Verwalten von Zertifikaten im FindIT Network Manager

Ziel

Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Bei der Installation generiert der FindIT Network Manager ein selbstsigniertes Zertifikat, um die Web- und andere Kommunikation mit dem Server zu sichern. Sie können dieses Zertifikat durch das Zertifikat ersetzen, das von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert wurde. Dazu müssen Sie eine CSR-Anfrage (Certificate Signing Request) für die Signierung durch die CA generieren.

Sie können auch ein Zertifikat und den zugehörigen privaten Schlüssel generieren, die völlig unabhängig vom Manager sind. Wenn dies der Fall ist, können Sie das Zertifikat und den privaten Schlüssel vor dem Hochladen in eine PKCS-#12-Formatdatei (Public Key Cryptography Standards) kombinieren.

Der FindIT Network Manager unterstützt nur Zertifikate im .pem-Format. Wenn Sie andere Zertifikatsformate erhalten, müssen Sie das Format oder die Anforderung des Zertifikats im .pem-Format erneut von der CA konvertieren.

Dieser Artikel enthält Anweisungen zum Verwalten von Zertifikaten unter FindIT Network Manager.

Anwendbare Geräte

- FindIT Network Manager

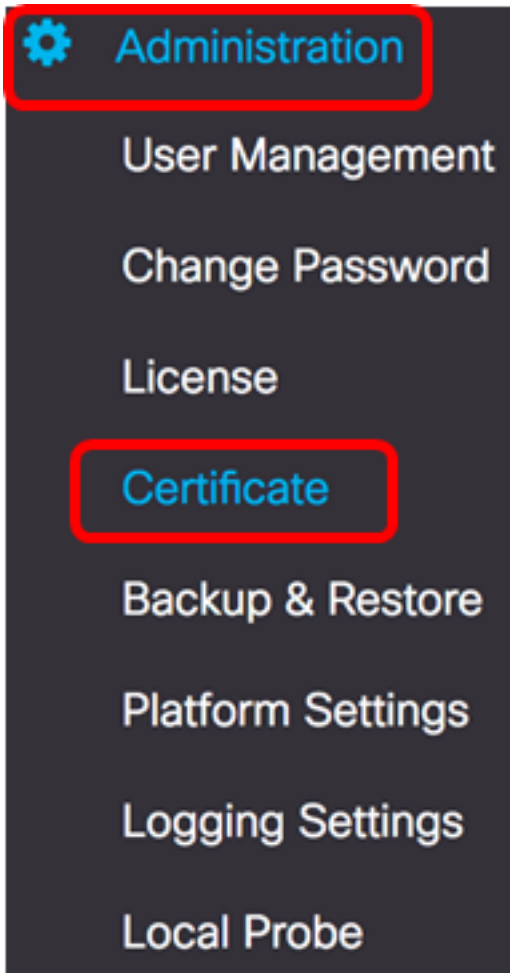
Softwareversion

- 1,1

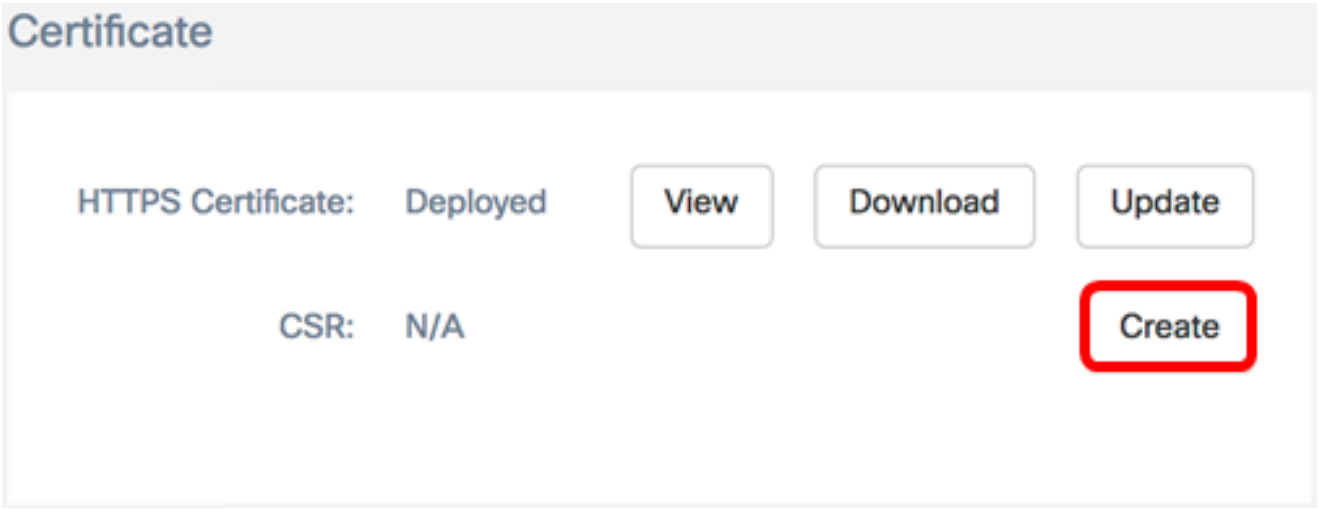
Verwalten von Zertifikaten in FindIT Network Manager

CSR erstellen

Schritt 1: Melden Sie sich bei der Verwaltungs-GUI Ihres FindIT Network Manager an, und wählen Sie dann **Administration > Certificate aus**.



