

# FindIT Network Manager에서 인증서 관리

## 목표

디지털 인증서는 인증서의 명명된 주체에 의해 공개 키의 소유권을 인증합니다. 이렇게 하면 신뢰 당사자가 인증된 공개 키에 해당하는 개인 키가 만든 서명 또는 어설션에 의존할 수 있습니다. 설치 시 FindIT Network Manager는 자체 서명 인증서를 생성하여 웹 및 서버와의 기타 통신을 보호합니다. 이 인증서를 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서로 바꿀 수 있습니다. 이렇게 하려면 CA에서 서명을 위해 CSR(Certificate Signing Request)을 생성해야 합니다.

또한 Manager와 완전히 독립적으로 인증서 및 해당 개인 키를 생성하도록 선택할 수 있습니다. 이 경우 업로드하기 전에 인증서와 개인 키를 PKCS(Public Key Cryptography Standards) #12 형식 파일로 결합할 수 있습니다.

FindIT Network Manager는 .pem 형식 인증서만 지원합니다. 다른 인증서 형식을 가져올 경우 CA에서 .pem 형식 인증서에 대한 형식 또는 요청을 다시 변환해야 합니다.

이 문서에서는 FindIT Network Manager에서 인증서를 관리하는 방법에 대한 지침을 제공합니다.

