

在FindIT网络管理器上管理证书

目标

数字证书通过证书的指定主题对公钥的所有权进行认证。这允许依赖方依赖由私钥所作的签名或断言，该私钥对应于经认证的公钥。安装后，FindIT Network Manager会生成自签名证书，以保护Web和与服务器的其他通信。您可以选择将此证书替换为由受信任证书颁发机构(CA)签名的证书。为此，您需要生成证书签名请求(CSR)以供CA签名。

您还可以选择生成完全独立于Manager的证书和相应的私钥。如果是，您可以在上传之前将证书和私钥合并到公钥加密标准(PKCS)#12格式文件中。

FindIT Network Manager仅支持.pem格式证书。如果您获得其他证书格式，则需要从CA再次转换.pem格式证书的格式或请求。

本文提供有关如何在FindIT Network Manager上管理证书的说明。

适用设备

- FindIT网络管理器

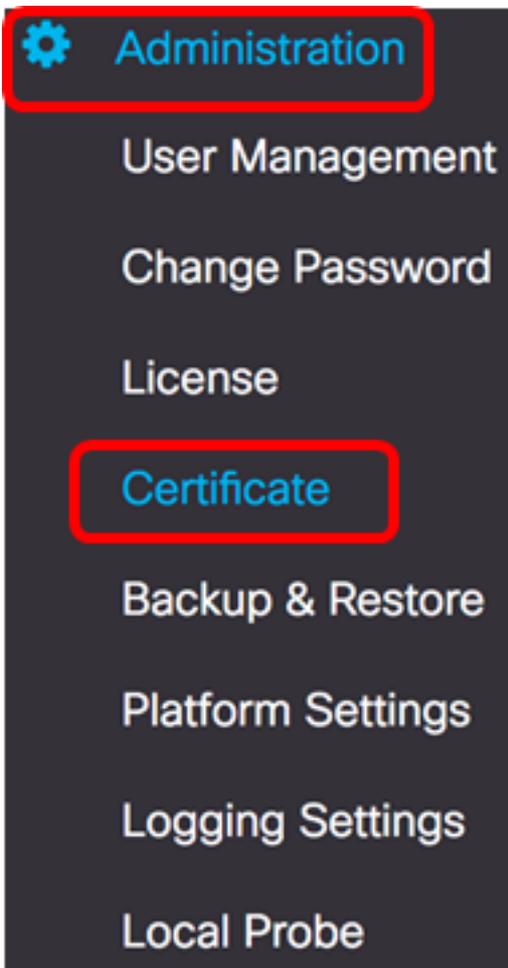
软件版本

- 1.1

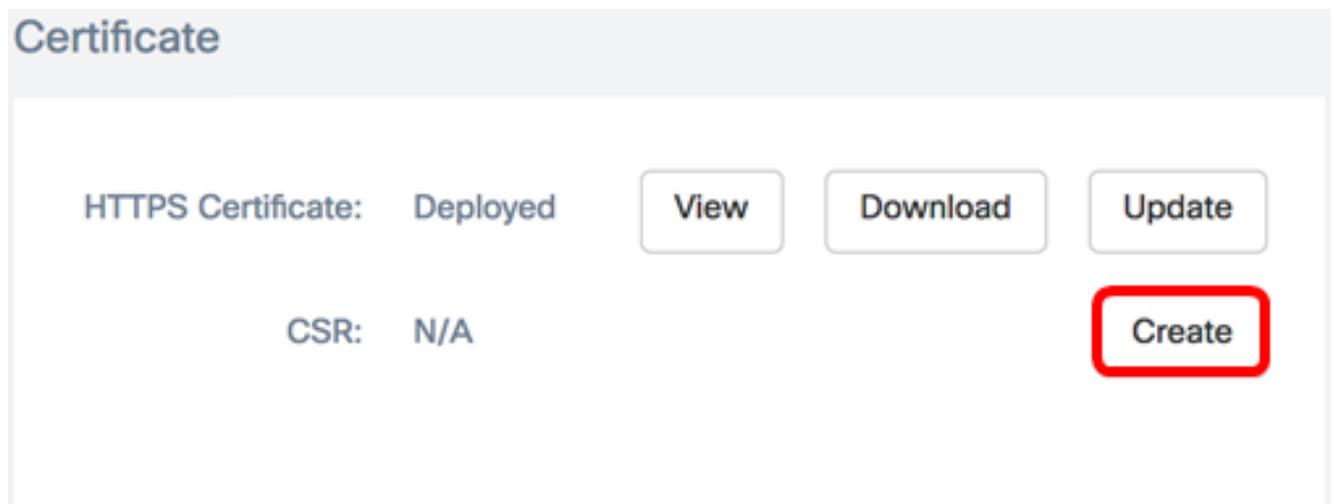
在FindIT Network Manager上管理证书

生成 CSR

步骤1.登录到FindIT Network Manager的Administration GUI，然后选择Administration > Certificate (证书)。



