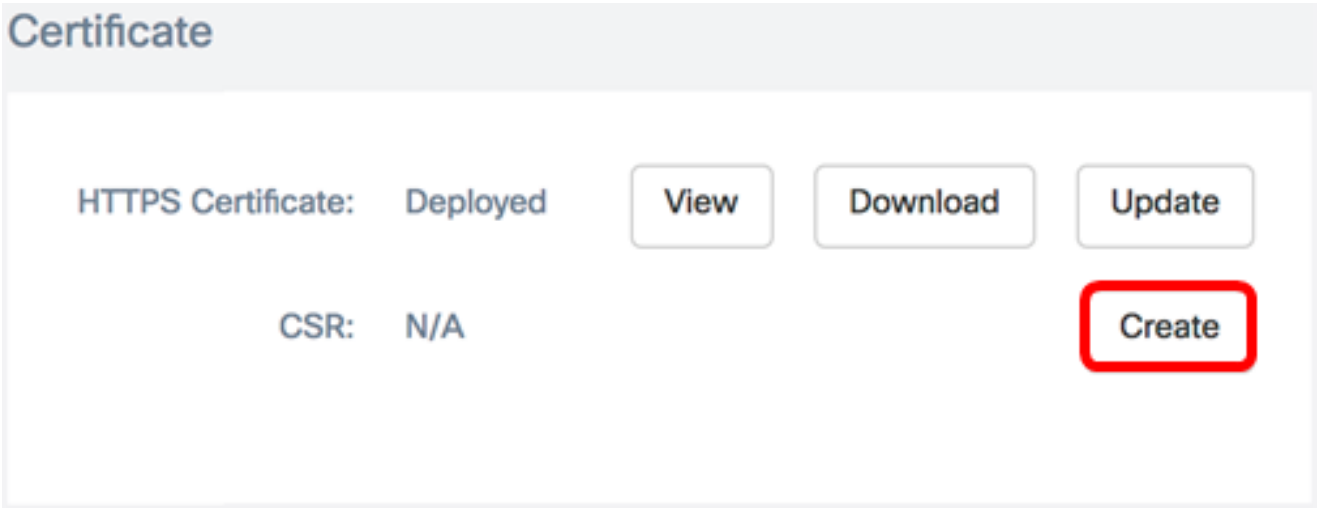
FindITネットワークマネージャでの証明書の管理

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。**

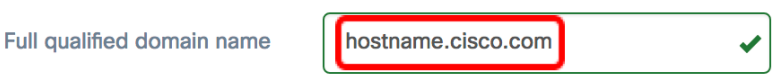


ステップ2:[CSR]領域で、[作成]ボタンをクリックします。



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。

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。

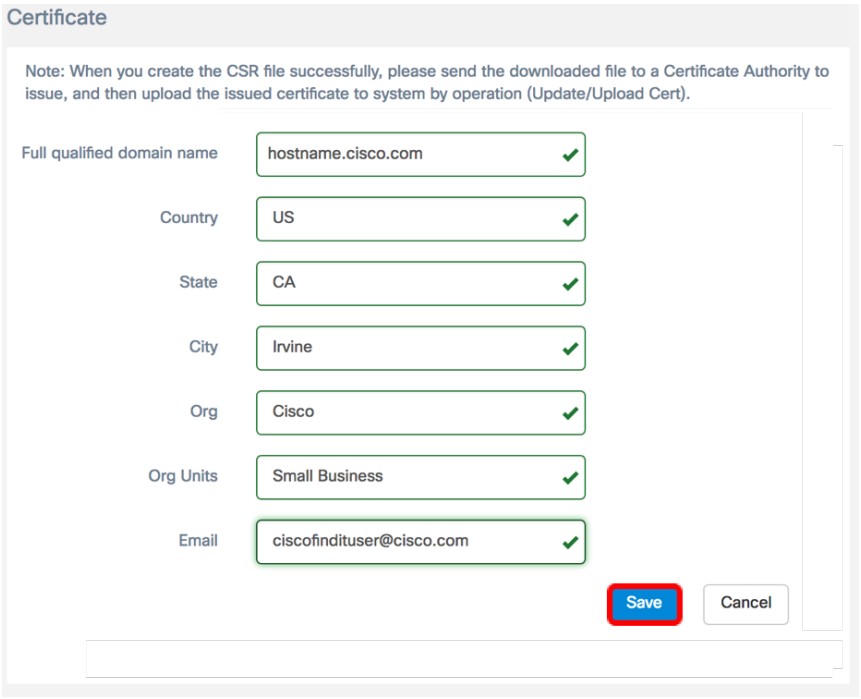
ステップ6:[City]フィールドに市を入力します。この例では、Irvineが使用されています。

