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

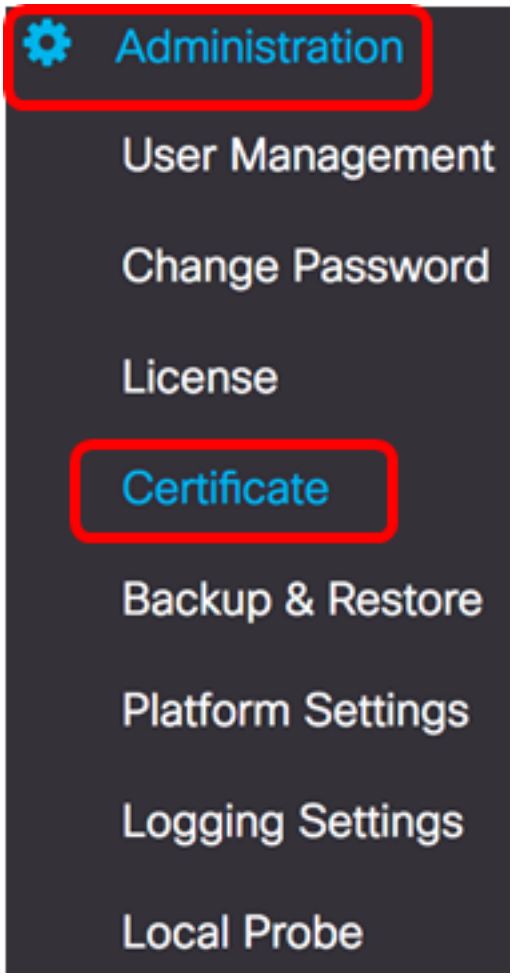
소프트웨어 버전

- 1.1

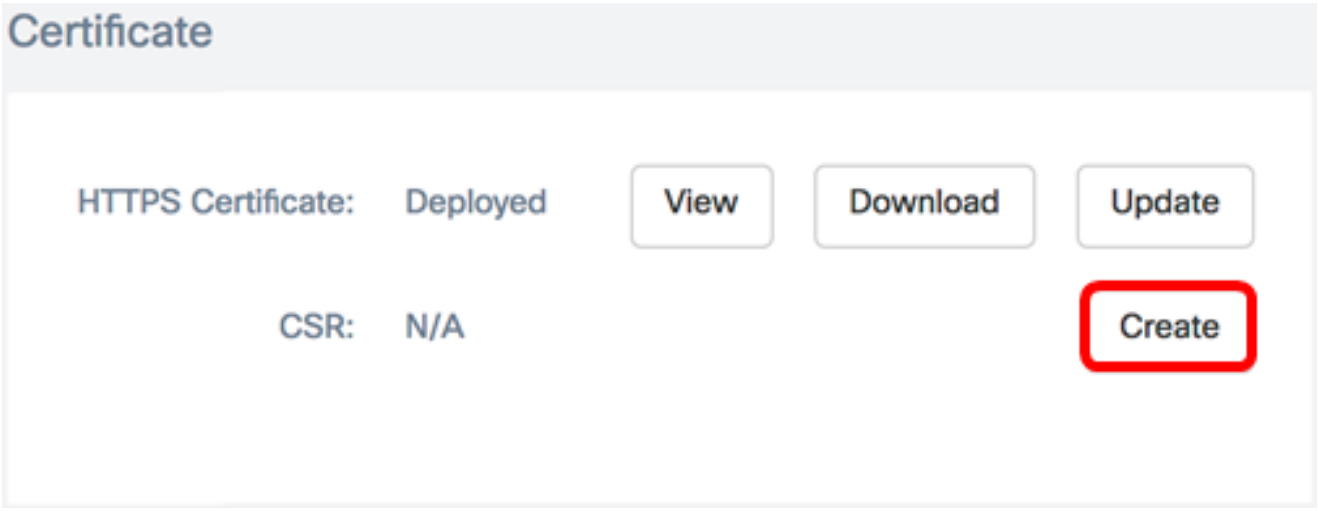
FindIT Network Manager에서 인증서 관리

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* 필드*에* 입력합니다.이 예에서는 hostname.cisco.com이 사용됩니다.

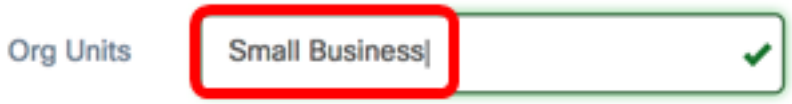
4단계. 국가 필드에 국가 코드를 *입력합니다*.이 예에서는 US가 사용됩니다.