步骤2.在CSR区域中，单击“创建”按钮。



在证书表单中输入的值将用于构建CSR，并包含在您从CA收到的签名证书中。

[步骤3](#).在“完全限定域名”字段中输入IP地址或域名。在本例中，使用hostname.cisco.com。



步骤4.在“国家/地区”字段中输入国家/地区代码。在本例中，使用US。

Country ✓

步骤5.在“状态”字段中输入状态代码。在本例中，使用CA。

State ✓

步骤6.在“城市”字段中输入该城市。在本例中，使用Irvine。

City ✓

步骤7.在“组织”字段中输入组织名称。在本例中，使用思科。

Org ✓

步骤8.在“组织单位”字段中输入组织单位。在本例中，使用S系列。

Org Units ✓

步骤9.在“电子邮件”字段中输入您的电子邮件地址。在本例中，输入 ciscofindituser@cisco.com。

Email ✓

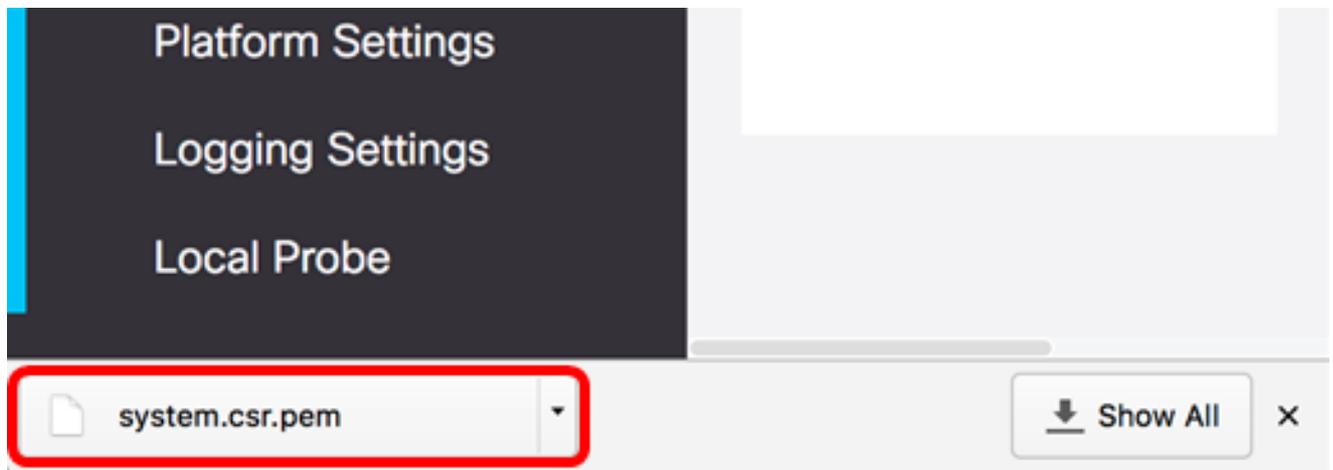
步骤10.单击“保存”。

Certificate

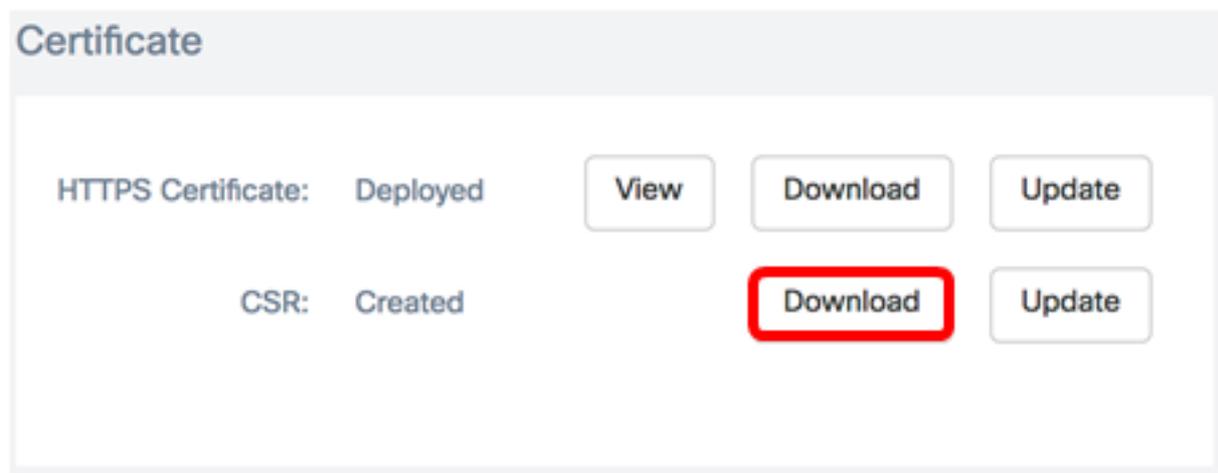
Note: When you create the CSR file successfully, please send the downloaded file to a Certificate Authority to issue, and then upload the issued certificate to system by operation (Update/Upload Cert).

| | |
|----------------------------|--|
| 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"/> ✓ |

