

在FindIT網路管理員上管理憑證

目標

數位證書通過證書的指定主題來證明公共金鑰的所有權。這允許依賴方依賴於由與經認證的公鑰對應的私鑰進行的簽名或斷言。安裝後，FindIT網路管理器生成自簽名證書以保護Web以及與伺服器的其它通訊。您可以選擇將此憑證替換為受信任憑證授權單位(CA)簽署的憑證。為此，您將需要生成證書簽名請求(CSR)，以由CA進行簽名。

也可以選擇完全獨立於管理器生成證書和相應的私鑰。如果是這樣，在上傳之前，可以將證書和私鑰組合到公鑰加密標準(PKCS#12加密格式檔案中)。

FindIT Network Manager僅支援.pem格式證書。如果您取得其他憑證格式，則需要再次從CA轉換.pem格式憑證的格式或要求。

本文提供有關如何在FindIT Network Manager上管理證書的說明。

適用裝置

- FindIT網路管理員

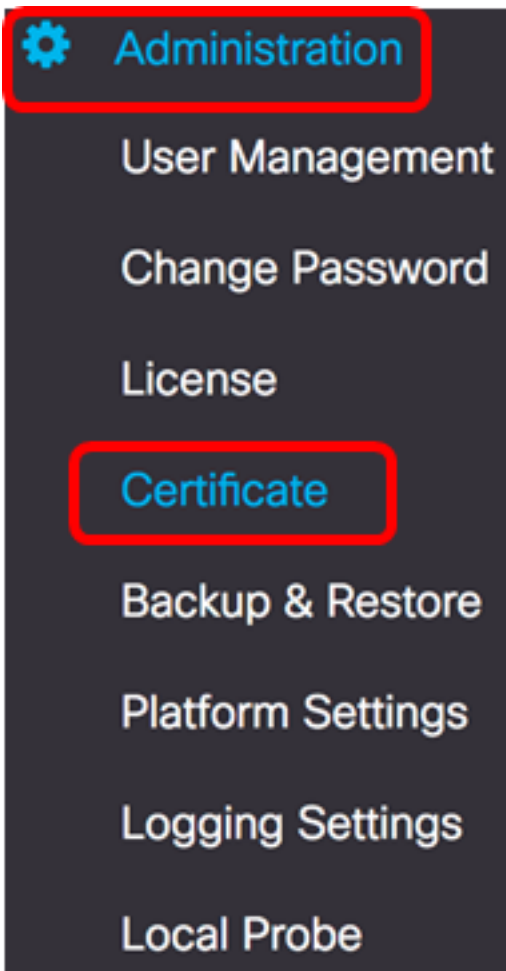
軟體版本

- 1.1

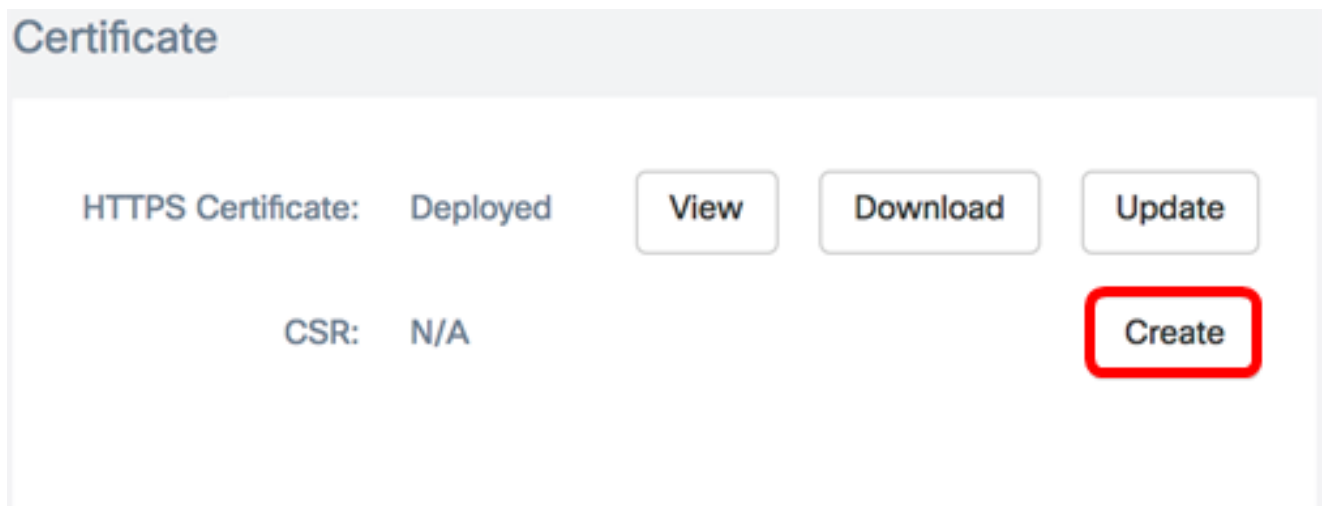
在FindIT網路管理員上管理憑證

產生CSR