## 적용 가능한 디바이스

- IT 네트워크 관리자 찾기

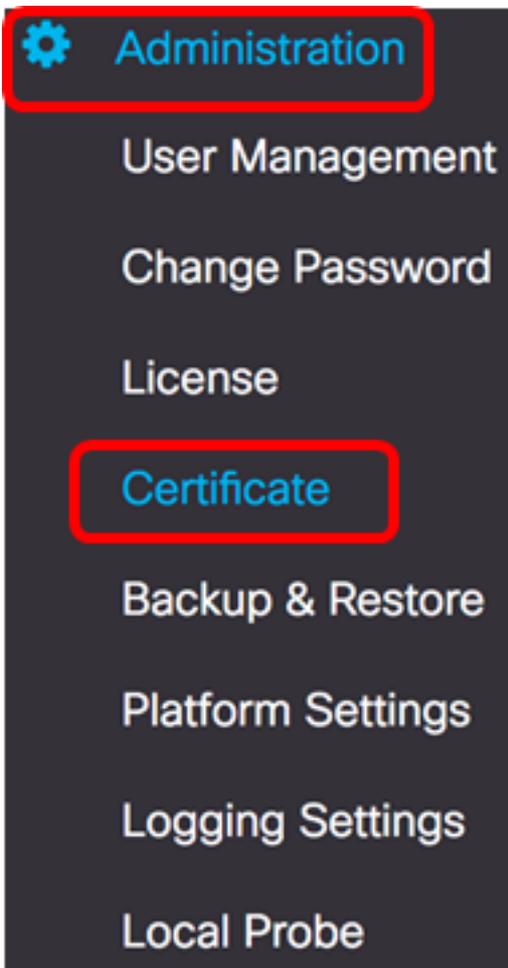
## 소프트웨어 버전

- 1.1

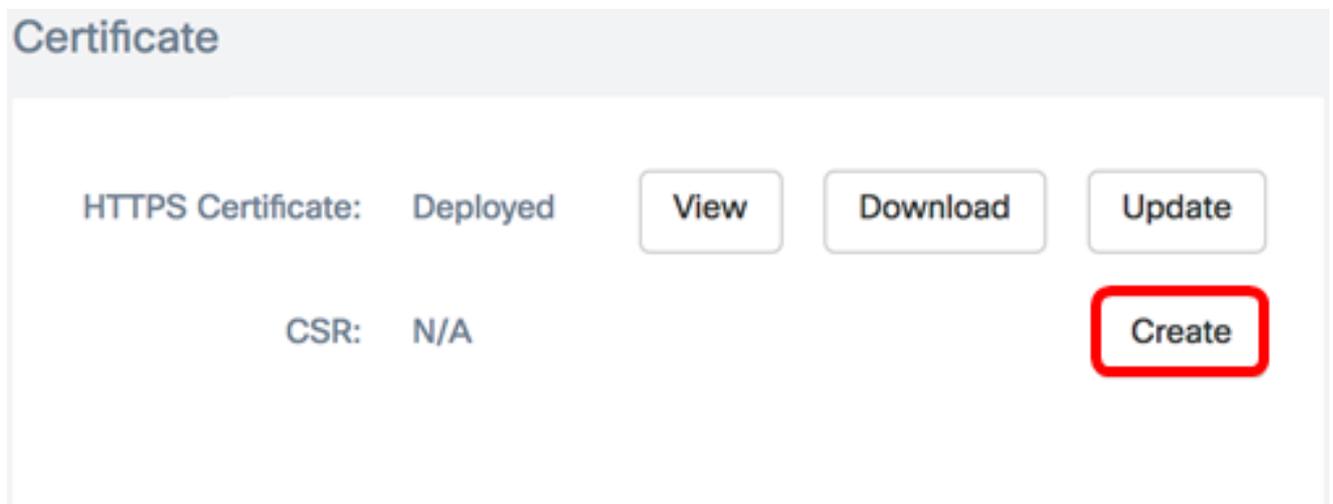
## FindIT Network Manager에서 인증서 관리

### CSR 생성

1단계. FindIT Network Manager의 Administration GUI에 로그인한 다음 **Administration > Certificate**를 선택합니다.



2단계. CSR 영역에서 **Create** 버튼을 클릭합니다.



인증서 양식에 입력한 값은 CSR을 구성하는 데 사용되며 CA에서 수신하는 서명된 인증서에 포함됩니다.

**3단계.** IP 주소 또는 도메인 이름을 Full qualified *domain name* 필드에 입력합니다. 이 예에서는 hostname.cisco.com이 사용됩니다.



4단계. 국가 필드에 국가 코드를 입력합니다. 이 예에서는 US가 사용됩니다.

Country  ✓

5단계. 상태 필드에 상태 코드를 입력합니다. 이 예에서는 CA가 사용됩니다.

State  ✓

6단계. 도시 필드에 도시를 입력합니다. 이 예에서는 Irvine이 사용됩니다.

City  ✓

7단계. 조직 필드에 조직명을 입력합니다. 이 예에서는 Cisco가 사용됩니다.

Org  ✓

8단계. 조직 단위 필드에 조직 단위를 입력합니다. 이 예에서는 Small Business가 사용됩니다.

Org Units  ✓

9단계. 이메일 필드에 이메일 주소를 입력합니다. 이 예에서는 [ciscofindituser@cisco.com](mailto:ciscofindituser@cisco.com)를 입력합니다.

Email  ✓

10단계. 저장을 클릭합니다.