Schritt 2: Klicken Sie im CSR-Bereich auf die Schaltfläche **Erstellen**.



Die im Zertifikatsformular eingegebenen Werte werden zur Erstellung des CSR verwendet und sind im signierten Zertifikat enthalten, das Sie von der Zertifizierungsstelle erhalten.

Schritt 3: Geben Sie die IP-Adresse oder den Domänennamen in das Feld *Vollqualifizierter Domänenname ein*. In diesem Beispiel wird hostname.cisco.com verwendet.

Schritt 4: Geben Sie den Ländercode in das Feld *Land ein*. In diesem Beispiel wird US verwendet.

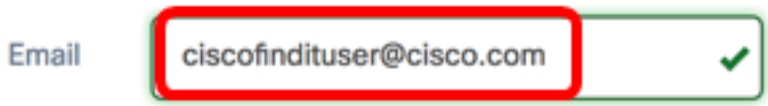
Schritt 5: Geben Sie den Statuscode in das Feld *Status ein*. In diesem Beispiel wird CA verwendet.

Schritt 6: Geben Sie die Stadt in das Feld *Stadt ein*. In diesem Beispiel wird Irvine verwendet.

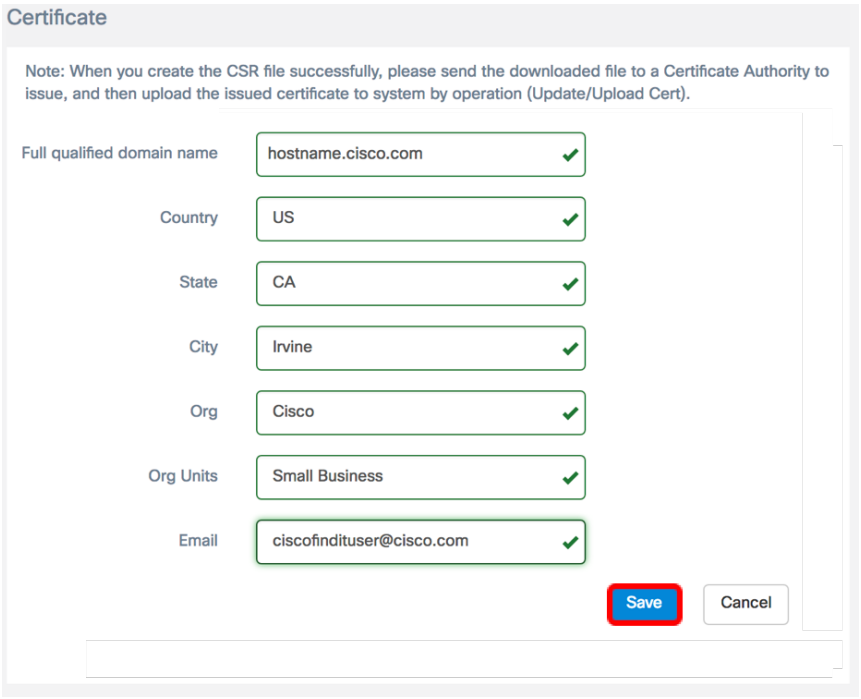
Schritt 7: Geben Sie den Organisationsnamen in das Feld *Org ein*. In diesem Beispiel wird Cisco verwendet.

Schritt 8: Geben Sie die Organisationseinheiten im Feld *Organisationseinheiten ein*. In diesem Beispiel wird Small Business verwendet.