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。

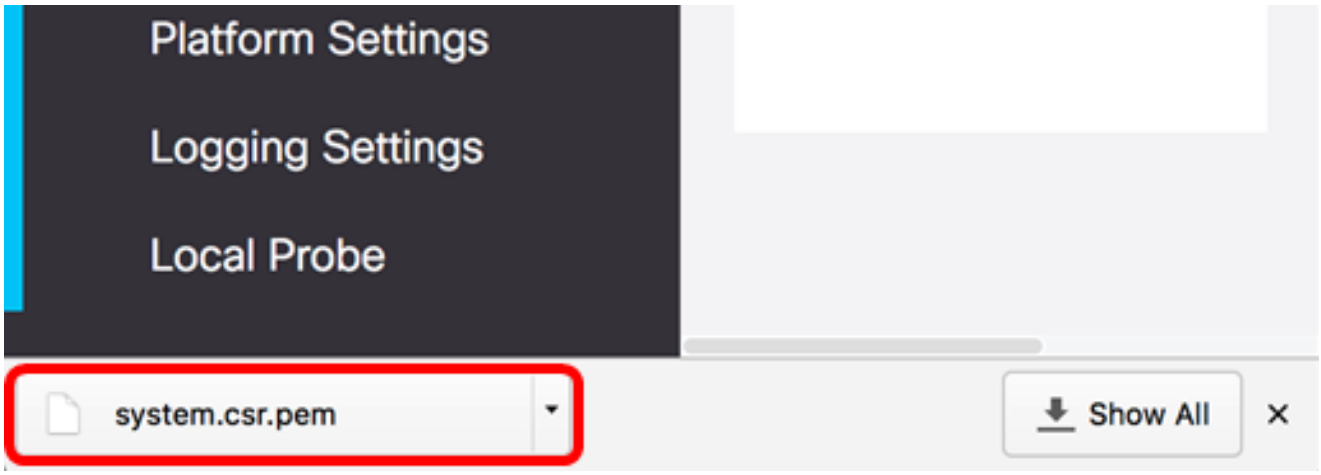
ステップ8:「組織単位」フィールドに組織*単位*を入力します。この例では、Small Businessが使用されています。