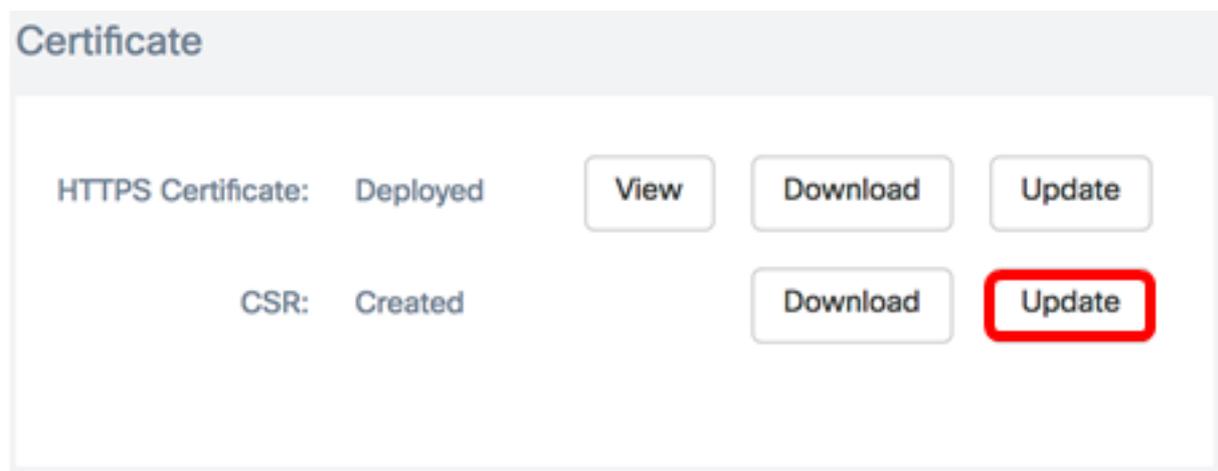
CSR文件将自动下载到您的计算机。在本例中，系统.csr.pem文件生成。



步骤11. (可选) 在CSR区域，状态将从N/A更新为Created。要下载创建的CSR，请单击“**下载**”按钮。



步骤12. (可选) 要更新创建的CSR，请单击“**更新**”按钮，然后返回[步骤3](#)。

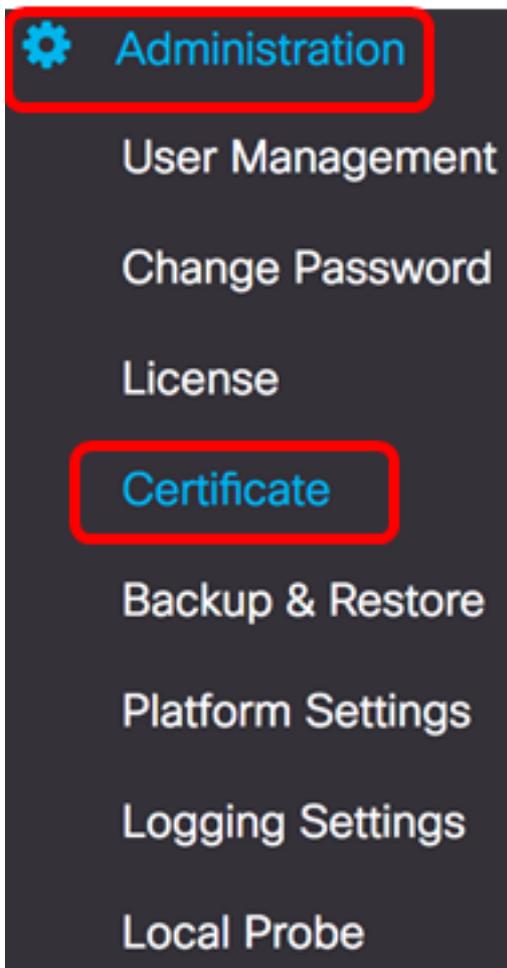