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

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

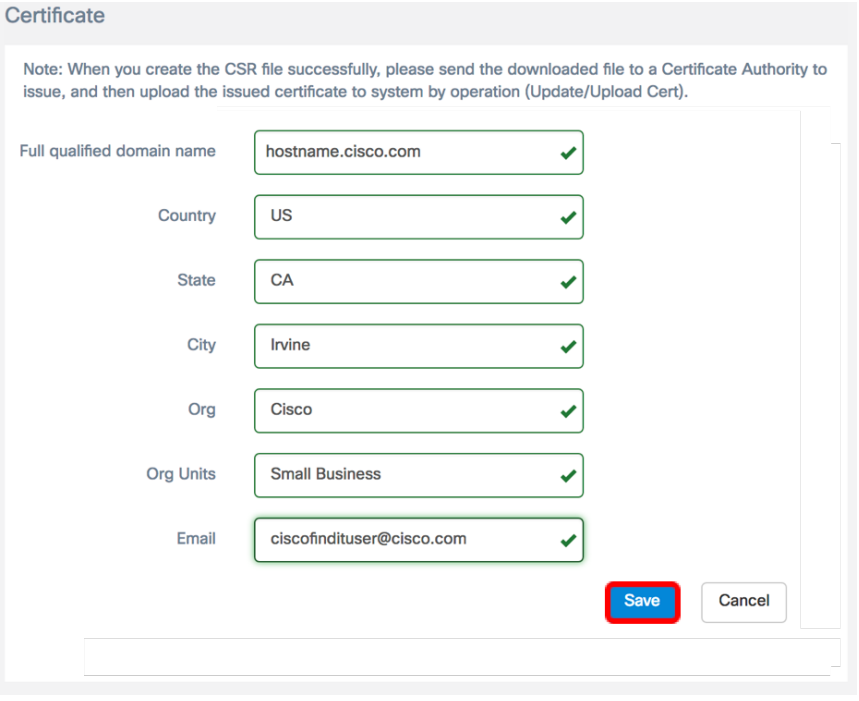
7단계. 조직 필드에 조직명을 *입력합니다*.이 예에서는 Cisco가 사용됩니다.

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



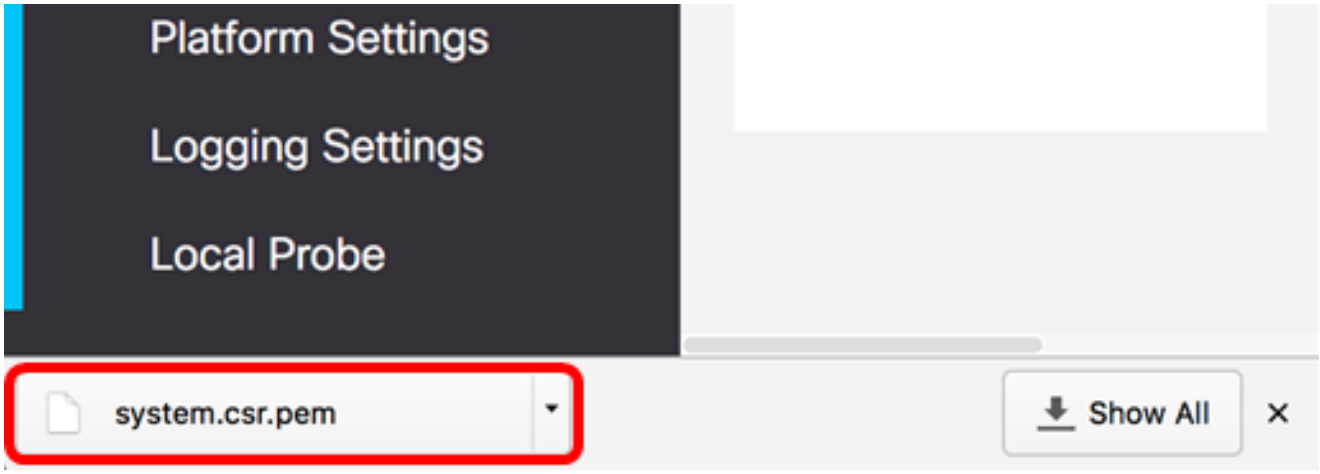
9단계. *이메일* 필드에 이메일 주소를 입력합니다.이 예에서는 ciscofindituser@cisco.com를 입력합니다.

10단계. 저장을 **클릭합니다**.