步驟1.登入到FindIT網路管理器的管理GUI，然後選擇**Administration > Certificate**。

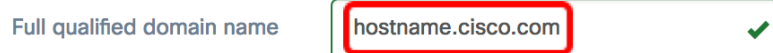


步驟2.在CSR區域中，按一下**Create**按鈕。



在證書表單中輸入的值將用於構建CSR，並將包含在您從CA接收的簽名證書中。

步驟3.在完全限定域名欄位中輸入IP地址或域名。在此示例中，使用hostname.cisco.com。



步驟4.在「國家/地區」欄位中輸入國家/地區代碼。在此示例中，使用US。

Country ✓

步驟5.在 *State* 欄位中輸入狀態代碼。本範例中使用的是CA。

State ✓

步驟6.在 *City* 欄位中輸入城市。在本示例中，使用了Irvine。

City ✓

步驟7.在「組織」欄位中輸入組織名稱。在本範例中使用的是Cisco。

Org ✓

步驟8.在「組織單位」欄位中輸入組織單位。本示例使用Small Business。

Org Units ✓

步驟9.在 *Email* (電子郵件) 欄位中輸入您的電子郵件地址。在此範例中，輸入 ciscofindituser@cisco.com。

Email ✓

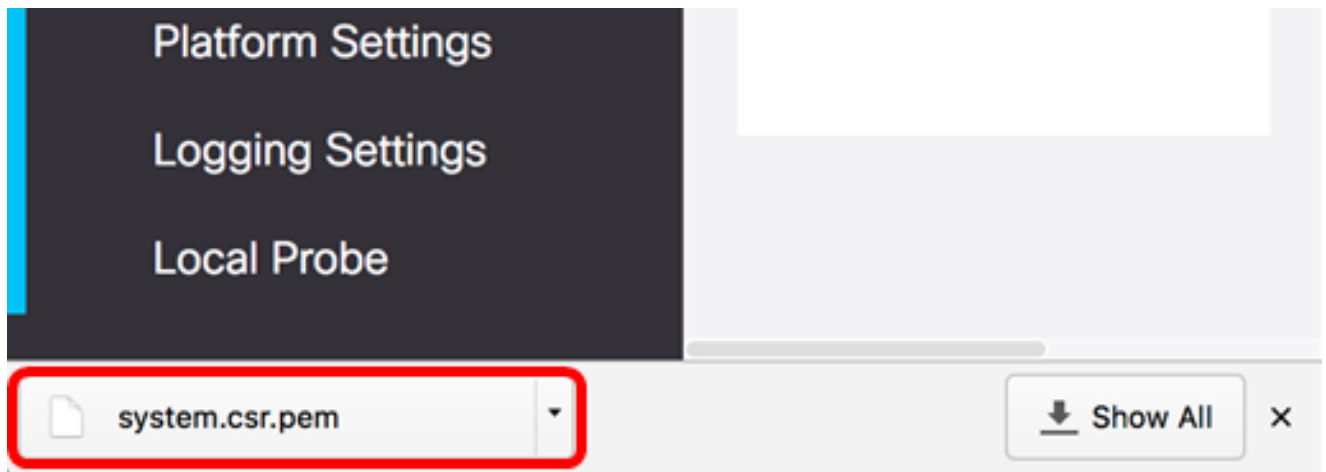
步驟10.按一下「**Save**」。

Certificate

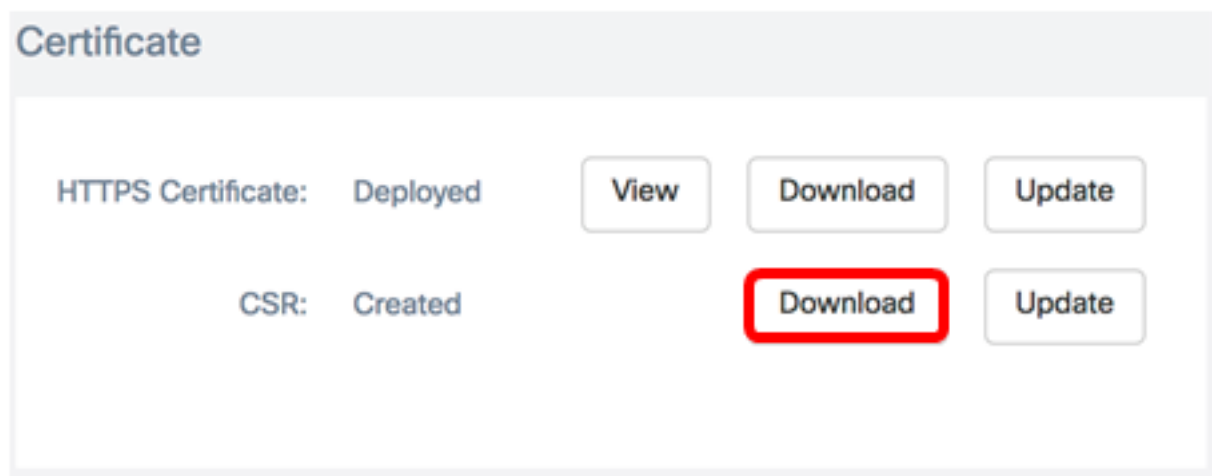
Note: When you create the CSR file successfully, please send the downloaded file to a Certificate Authority to issue, and then upload the issued certificate to system by operation (Update/Upload Cert).

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"/> ✓

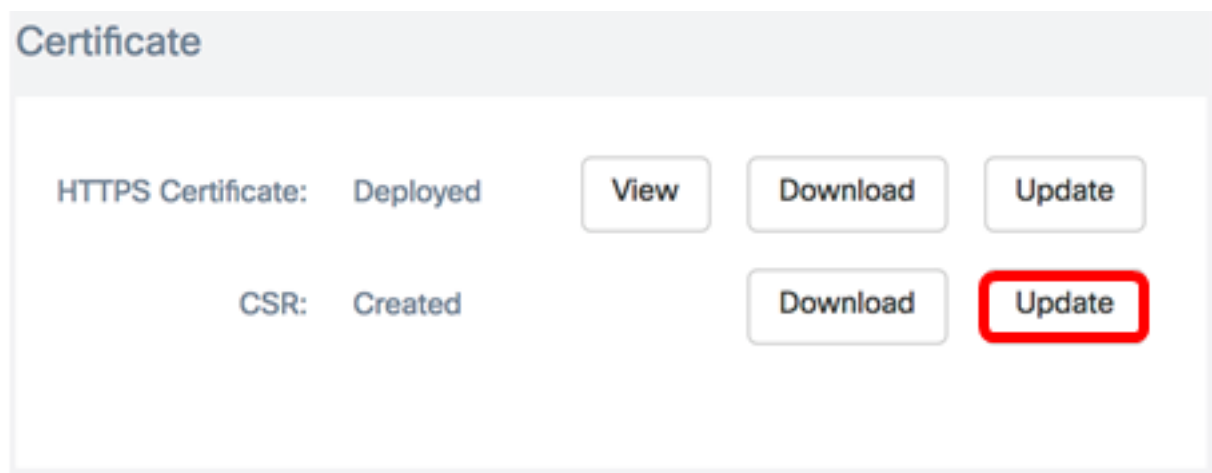
CSR檔案將自動下載到您的電腦。在此範例中，系統會產生system.csr.pem檔案。