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と入力しています。

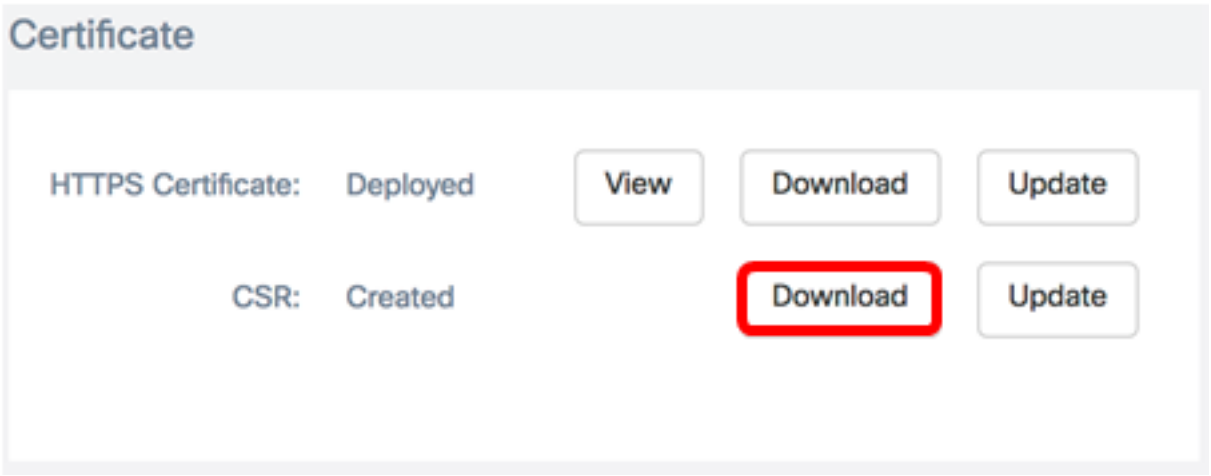
ステップ10:**[Save]をクリックします。**



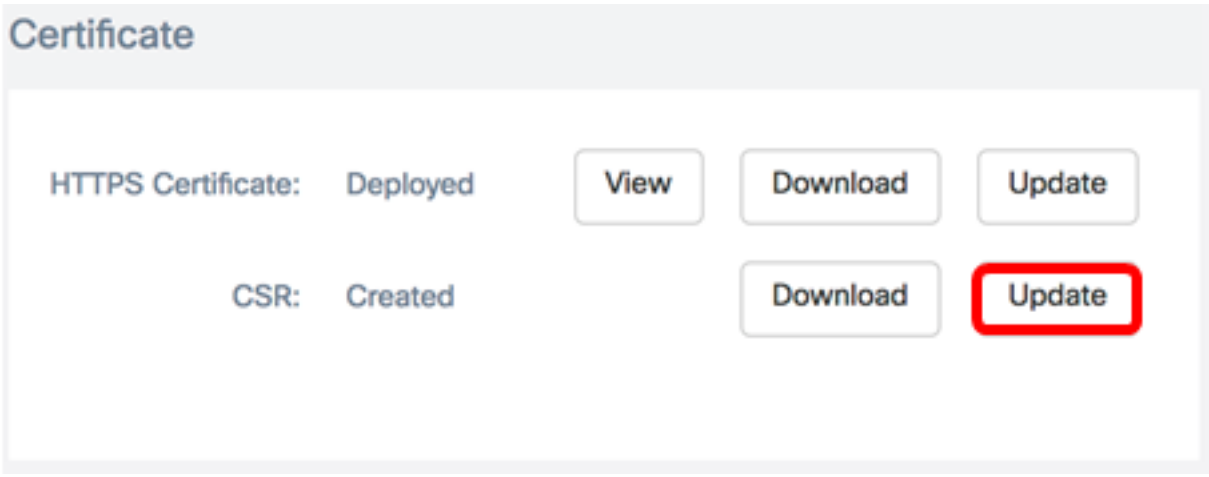
CSRファイルが自動的にコンピュータにダウンロードされます。この例では、system.csr.pemファイルが生成されます。