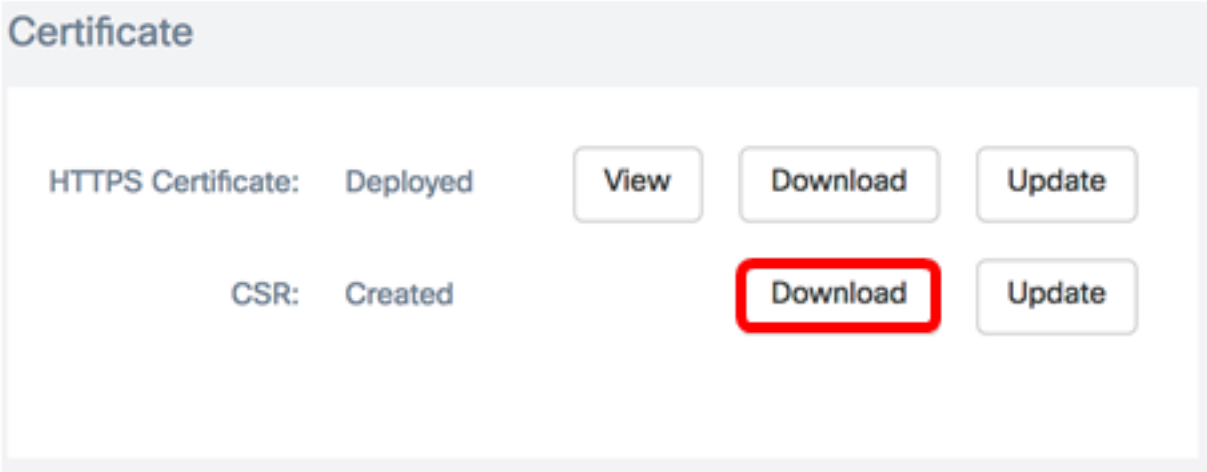


CSR 파일이 자동으로 컴퓨터에 다운로드됩니다.이 예에서는 system.csr.pem 파일이 생성됩

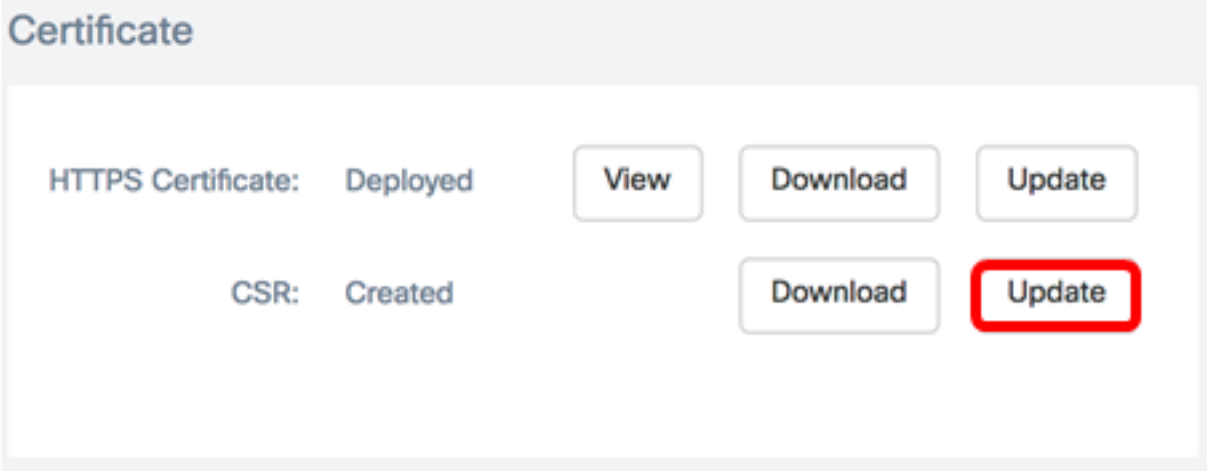
니다.



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 3단계로 돌아갑니다.