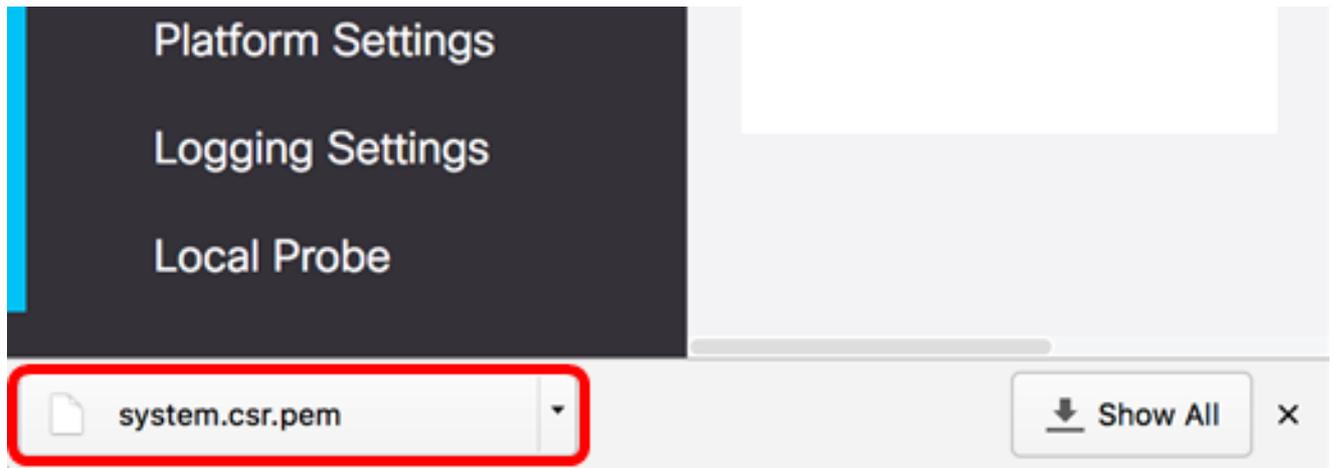
Certificate

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).

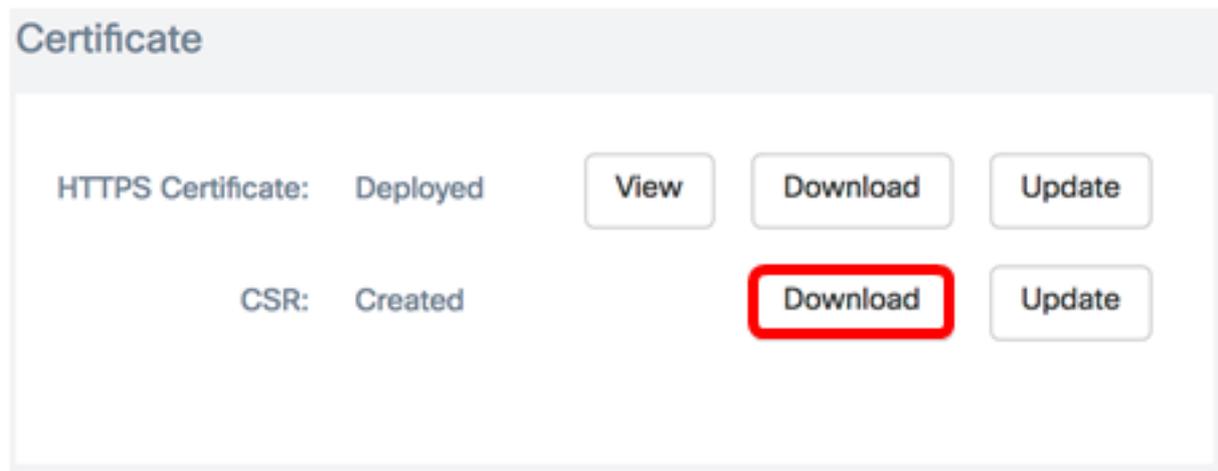
Full qualified domain name	<input type="text" value="hostname.cisco.com"/> ✓
Country	<input type="text" value="US"/> ✓
State	<input type="text" value="CA"/> ✓
City	<input type="text" value="Irvine"/> ✓
Org	<input type="text" value="Cisco"/> ✓
Org Units	<input type="text" value="Small Business"/> ✓
Email	<input type="text" value="ciscofindituser@cisco.com"/> ✓