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。



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。

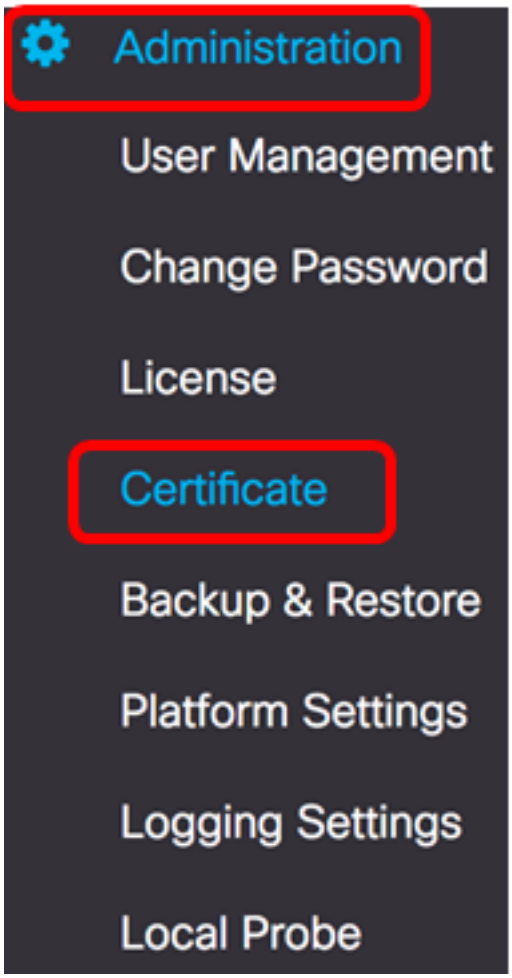


これで、FindITネットワークマネージャでCSRが正常に生成されました。ダウンロードしたCSRファイルをCAに送信できるようになりました。

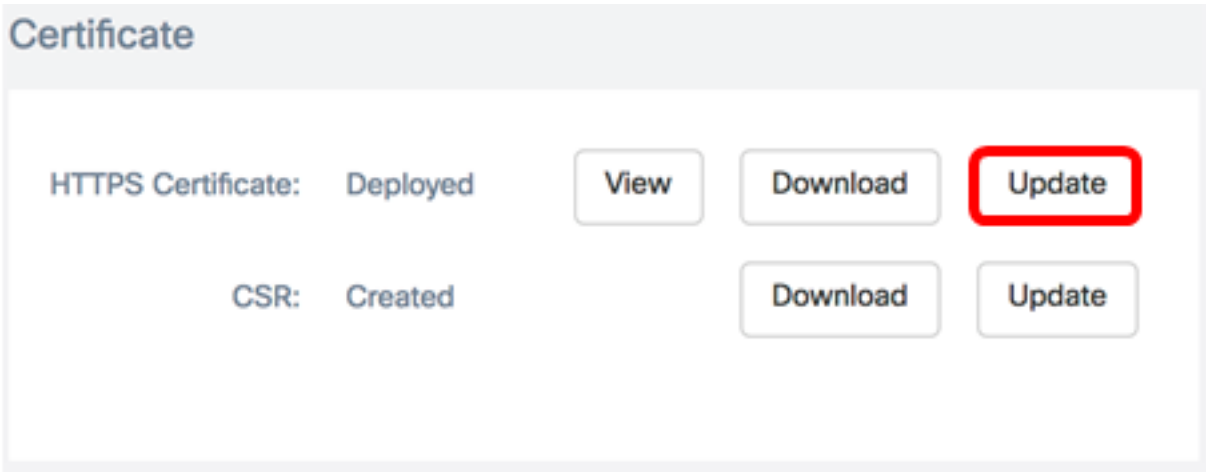
CAからの署名付き証明書のアップロード

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。

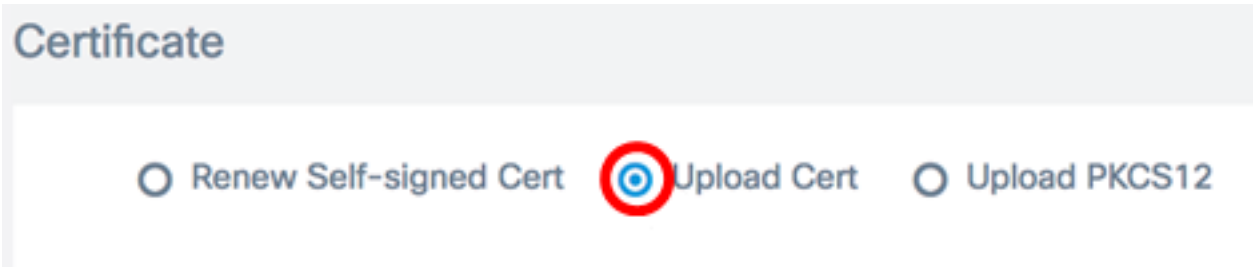
ステップ1:FindITネットワークマネージャの管理GUIにログインし、[管理(**Administration**)] > **[証明書(Certificate)]を選択します**。