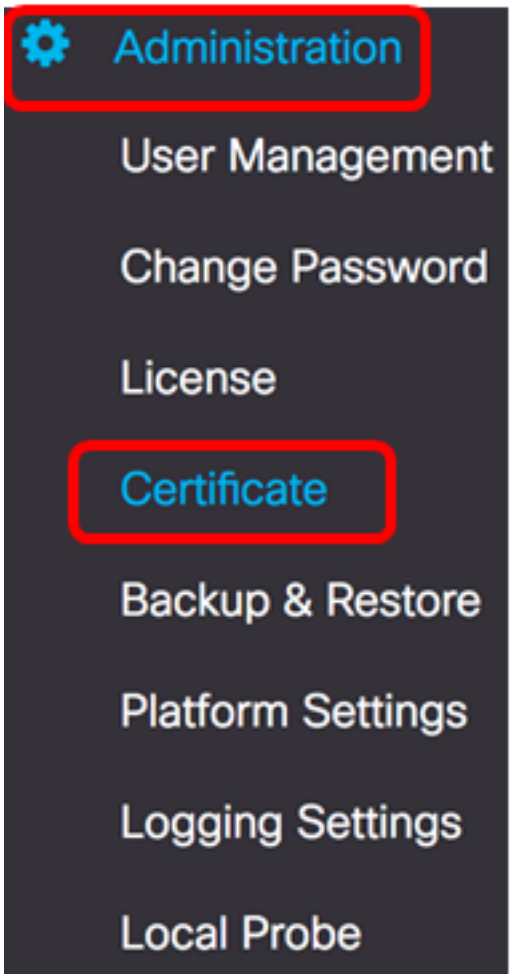


이제 FindIT Network Manager에서 CSR을 생성했습니다.이제 다운로드한 CSR 파일을 CA에 보낼 수 있습니다.

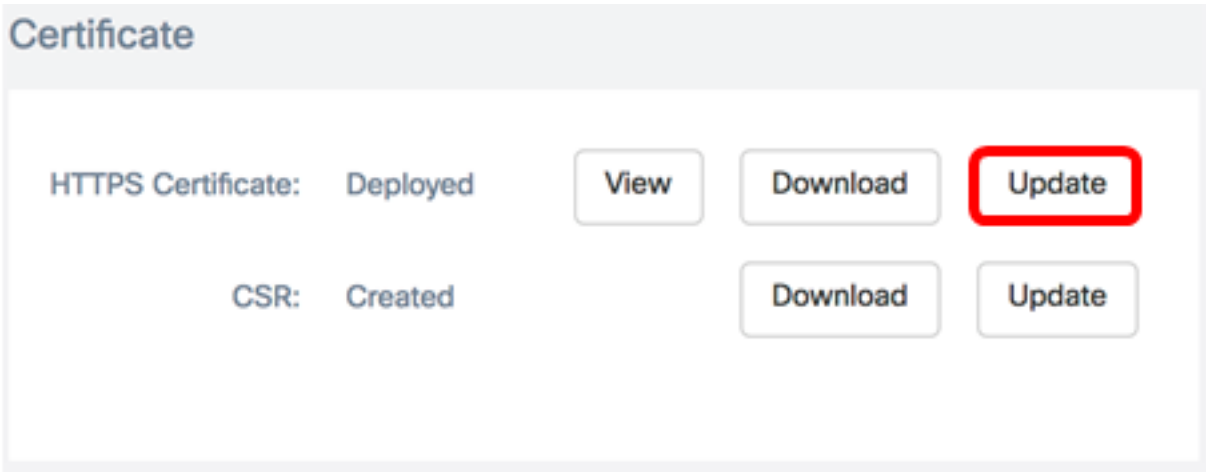
CA에서 서명된 인증서 업로드

CA에서 서명된 CSR을 수신하면 이제 Manager에 업로드할 수 있습니다.

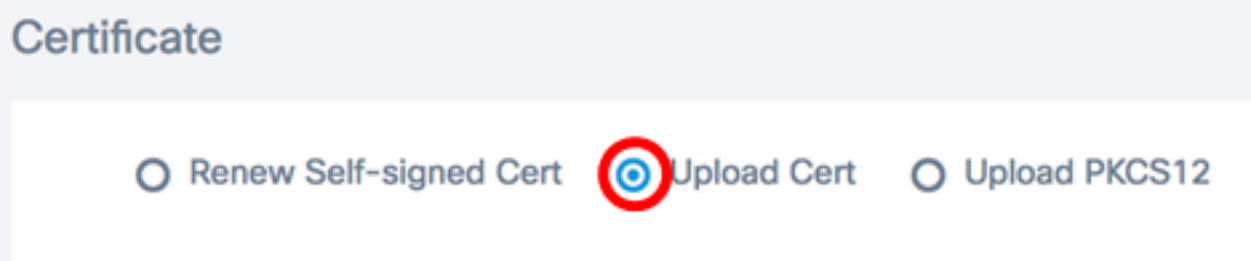
1단계. FindIT Network Manager의 Administration GUI에 로그인한 다음 **Administration > Certificate**를 선택합니다.