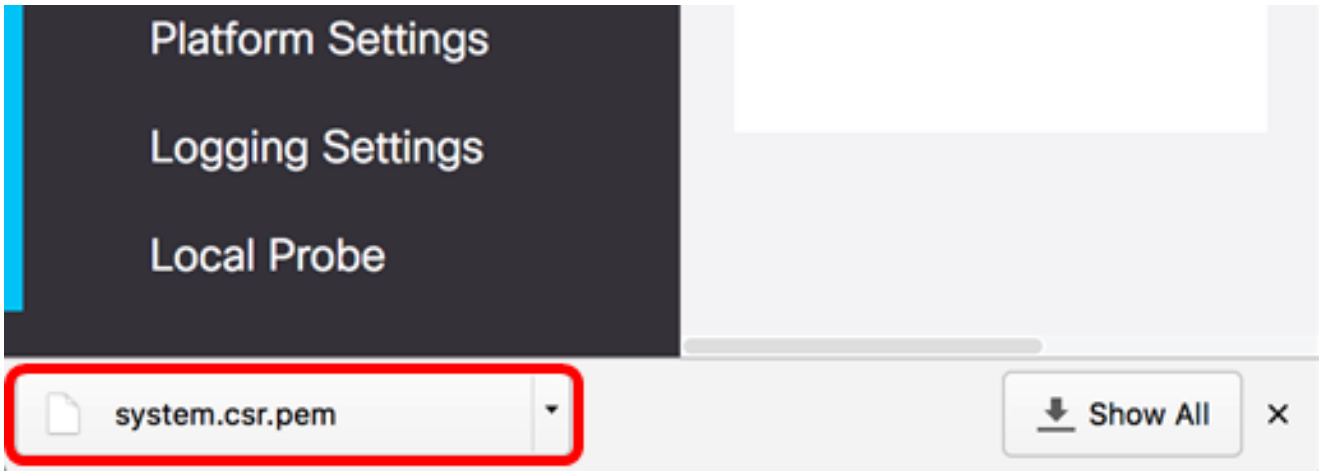
Schritt 9: Geben Sie Ihre E-Mail-Adresse in das Feld *E-Mail ein*. In diesem Beispiel wird ciscofinduser@cisco.com eingegeben.



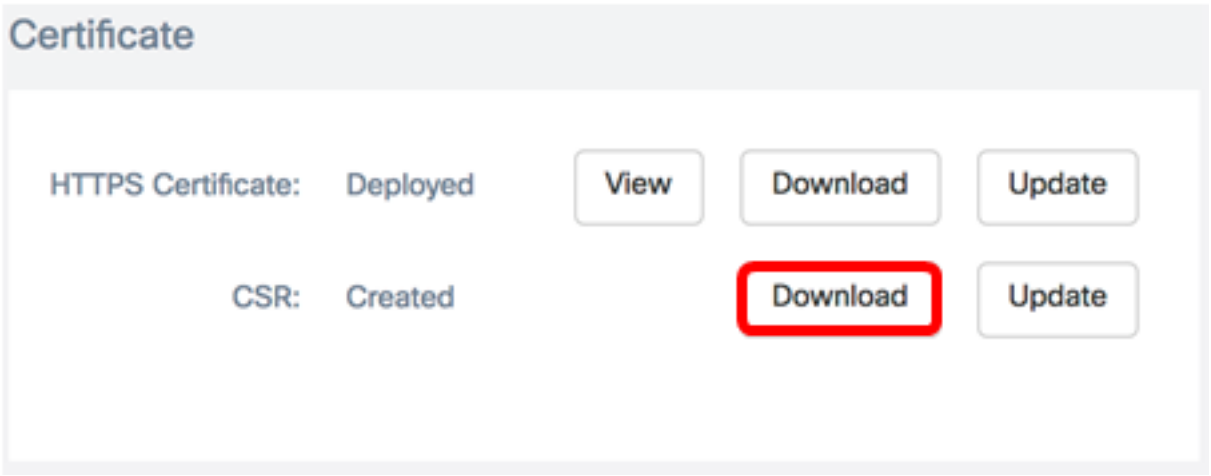
Schritt 10: Klicken Sie auf **Speichern**.



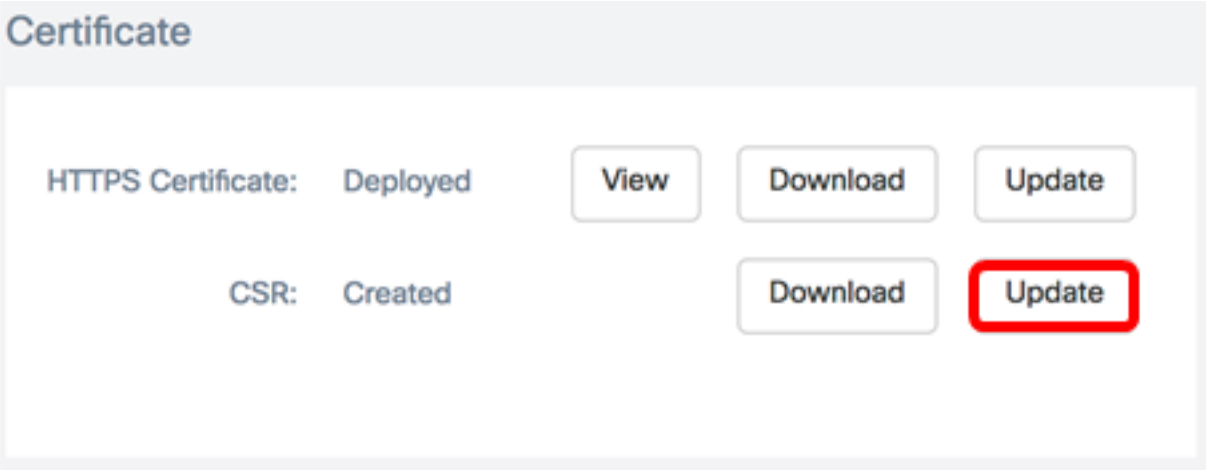
Die CSR-Datei wird automatisch auf Ihren Computer heruntergeladen. In diesem Beispiel wird die Datei system.csr.pem generiert.