CSR 파일이 자동으로 컴퓨터에 다운로드됩니다. 이 예에서는 system.csr.pem 파일이 생성됨

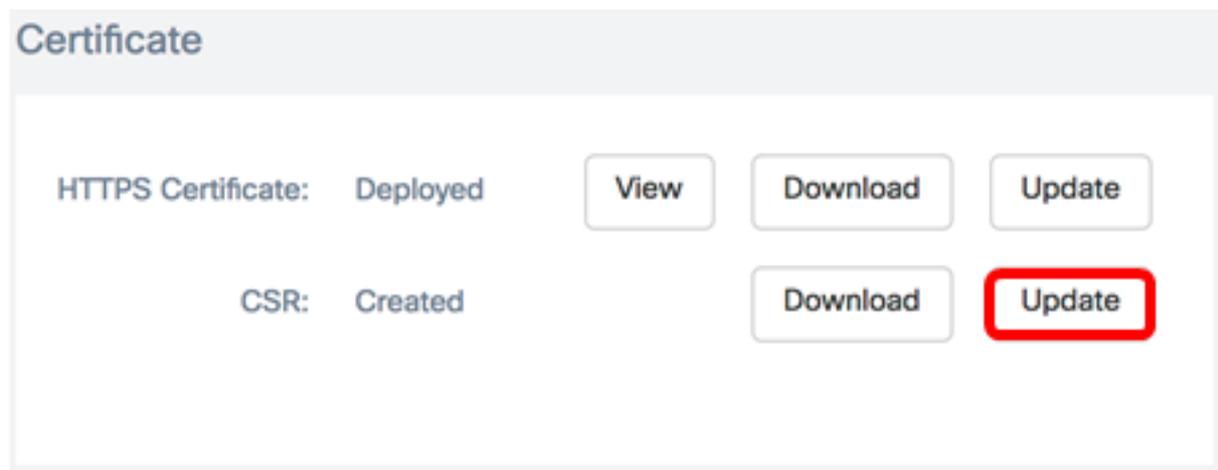
니다.



11단계. (선택 사항) CSR 영역에서 상태가 N/A에서 Created로 업데이트됩니다. 생성된 CSR을 다운로드하려면 **Download** 버튼을 클릭합니다.



12단계(선택 사항) 생성된 CSR을 업데이트하려면 **Update(업데이트)** 버튼을 클릭한 다음 [3단계](#)로 돌아갑니다.

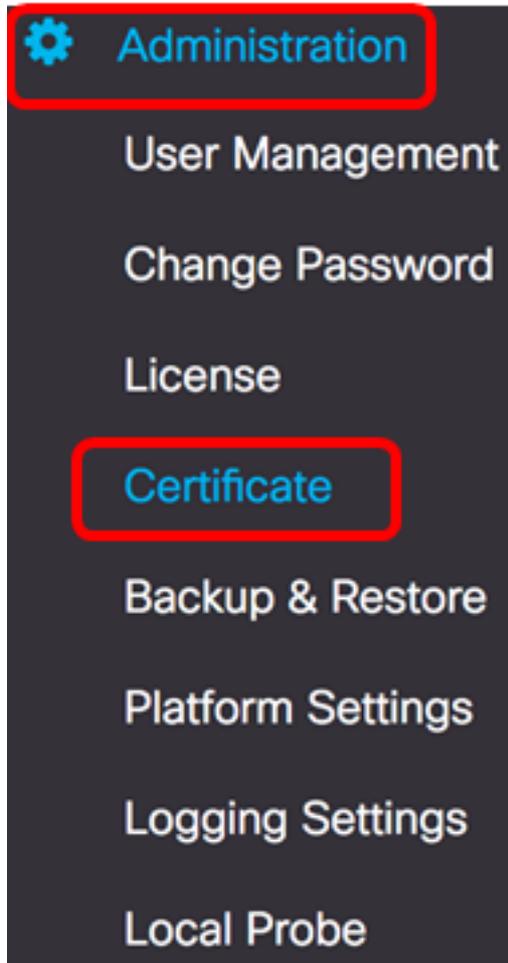


이제 FindIT Network Manager에서 CSR을 생성했습니다. 이제 다운로드한 CSR 파일을 CA에 보낼 수 있습니다.