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

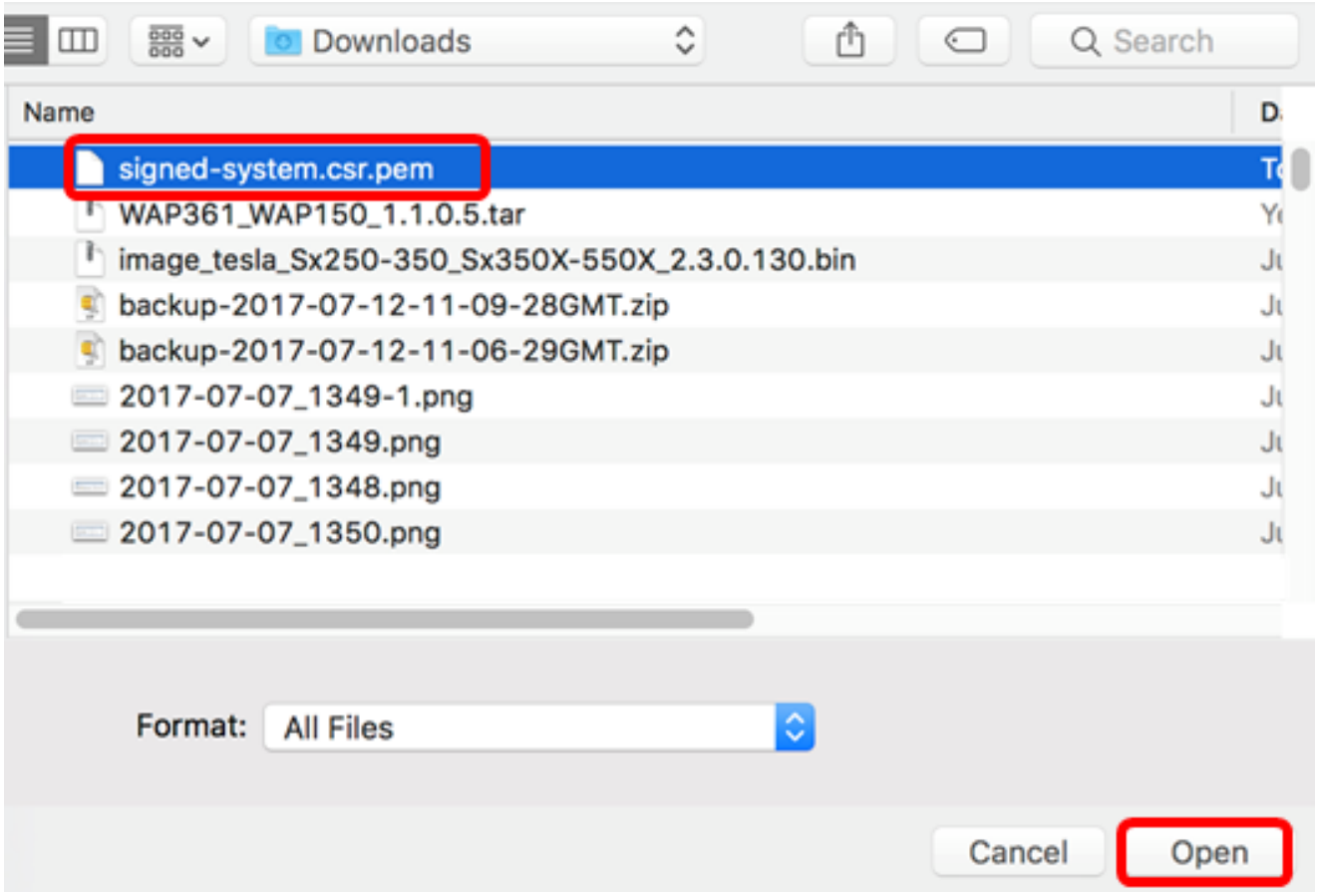


3단계. UploadCert 라디오 버튼을 클릭합니다.