Schritt 11: (Optional) Im Bereich CSR wird der Status von N/A auf Created aktualisiert. Klicken Sie zum Herunterladen des erstellten CSR auf die Schaltfläche **Herunterladen**.



Schritt 12: (Optional) Um den erstellten CSR zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** und kehren Sie dann zu Schritt 3 zurück.

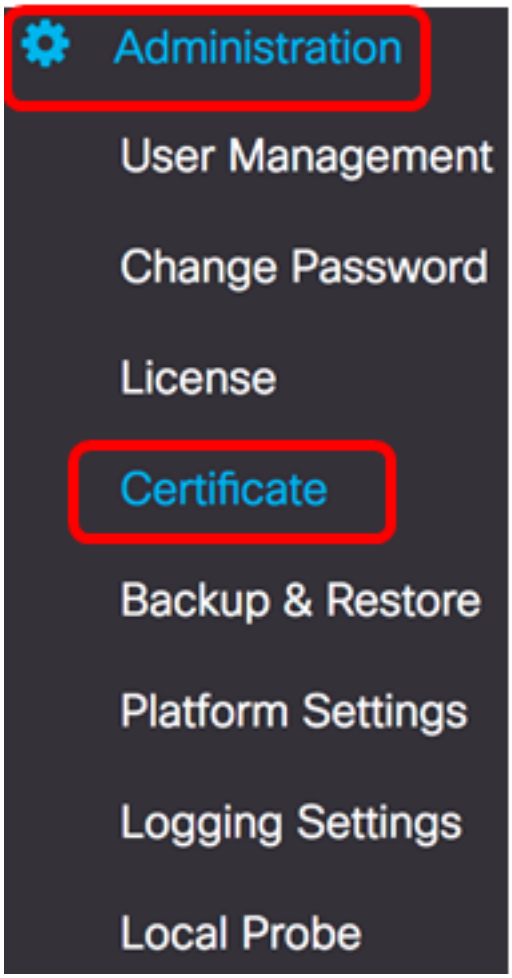


Sie sollten jetzt erfolgreich eine CSR-Anfrage für Ihren FindIT Network Manager erstellt haben. Sie können die heruntergeladene CSR-Datei jetzt an die CA senden.

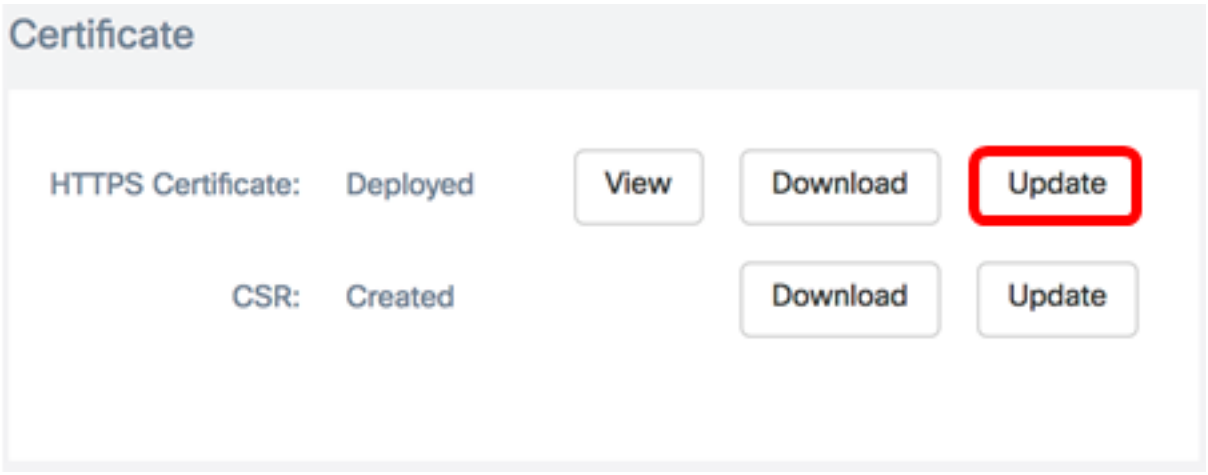
Ein signiertes Zertifikat von der CA hochladen

Sobald Sie die signierte CSR-Anfrage von der CA erhalten haben, können Sie sie jetzt in den Manager hochladen.