现在，您应该已在FindIT Network Manager上成功生成CSR。您现在可以将下载的CSR文件发送到CA。

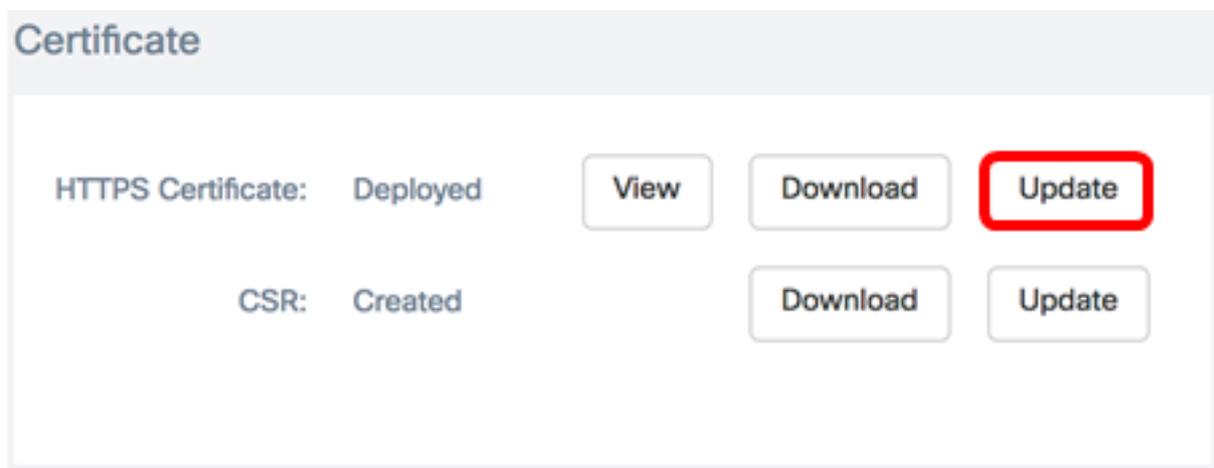
从CA上传签名证书

从CA收到签名的CSR后，您现在可以将其上传到Manager。

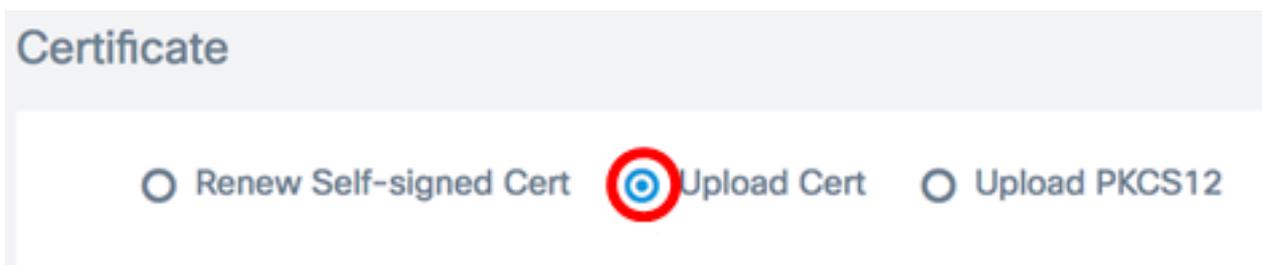
步骤1. 登录到FindIT Network Manager的Administration GUI，然后选择Administration > **Certificate (证书)**。