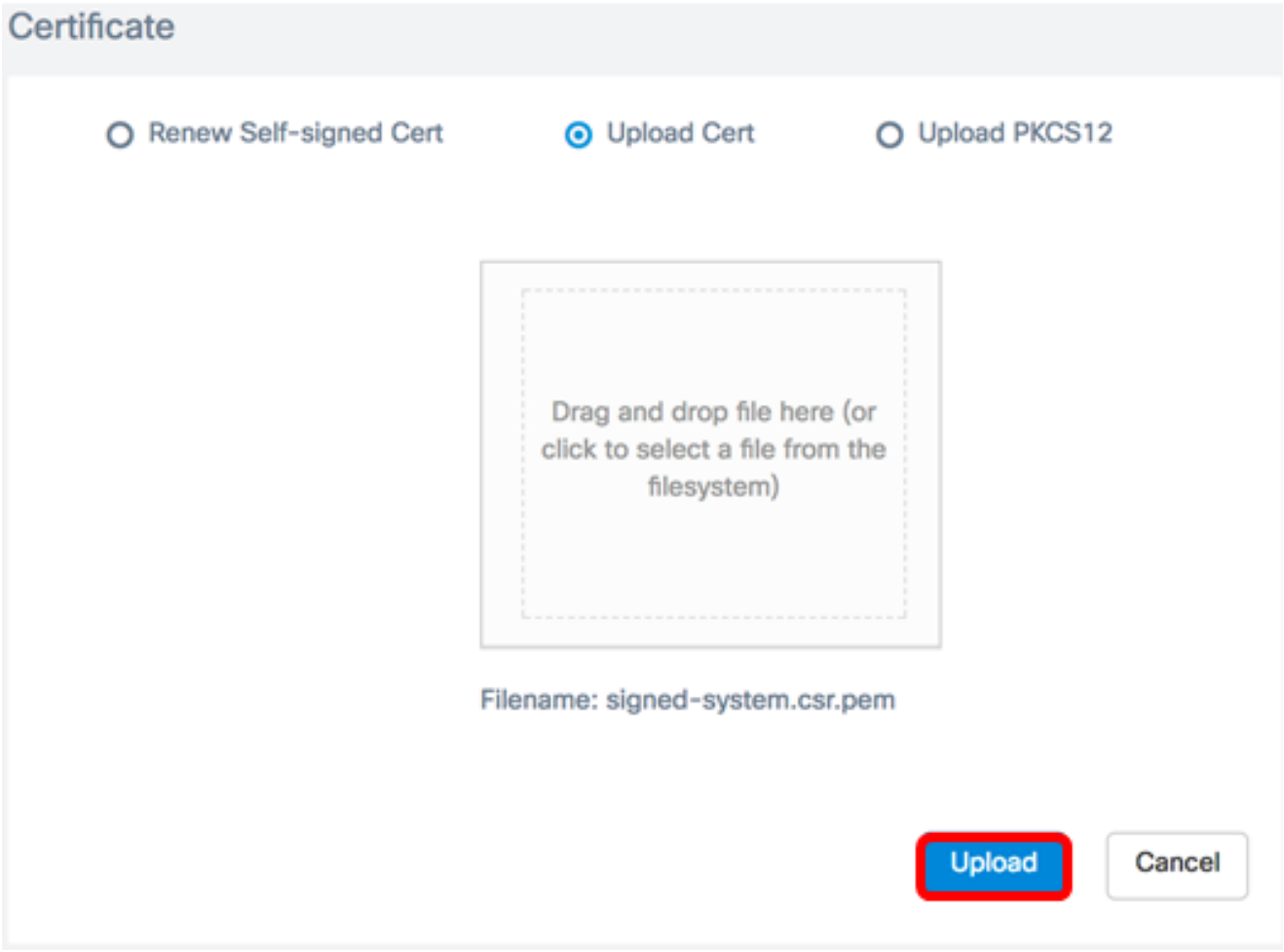
참고:또는 Upload PKCS**12** 라디오 버튼을 선택하여 연결된 개인 키가 있는 인증서를 PKCS#12 형식으로 업로드할 수 있습니다.파일 잠금을 해제할 비밀번호를 *Password* 필드에 지정해야 합니다.

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



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

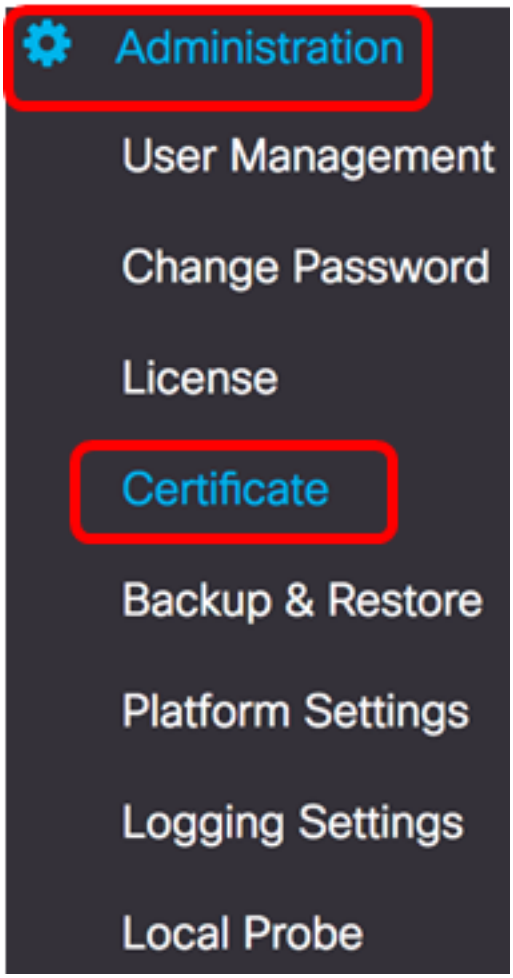
5단계. Upload(**업로드)를 클릭합니다**.