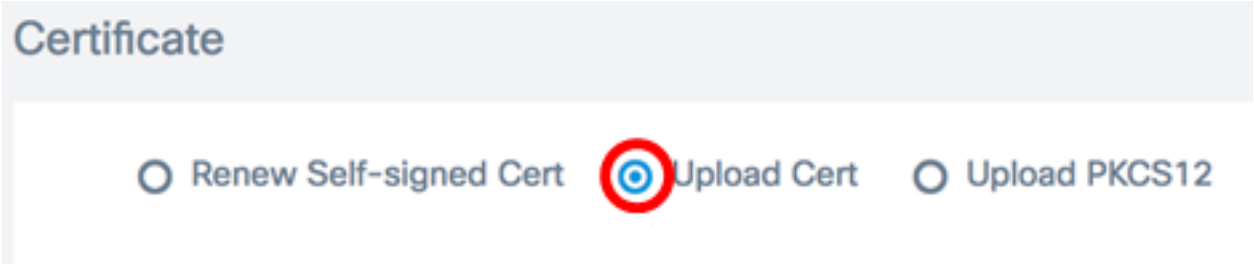
Schritt 1: Melden Sie sich bei der Verwaltungs-GUI Ihres FindIT Network Manager an, und wählen Sie dann **Administration > Certificate aus**.



Schritt 2: Klicken Sie im Bereich HTTPS-Zertifikat auf die Schaltfläche **Aktualisieren**.

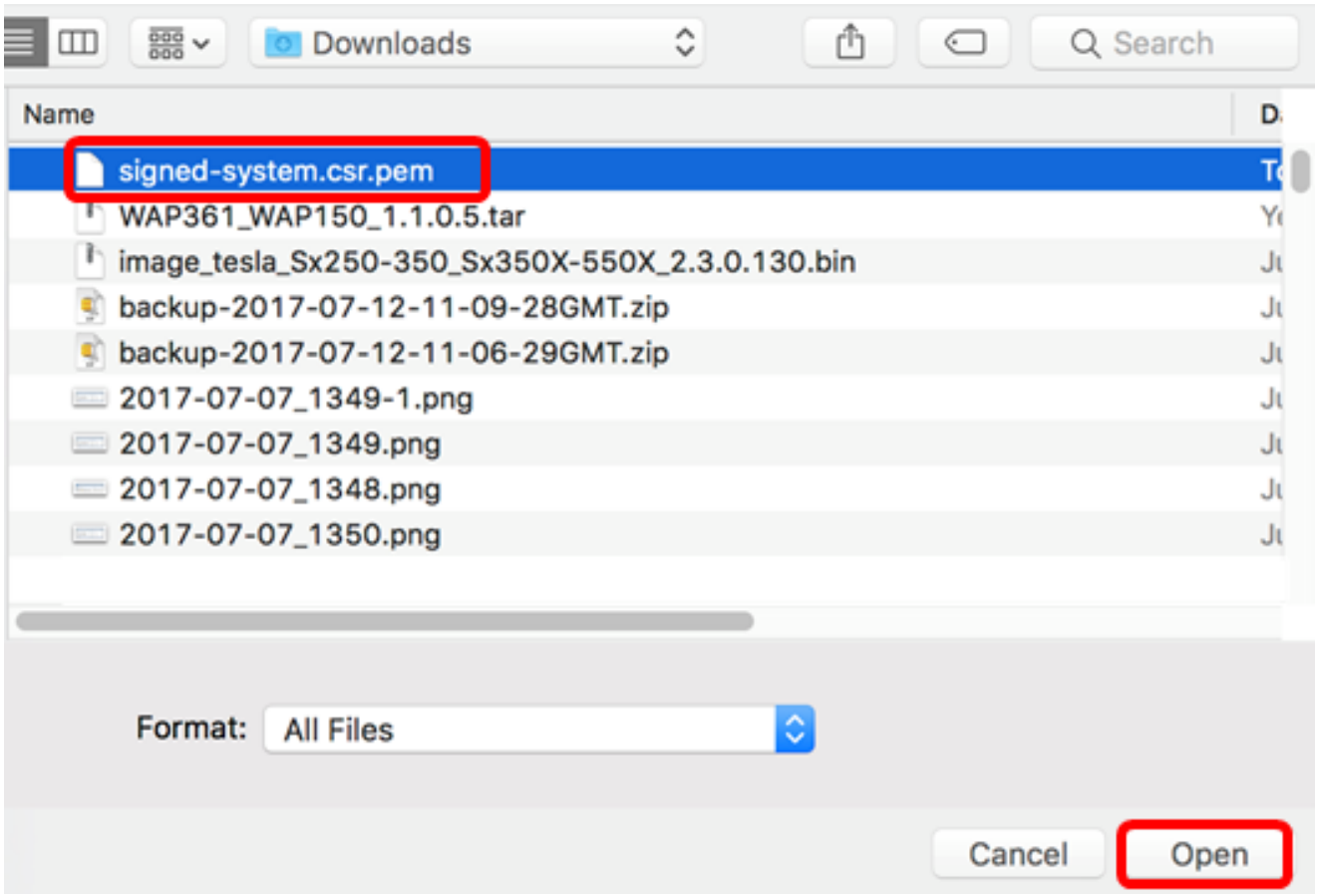


Schritt 3: Klicken Sie auf das Optionsfeld **UploadCert**.