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

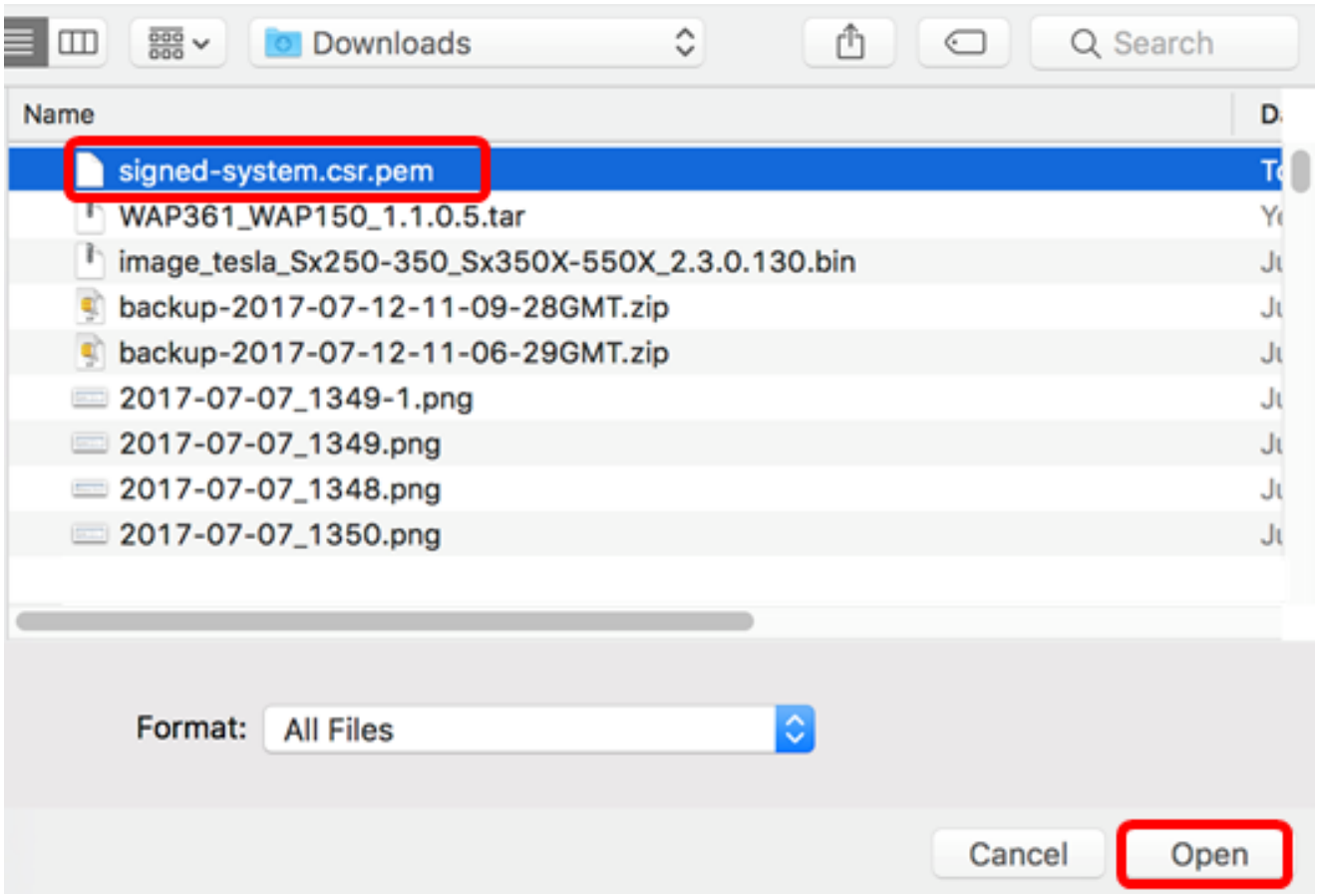


ステップ3:[UploadCert]ラジオボ**タンを**クリックします。