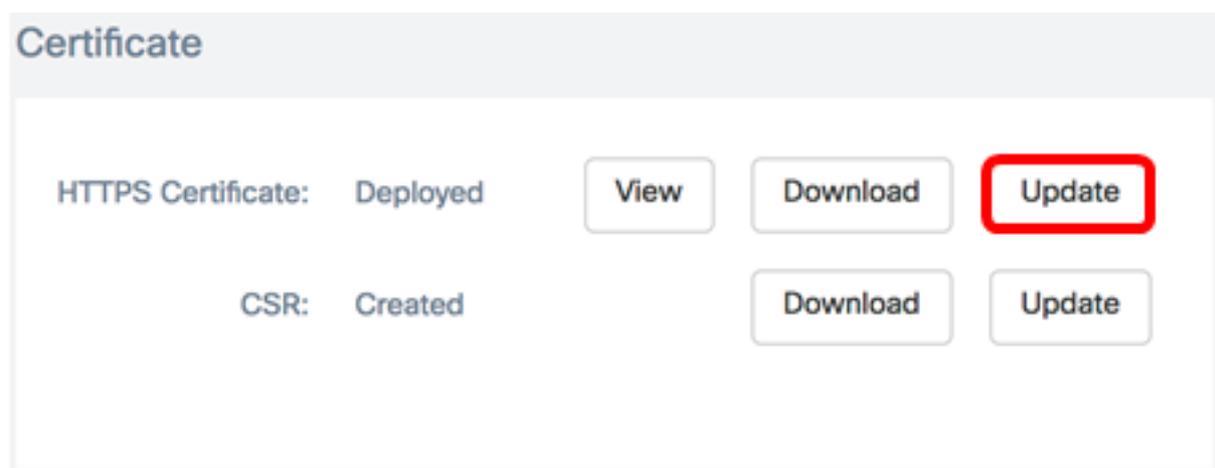
## CA에서 서명된 인증서 업로드

CA에서 서명된 CSR을 수신하면 이제 Manager에 업로드할 수 있습니다.

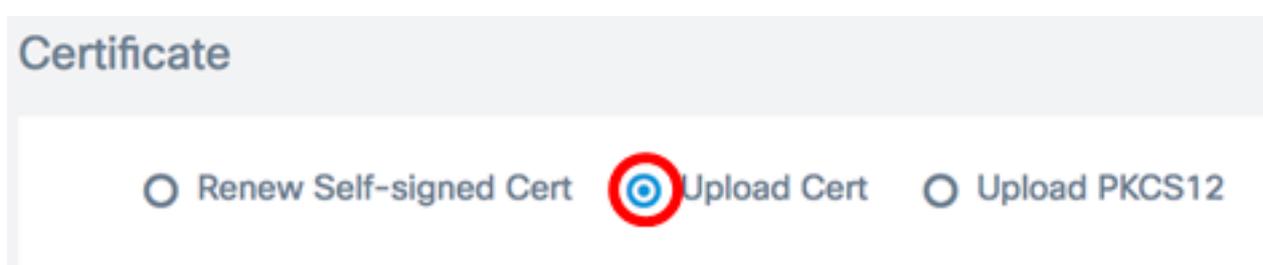
1단계. FindIT Network Manager의 Administration GUI에 로그인한 다음 **Administration > Certificate**를 선택합니다.



2단계. HTTPS Certificate(HTTPS 인증서) 영역에서 Update(업데이트) 버튼을 클릭합니다.



3단계. UploadCert 라디오 버튼을 클릭합니다.