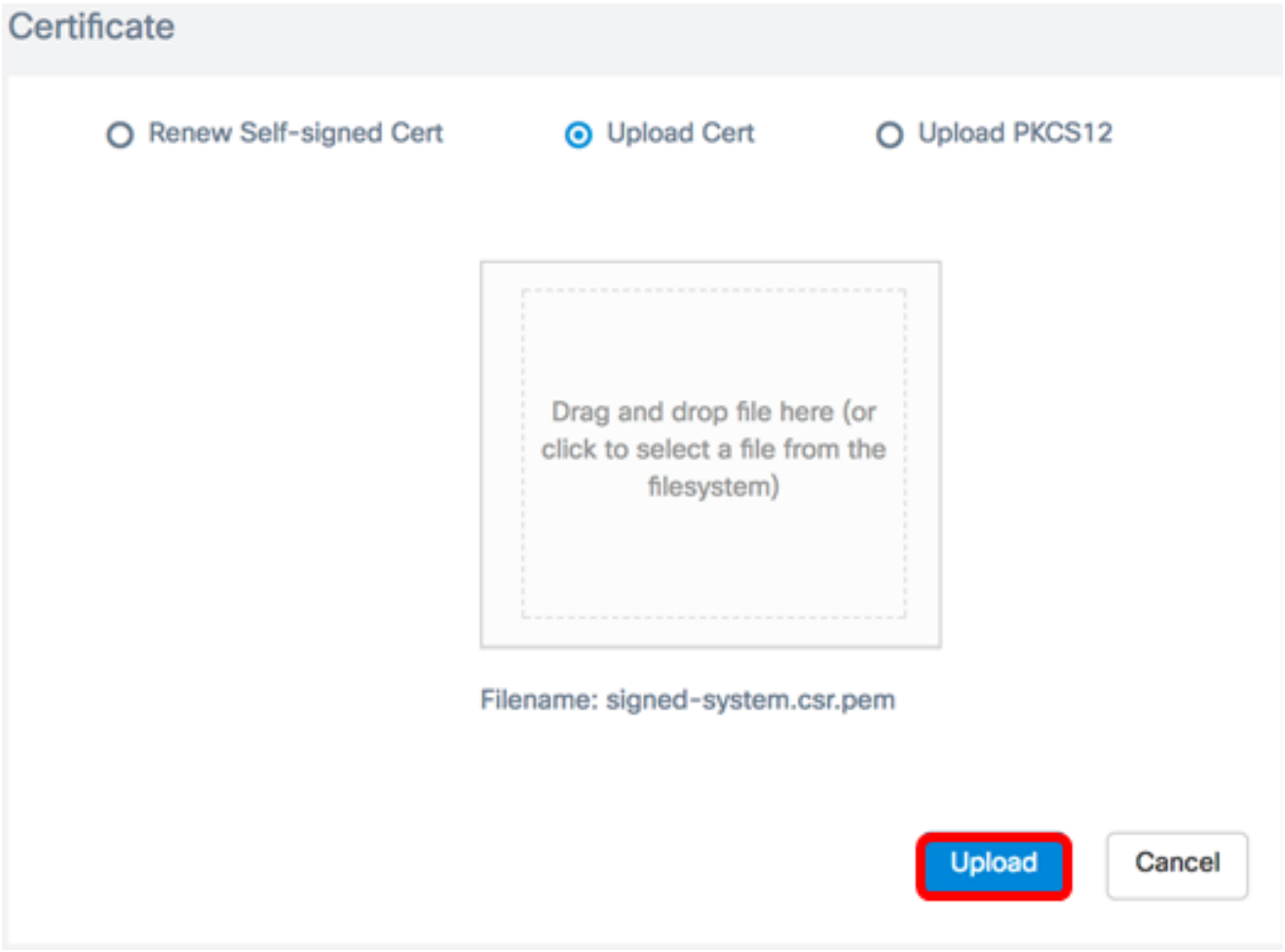
Hinweis: Alternativ können Sie ein Zertifikat mit dem zugehörigen privaten Schlüssel im PKCS#12-Format hochladen, indem Sie das Optionsfeld **PKCS12 hochladen** aktivieren. Das Kennwort zum Entsperren der Datei sollte im dafür vorgesehenen Feld *Kennwort* angegeben werden.

Schritt 4: Legen Sie das signierte Zertifikat im Zielbereich ab, oder klicken Sie auf den Zielbereich, um das Dateisystem zu durchsuchen, und klicken Sie dann auf **Öffnen**. Die Datei sollte im .pem-Format vorliegen.



Hinweis: In diesem Beispiel wird signed-system.csr.pem verwendet.