步驟11。(可選)在CSR區域中，狀態將從N/A更新為「已建立」。要下載建立的CSR，請按一下Download按鈕。



步驟12。(可選)若要更新建立的CSR，請按一下Update按鈕，然後返回[步驟3](#)。

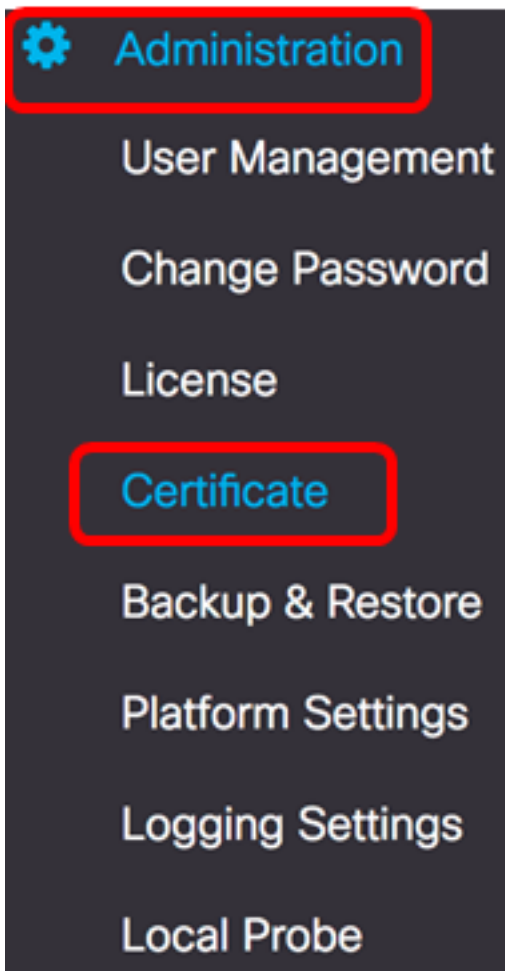


現在，您應該已經在FindIT網路管理員上成功產生CSR。現在，您可以將下載的CSR檔案傳送到CA。

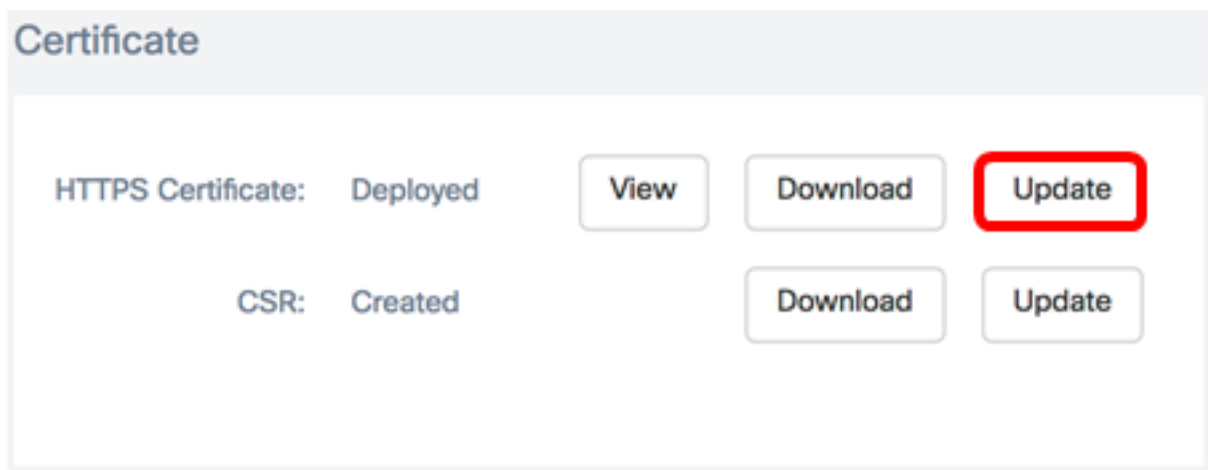
從CA上傳簽署憑證

收到來自CA的已簽署CSR後，您現在可以將它上傳到Manager。

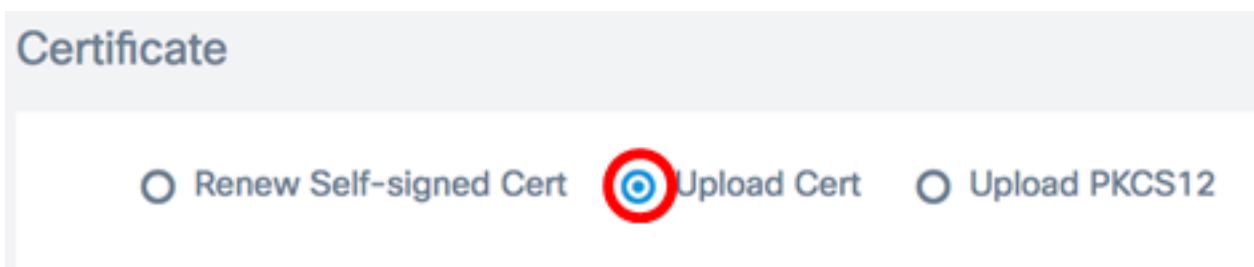
步驟1.登入到FindIT網路管理器的管理GUI，然後選擇Administration > Certificate。