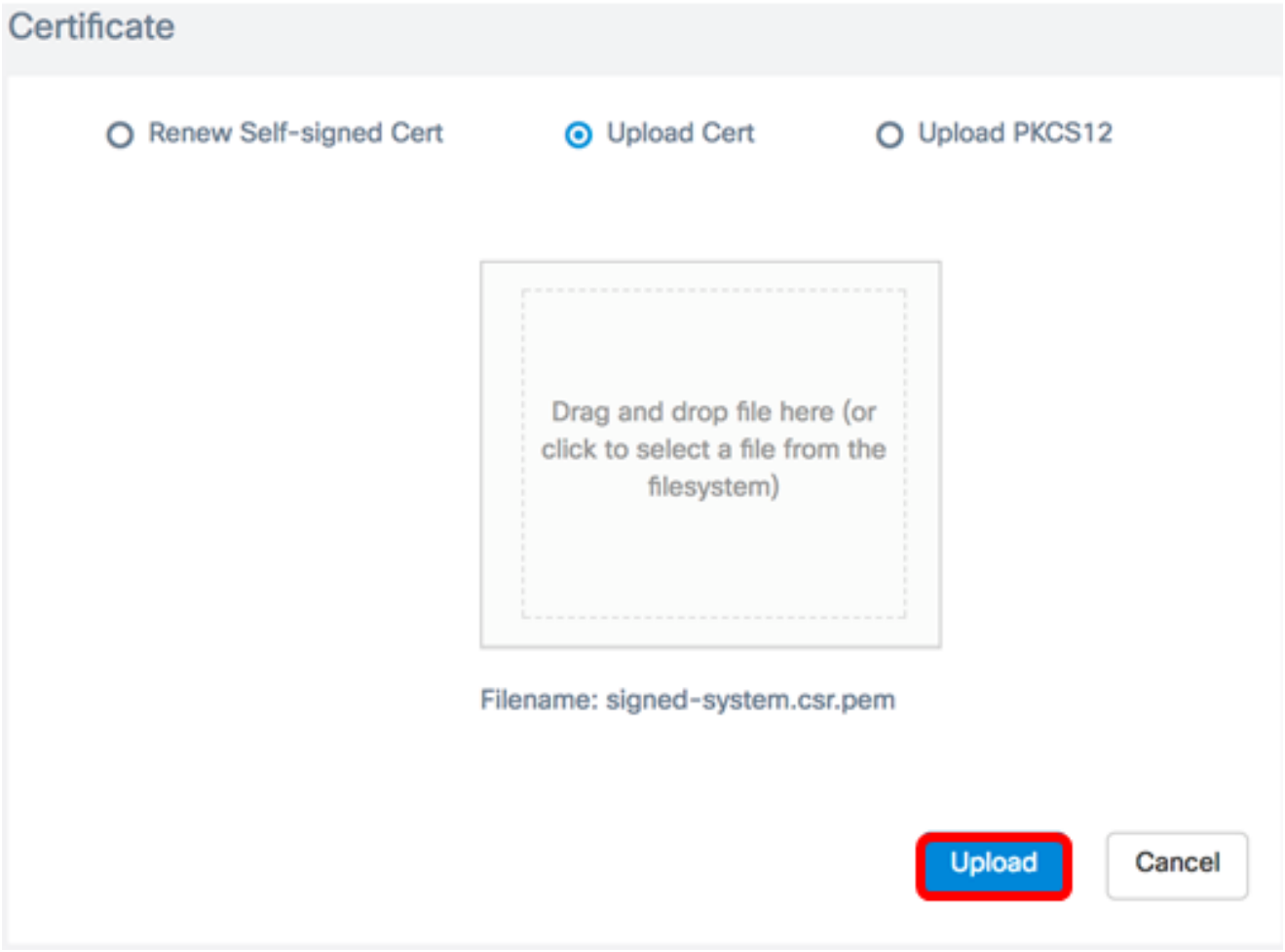
注：または、[PKCS12のアップロード]オプションボタンを選択して、PKCS#12形式で関連付けられた秘密キーを使用して証明書**をアップロード**できます。ファイルのロックを解除するパスワードは、指定された[パスワード]フィールドで指定する*必要*があります。