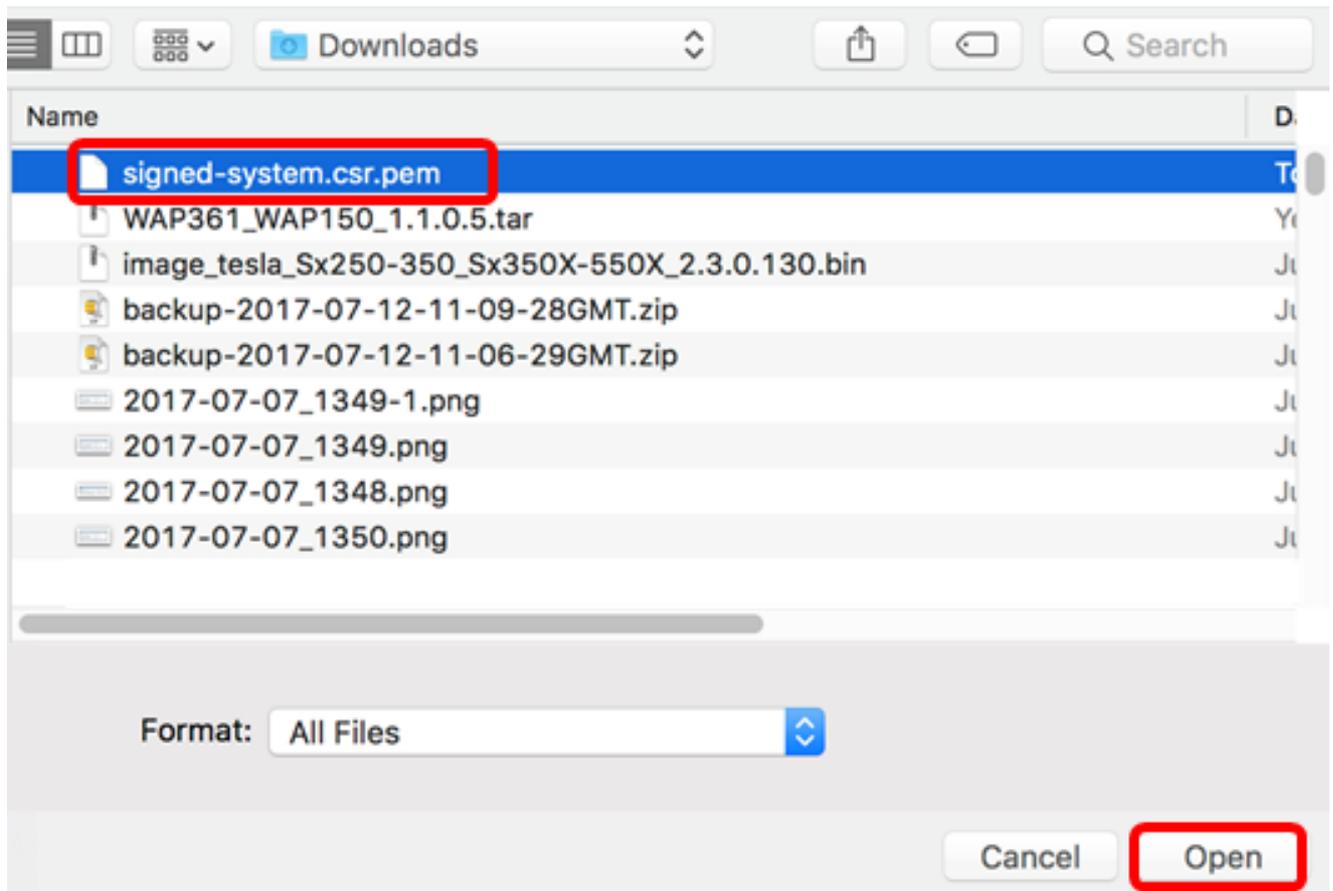


**참고:**또는 Upload PKCS12 라디오 버튼을 선택하여 연결된 개인 키가 있는 인증서를 PKCS#12 형식으로 업로드할 수 있습니다.파일 잠금을 해제할 비밀번호를 *Password* 필드에 지정해야 합니다.

Upload Cert     Upload PKCS12

Password:

4단계. 대상 영역에 서명된 인증서를 삭제하거나 대상 영역을 클릭하여 파일 시스템을 찾은 다음 열기를 클릭합니다.파일은 .pem 형식이어야 합니다.



**참고:**이 예에서는 signed-system.csr.pem이 사용됩니다.

5단계. Upload(업로드)를 클릭합니다.