步驟2.在HTTPS Certificate區域中，按一下Update按鈕。



步驟3.按一下UploadCert單選按鈕。

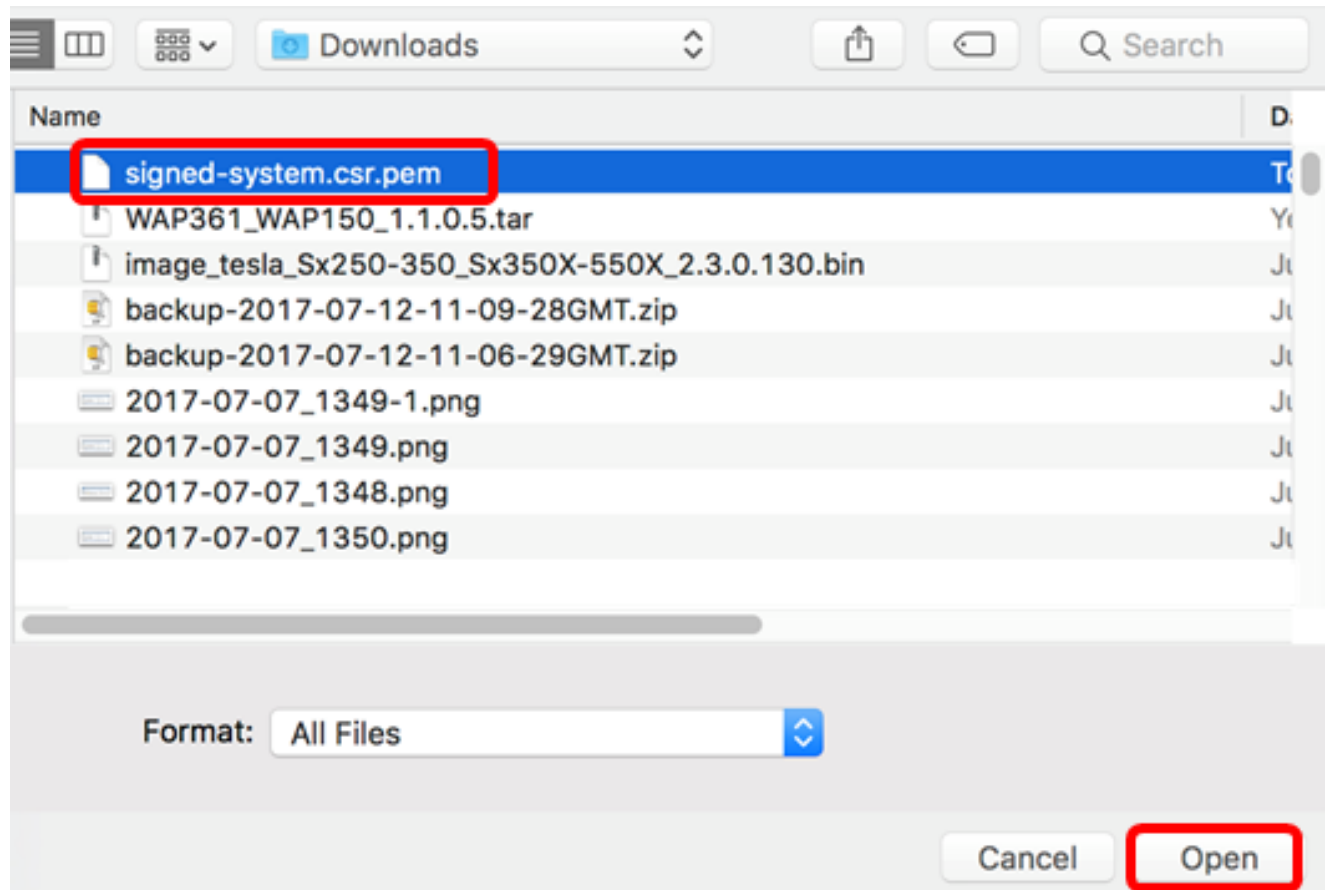


附註：或者，也可以通過選擇Upload PKCS12單選按鈕來上傳具有PKCS#12格式的相關私鑰的證書。應在提供的密碼欄位中指定用於解鎖檔案的密碼。

Upload Cert Upload PKCS12

Password:

步驟4.將簽名證書放到目標區域，或者按一下目標區域瀏覽檔案系統，然後按一下**開啟**。檔案格式應為.pem。



附註：在此範例中，使用的是signed-system.csr.pem。

步驟5.按一下**Upload**。

Certificate

Renew Self-signed Cert Upload Cert Upload PKCS12

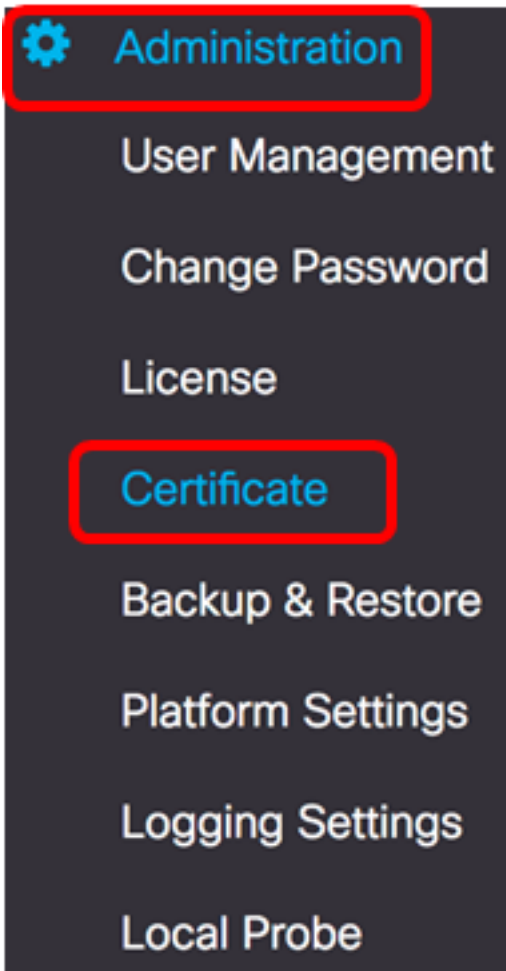
Drag and drop file here (or
click to select a file from the
filesystem)

Filename: signed-system.csr.pem

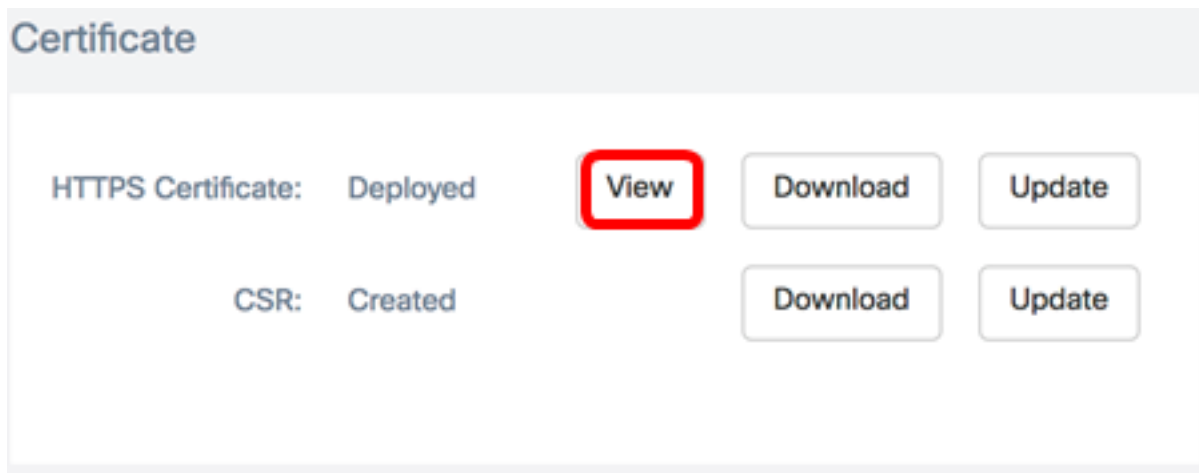
現在，您應該已經成功地將簽名證書上傳到FindIT網路管理器。

管理當前證書

步驟1. 登入到FindIT網路管理器的管理GUI，然後選擇**Administration > Certificate**。



步驟2.在HTTPS Certificate區域中，按一下**View**按鈕。



步驟3.將在新的瀏覽器視窗中以純文字檔案格式顯示當前證書。按一下x或取消按鈕關閉視窗。


```
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.
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

步驟4. (可選) 若要下載目前憑證的副本，請按一下HTTPS Certificate區域中的Download按鈕。

Certificate

HTTPS Certificate:	Deployed	View	Download	Update
CSR:	Created		Download	Update

現在，您應該已經成功管理了FindIT網路管理器上的當前證書。