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。

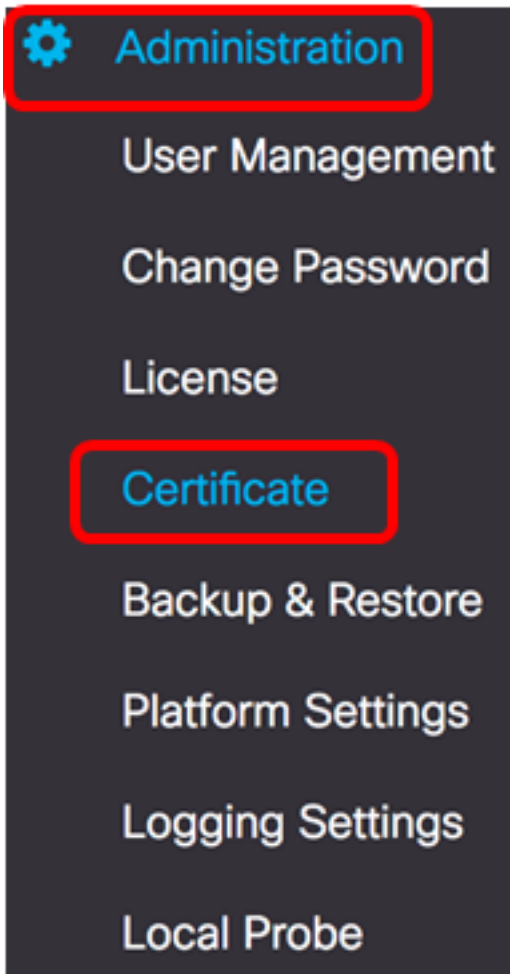
ステップ5:[Upload]をクリックします。



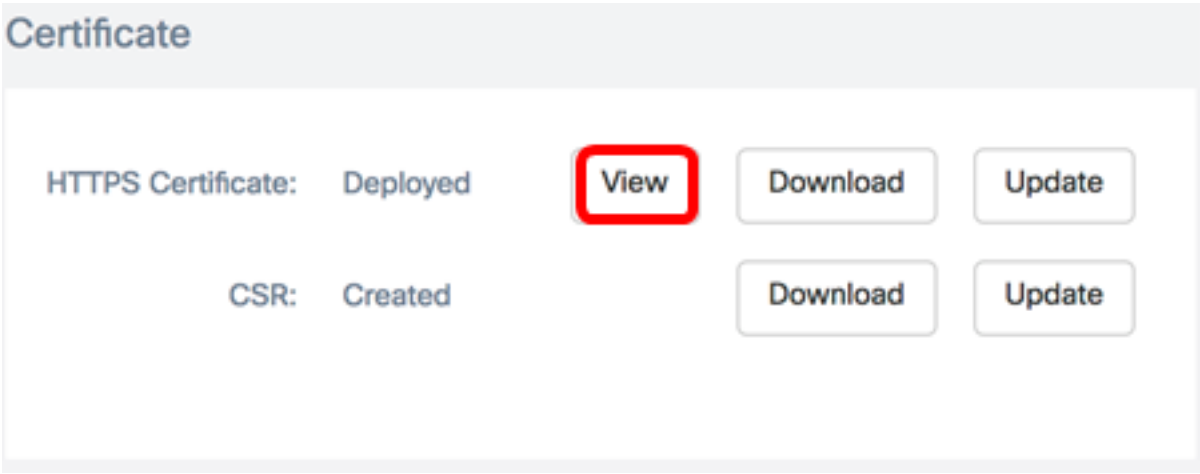
これで、署名付き証明書がFindITネットワークマネージャに正常にアップロードされました。