**Certificate**

Renew Self-signed Cert     Upload Cert     Upload PKCS12

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

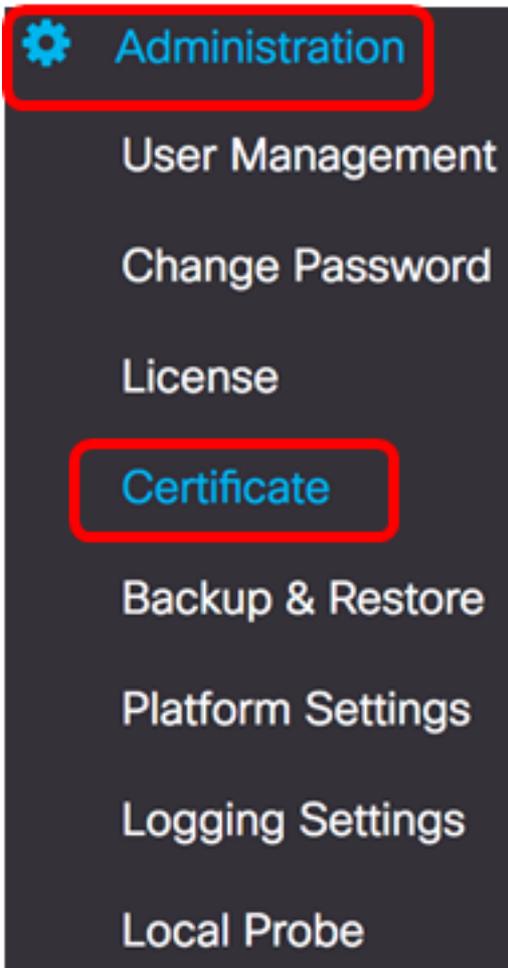
Filename: signed-system.csr.pem

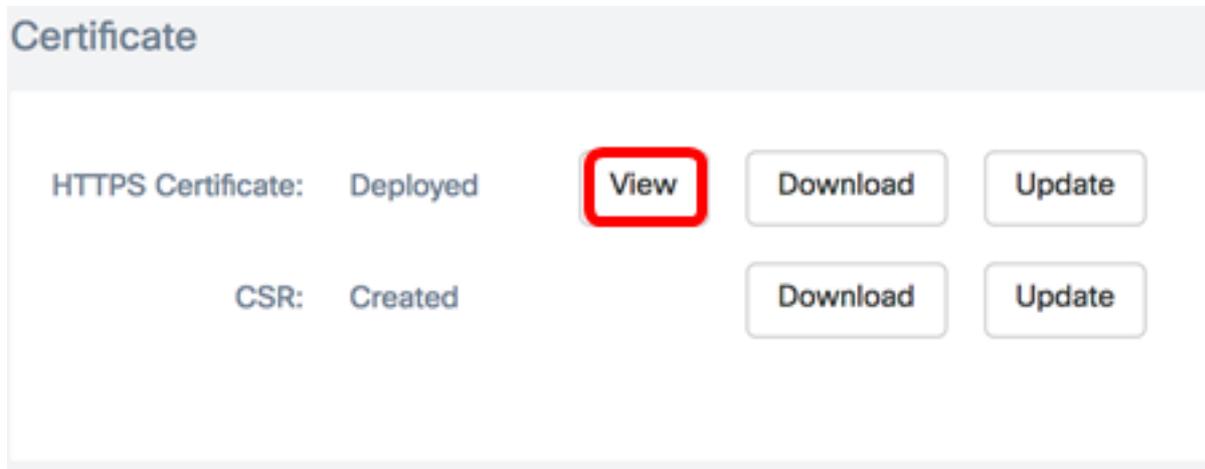
이제 서명된 인증서를 FindIT Network Manager에 업로드해야 합니다.

## 현재 인증서 관리

1단계. FindIT Network Manager의 Administration GUI에 로그인한 다음 **Administration > Certificate**를 선택합니다.



2단계. HTTPS Certificate(HTTPS 인증서) 영역에서 View(보기) 버튼을 클릭합니다.



3단계. 현재 인증서가 새 브라우저 창에 일반 텍스트 형식으로 표시됩니다.x 또는 취소 버튼을 클릭하여 창을 닫습니다.

```

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=ciscofindituser@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=ciscofindituser@cisco.c
    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

4단계. (선택 사항) 현재 인증서의 사본을 다운로드하려면 HTTPS Certificate(HTTPS 인증서) 영역에서 Download(다운로드) 버튼을 클릭합니다.

### Certificate

HTTPS Certificate:	Deployed	<a href="#">View</a>	<a href="#">Download</a>	<a href="#">Update</a>
CSR:	Created	<a href="#">Download</a>	<a href="#">Update</a>	

이제 FindIT Network Manager에서 현재 인증서를 성공적으로 관리했어야 합니다.