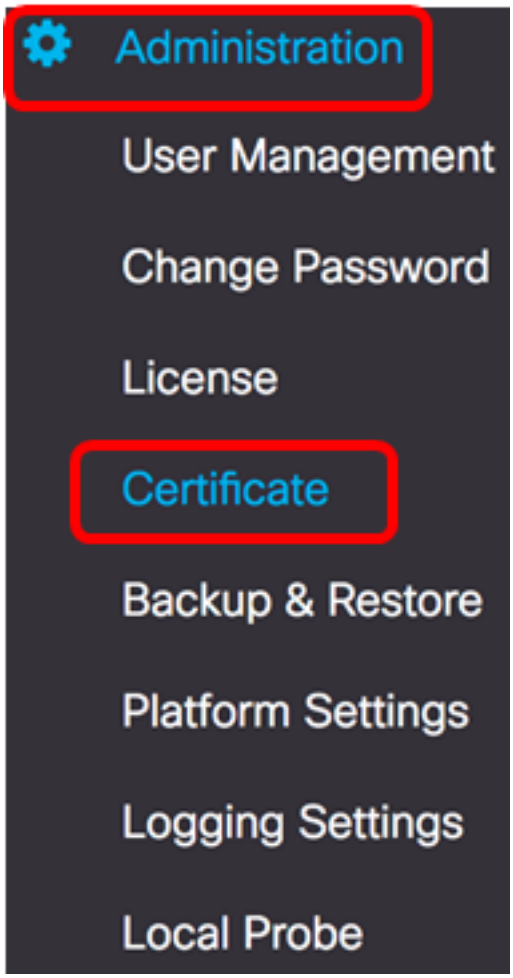
Schritt 5: Klicken Sie auf **Hochladen**.



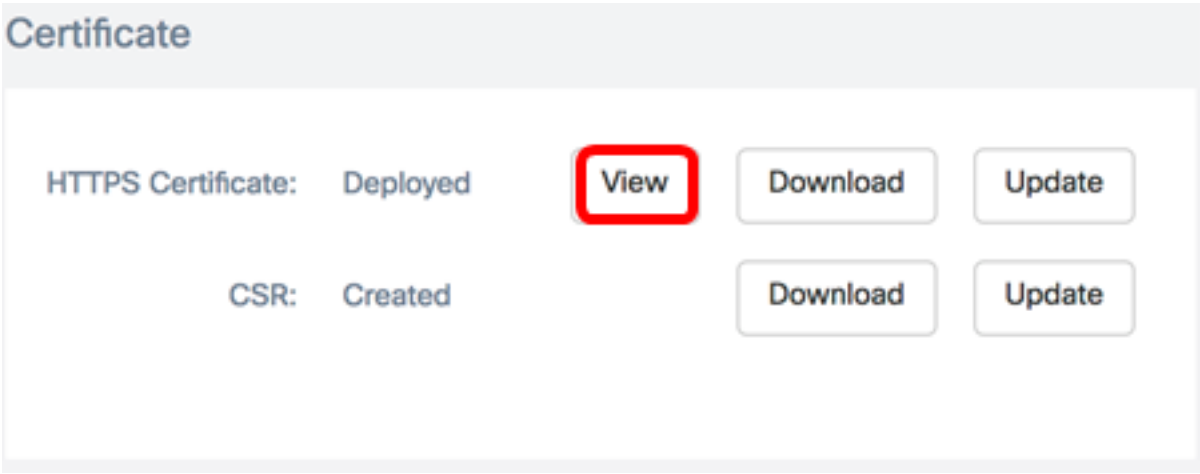
Sie sollten jetzt ein signiertes Zertifikat erfolgreich in den FindIT Network Manager hochgeladen haben.