現在の証明書の管理

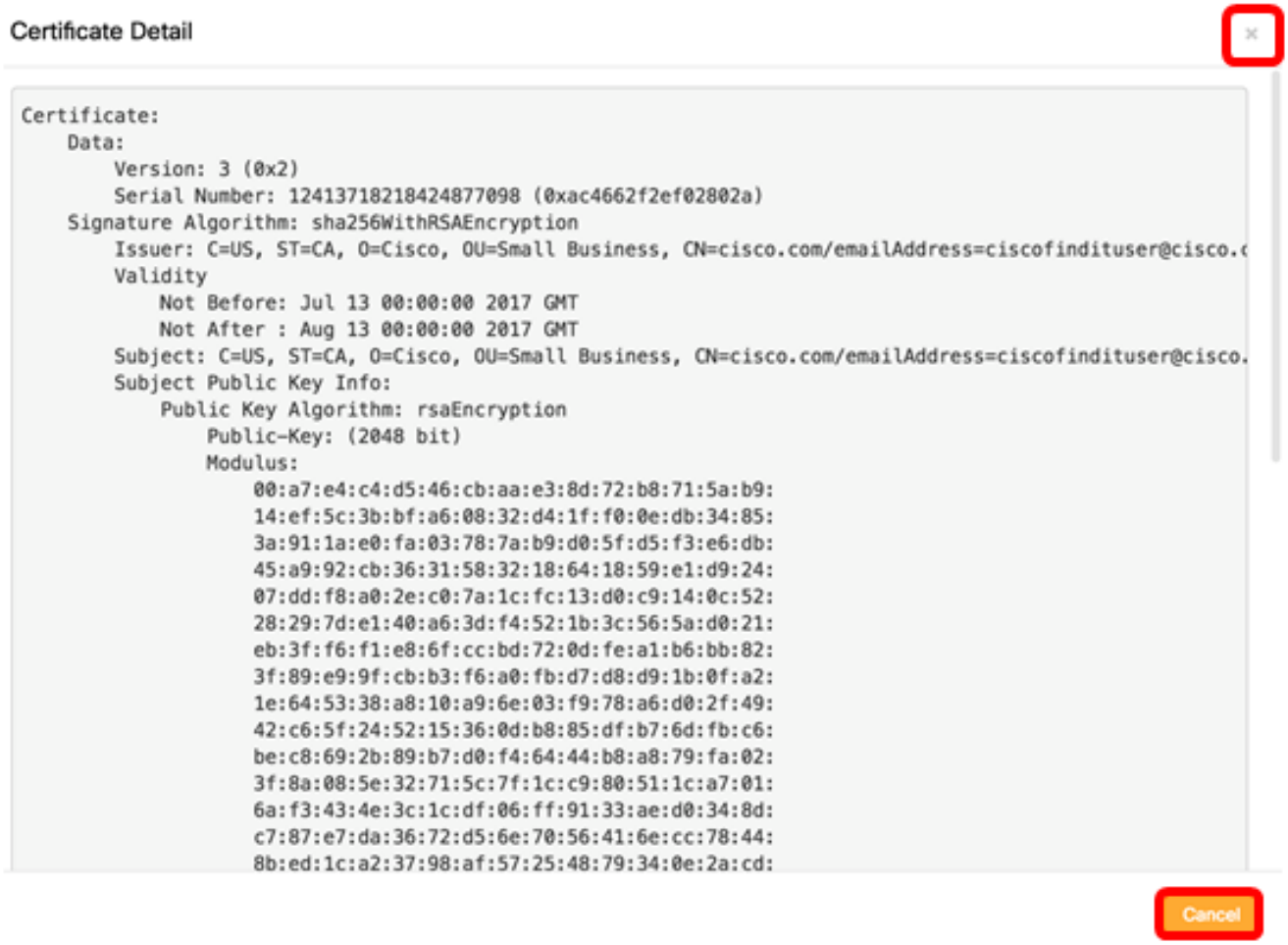
ステップ1:FindITネットワークマネージャの管理GUIにログインし、[管理(**Administration**)] > **[証明書(Certificate)]を選択します**。



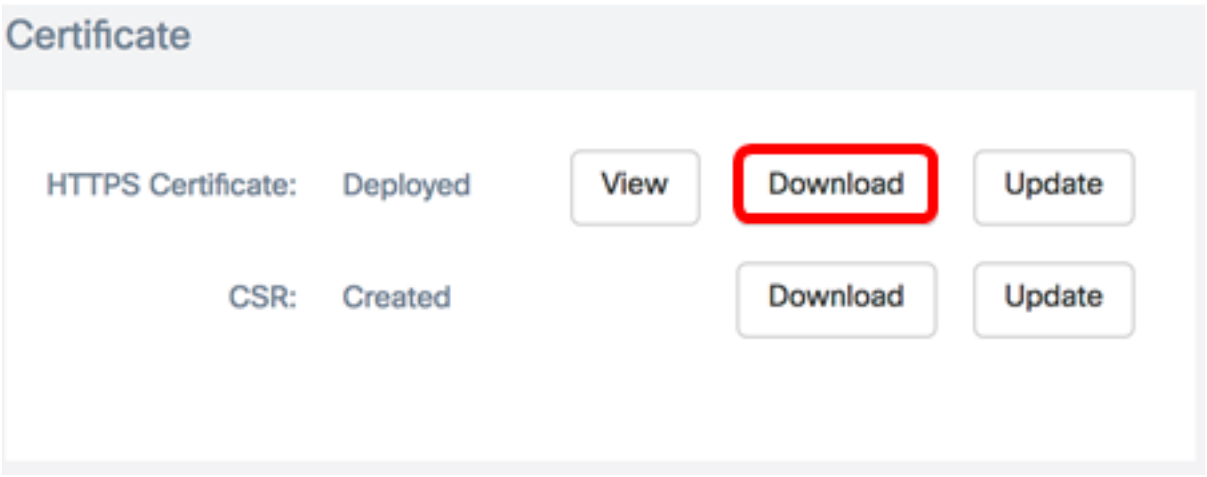
ステップ2:[HTTPS Certificate]領域で、[**View**]ボタンをクリ**ック**します。



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。



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。



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。