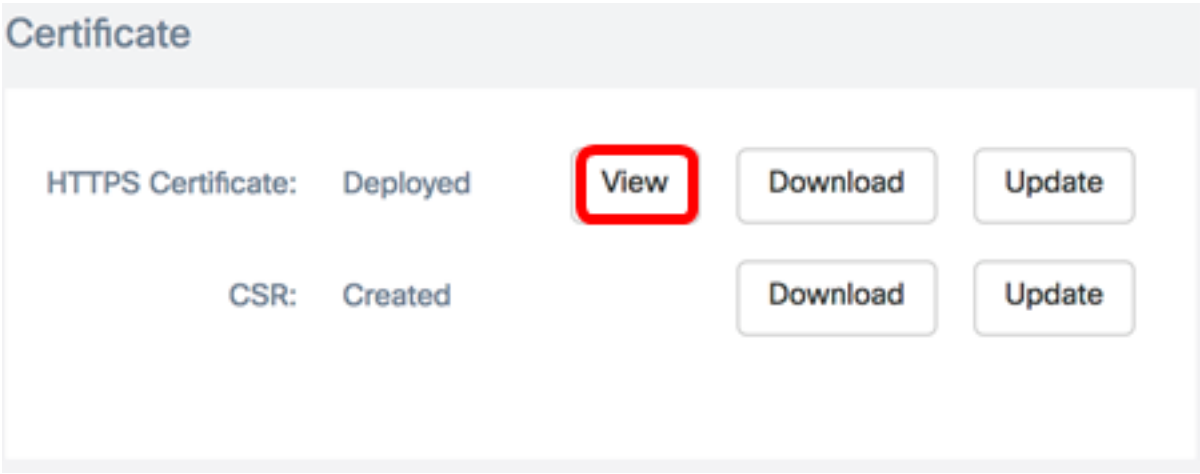
이제 서명된 인증서를 FindIT Network Manager에 업로드해야 합니다.