Aktuelles Zertifikat verwalten

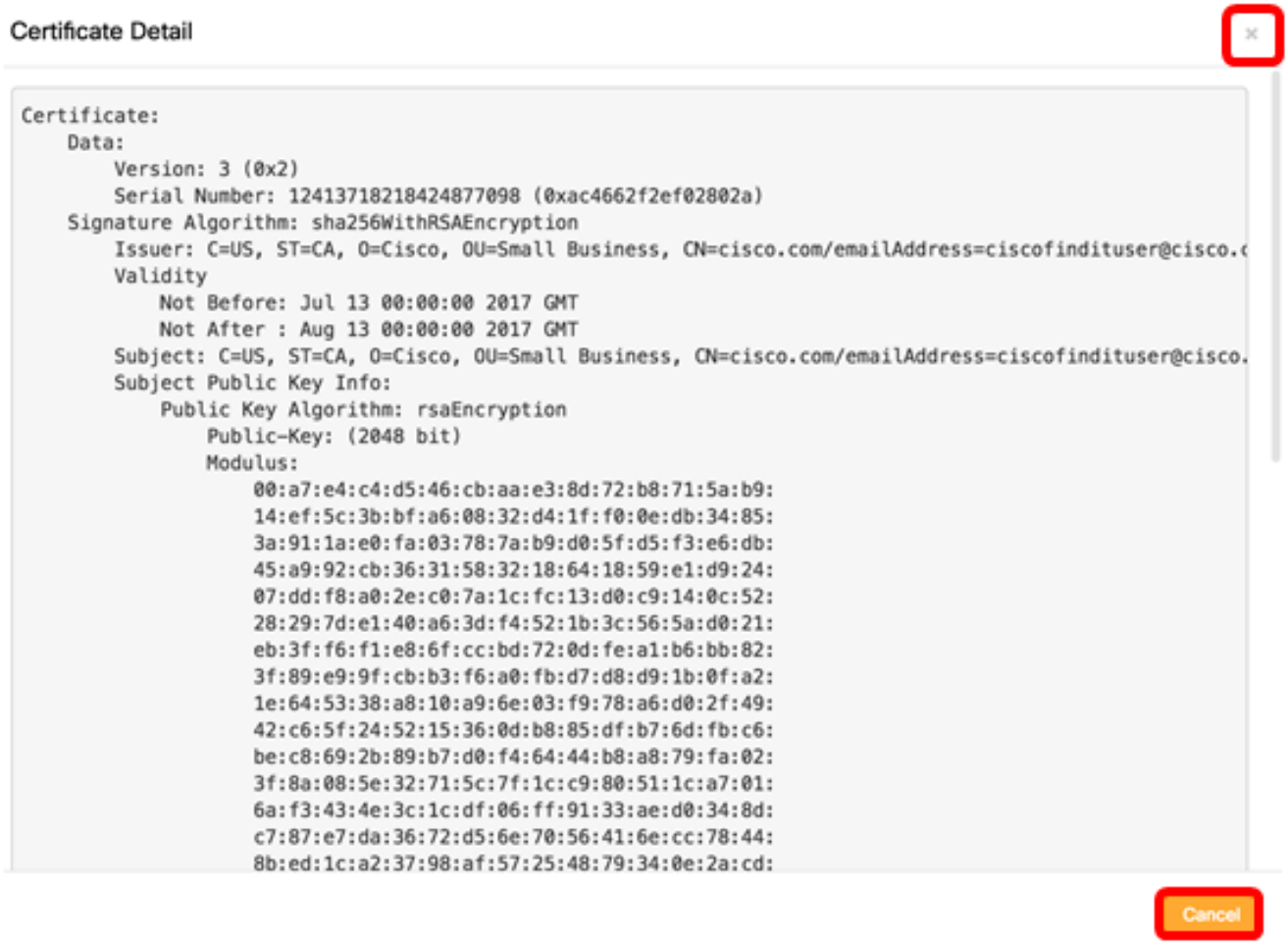
Schritt 1: Melden Sie sich bei der Verwaltungs-GUI Ihres FindIT Network Manager an, und wählen Sie dann **Administration > Certificate aus**.



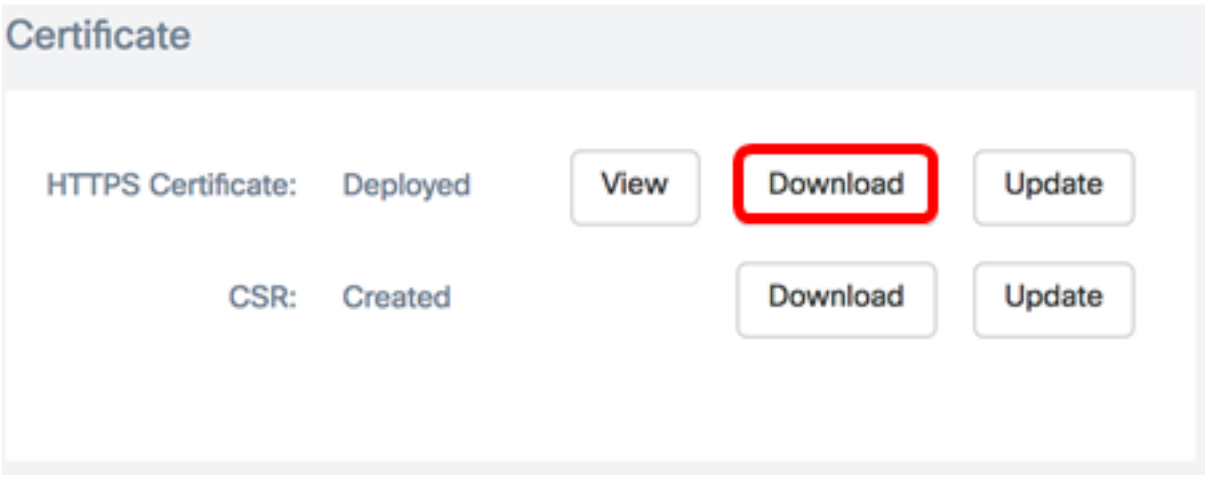
Schritt 2: Klicken Sie im Bereich HTTPS-Zertifikat auf die Schaltfläche **Anzeigen**.



Schritt 3: Das aktuelle Zertifikat wird in einem neuen Browserfenster im Textformat angezeigt. Klicken Sie auf die Schaltfläche **x** oder **Cancel (Abbrechen)**, um das Fenster zu schließen.



Schritt 4: (Optional) Um eine Kopie des aktuellen Zertifikats herunterzuladen, klicken Sie im Bereich für das HTTPS-Zertifikat auf die Schaltfläche **Download**.



Sie sollten jetzt das aktuelle Zertifikat erfolgreich auf Ihrem FindIT Network Manager verwalten.