步骤2.在HTTPS Certificate区域中，单击Update按钮。



步骤3.单击UploadCert单选按钮。

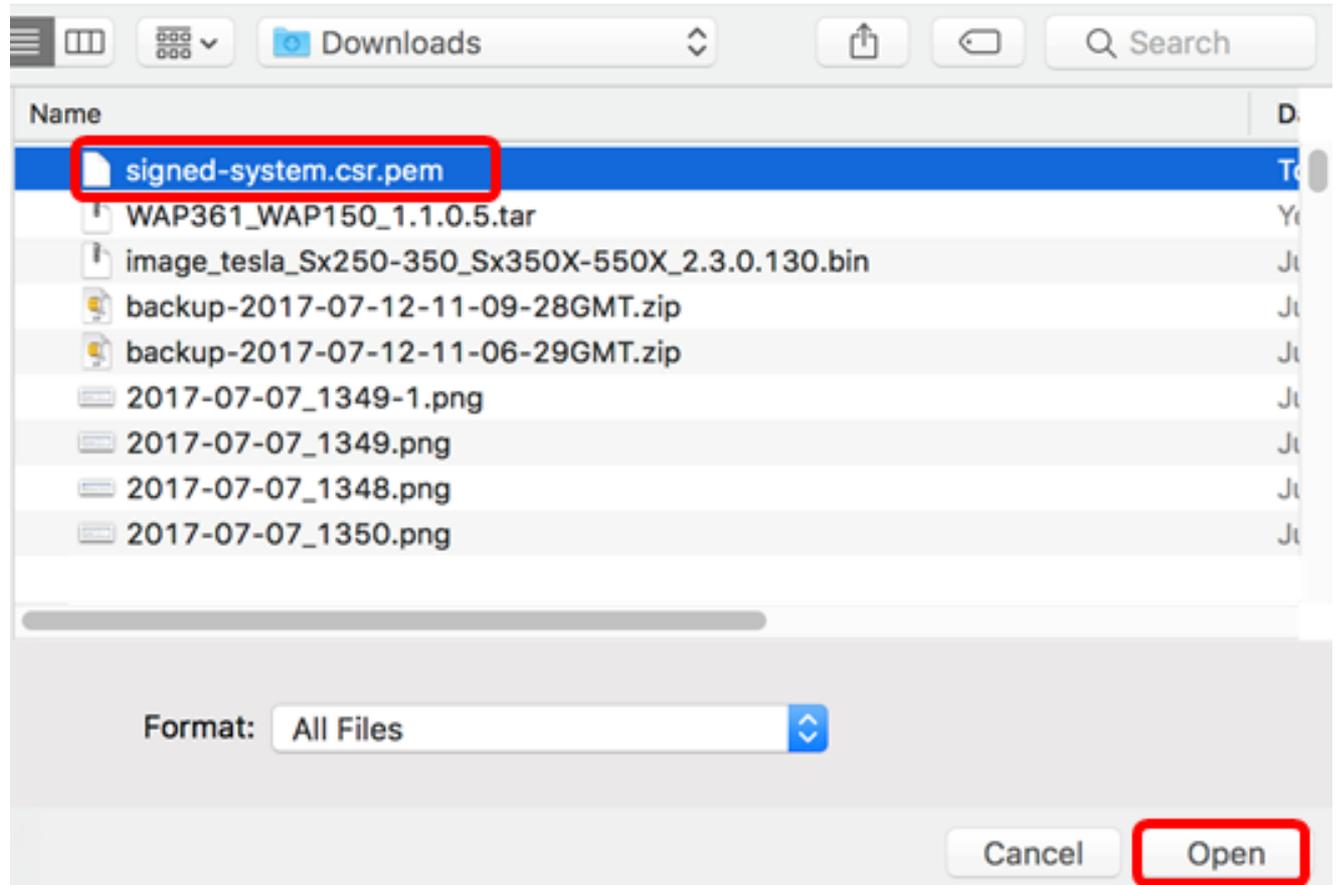


注意：或者，您也可以通过选择Upload PKCS12单选按钮，以PKCS#12格式上传具有相关私钥的证书。应在提供的“密码”字段中指定用于解锁文件的密码。

Upload Cert Upload PKCS12

Password:

步骤4. 在目标区域上删除签名的证书，或者单击目标区域浏览文件系统，然后单击**Open**。文件应为.pem格式。



注意：在本示例中，使用signed-system.csr.pem。

步骤5. 单击**Upload**。

Certificate

Renew Self-signed Cert Upload Cert Upload PKCS12

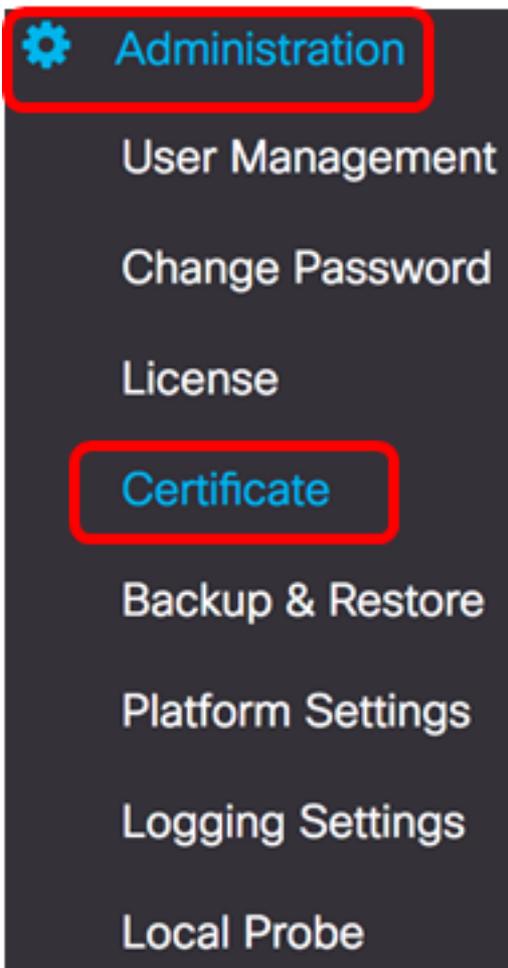
Drag and drop file here (or
click to select a file from the
filesystem)

Filename: signed-system.csr.pem

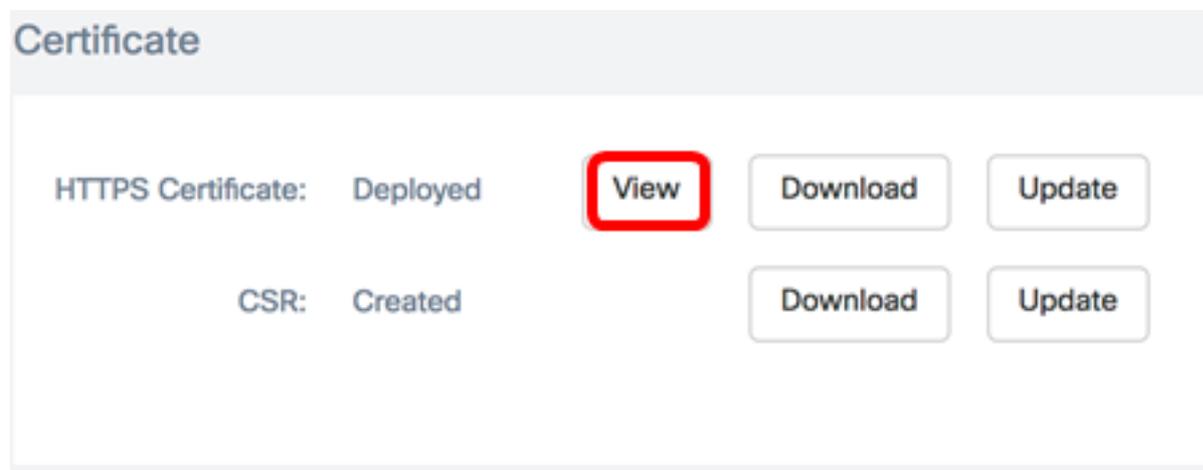
现在，您应该已成功将签名证书上传到FindIT网络管理器。

管理当前证书

步骤1. 登录到FindIT Network Manager的Administration GUI，然后选择Administration > Certificate（证书）。



步骤2.在HTTPS Certificate区域中，单击View按钮。



步骤3.当前证书将以纯文本格式显示在新的浏览器窗口中。单击x或取消按钮关闭窗口。

```
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

第4步。(可选)要下载当前证书的副本，请点击HTTPS Certificate区域中的Download按钮。

Certificate

HTTPS Certificate: Deployed

View

Download

Update

CSR: Created

Download

Update

现在，您应该已成功管理FindIT网络管理器上的当前证书。