현재 인증서 관리

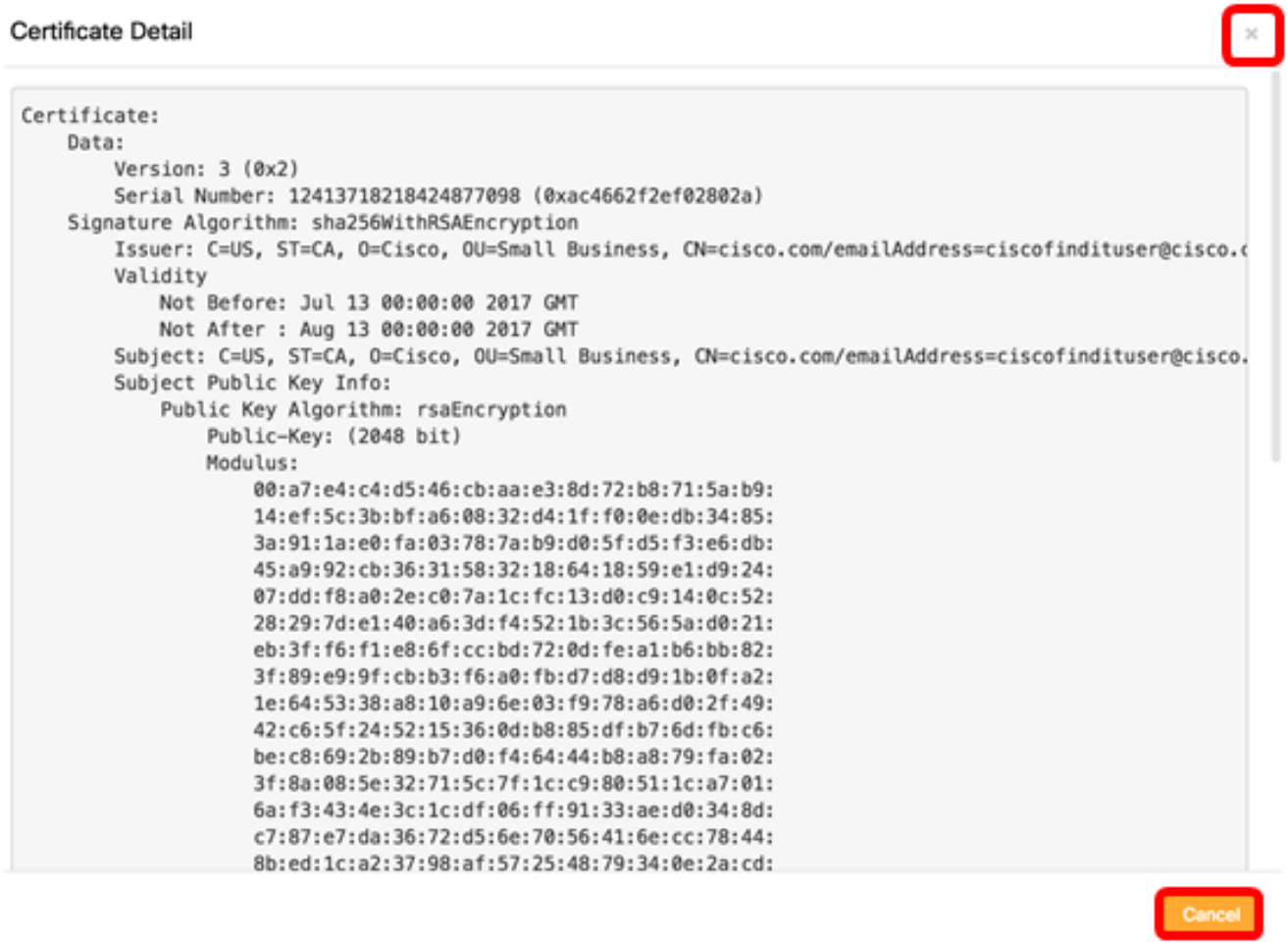
1단계. FindIT Network Manager의 Administration GUI에 로그인한 다음 **Administration > Certificate**를 선택합니다.



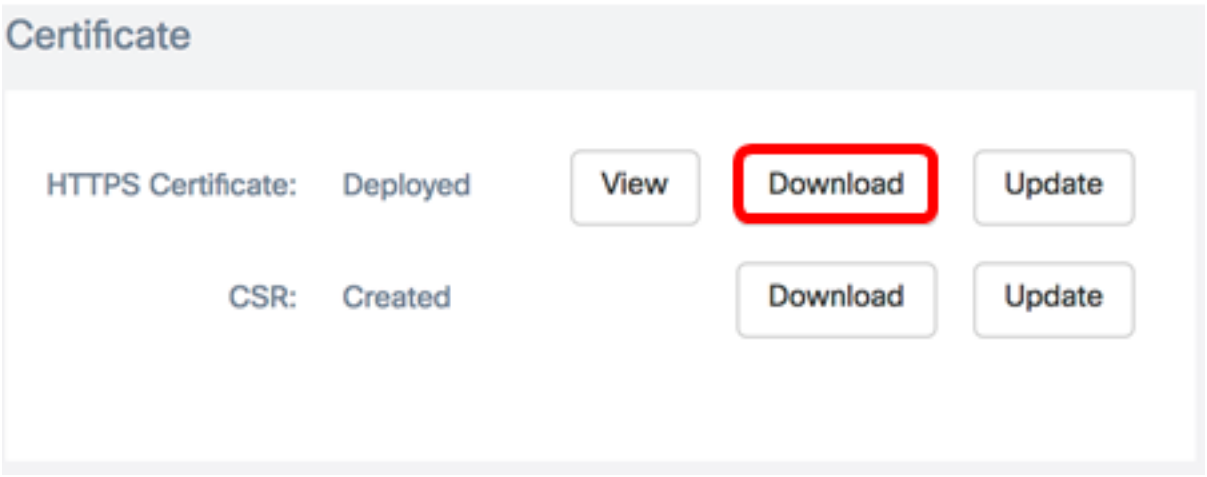
2단계. HTTPS Certificate(HTTPS 인증서) 영역에서 View(**보기**) 버튼을 클릭합니다.



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



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



이제 FindIT Network Manager에서 현재 인증서를 성공적으로 관리했어야 합니다.