# 使用多個URL建立自簽名證書

## 目錄



## 簡介

本文檔介紹如何建立可供CloudCenter使用多個URL的自簽名證書。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 憑證
- Linux

### 採用元件

本文檔中的資訊基於CentOS7。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 問題

CloudCenter標準證書或可使用Cisco Call Manager(CCM)配置嚮導建立的證書沒有主題備用名稱(SAN)，某些瀏覽器（如Google Chrome）將此名稱視為錯誤並警告您。可以覆蓋此內容，但如果不使用SAN，則證書只能從一個特定URL中有效。

例如，如果您的IP位址為10.11.12.13的憑證有效，則如果您的DNS名稱為www.opencart.com，則您會收到憑證錯誤，因為該URL不是憑證的用途(即使www.opencart.com在hosts檔案中列為屬於10.11.12.13的來源)。 如果CloudCenter的子租戶正在使用單點登入(SSO)，則可能會發生此情況，因為每個SSO伺服器都有自己的URL。

## 解決方案

解決此問題的最簡單方法是建立一個新的自簽名證書，該證書中包含SAN，其中列出引導您訪問同

一IP地址的任何URL。該指南試圖將最佳做法應用於此過程。

步驟1.導航到根**目錄**，並建立一個新資料夾來存放證書：

```
sudo -s
cd /root
mkdir ca
```

步驟2.導航到新資料夾並建立子資料夾以組織證書、私鑰和日誌。

```
cd ca
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

步驟3.將CAopenssl.conf的**內容複製到/root/ca/openssl.cnf**

> **附註**：此檔案包含證書頒發機構(CA)的配置選項以及可能適用於CloudCenter的預設選項。

步驟4.為CA產生私鑰和憑證。

```
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 private/ca.key.pem
openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -days 7300 -sha256 -
extensions v3_ca -out certs/ca.cert.pem
chmod 444 certs/ca.cert.pem
```

步驟5.您的CA是驗證任何證書是否有效的最終方式，未經授權的個人不得訪問此證書，也不得暴露在Internet上。由於此限制，您必須建立簽署結束憑證的中繼CA，這會在中間授權憑證遭到破壞的情況下產生一個中斷，如果中斷可撤銷該中間授權憑證，並頒發一個新的中間授權憑證。

步驟6.為中間CA建立新子目錄。

```
mkdir /root/ca/intermediate
cd /root/ca/intermediate/
mkdir certs crl csr newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
echo 1000 > /root/ca/intermediate/crlnumber
```

步驟7.將**Intermediateopenssl.conf**的內容複製到**/root/ca/intermediate/openssl.cnf**。

> **附註**：此檔案包含與CA幾乎相同的配置選項，只是進行一些小調整以使其特定於某個中間裝置。

步驟8.生成中間金鑰和證書。

```
cd /root/ca
openssl genrsa -aes256 -out intermediate/private/intermediate.key.pem 4096
chmod 400 intermediate/private/intermediate.key.pem
openssl req -config intermediate/openssl.cnf -new -sha256 -key
intermediate/private/intermediate.key.pem -out intermediate/csr/intermediate.csr.pem
```

步驟9.使用CA憑證簽署中間憑證，這會建立瀏覽器用於驗證憑證真實性的信任鏈。

```
openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in
intermediate/csr/intermediate.csr.pem -out intermediate/certs/intermediate.cert.pem
chmod 444 intermediate/certs/intermediate.cert.pem
```

步驟10.建立CA鏈，由於您不希望Internet上的CA，因此您可以建立CA鏈，瀏覽器一直使用該鏈驗證真實性直至CA。

```
cat intermediate/certs/intermediate.cert.pem certs/ca.cert.pem > intermediate/certs/ca-
chain.cert.pem
chmod 444 intermediate/certs/ca-chain.cert.pem
```

步驟11.為CCM建立新金鑰和證書。

```
openssl genrsa -out intermediate/private/ccm.com.key.pem 2048
openssl req -new -sha256 -key intermediate/private/ccm.com.key.pem -subj
"/C=US/ST=NC/O=Cisco/CN=ccm.com" -reqexts SAN -config <(cat intermediate/openssl.cnf <(printf
"[SAN]\nsubjectAltName=DNS:ccm.com,DNS:www.ccm.com,IP:10.11.12.13")) -out
intermediate/csr/ccm.com.csr
```

步驟12.此操作包含命令中的所有必需欄位，必須手動編輯。

- /C=US是指國家/地區（2字元限制）
- /ST=NC指狀態，可能包含空格
- /O=思科是指組織
- /CN=ccm.com引用公用名，它應該是用於訪問CCM的主要URL。
- SAN\nSubjectAltName=是替代名稱，公用名稱應在此清單中，並且您的SAN數量沒有限制。

步驟13.使用中間憑證簽署最終憑證。

```
openssl ca -config intermediate/openssl.cnf -extensions server_cert -days 375 -notext -md sha256
-in intermediate/csr/ccm.com.csr -out intermediate/certs/ccm.com.cert.pem
```

步驟14.驗證證書是否已正確簽名。

```
openssl verify -CAfile intermediate/certs/ca-chain.cert.pem intermediate/certs/ccm.com.cert.pem
```

步驟15。它可以返回OK或Fail。

步驟16.將新證書、其金鑰和CA鏈複製到Catalina檔案夾。

```
cd /root/ca/intermediate/certs
cp ccm.com.cert.pem /usr/local/tomcat/conf/ssl/ccm.com.crt
cp ca-chain.cert.pem /usr/local/tomcat/conf/ssl/ca-chain.crt
cd ../private
cp ccm.com.key.pem /usr/local/tomcat/conf/ssl/ccm.com.key
```

步驟17.授予cliqruser所有權並正確設定許可權。

```
chown cliqruser:cliqruser ccm.com.crt
chown cliqruser:cliqruser ccm.com.key
chown cliqruser:cliqruser ca-chain.crt
chmod 644 ccm.com.crt
chmod 644 ccm.com.key
chmod 644 ca-chain.crt
```

步驟18.在進行任何更改之前備份**server.xml**檔案。

```
cd ..
cp server.xml server.xml.bak
```

步驟19.**編輯server.xml:**

1. 找到以**<Connector port="10443" maxHttpHeaderSize="8192"開頭的部分**
2. 將**SSLCertificateFile** 更改為指向ccm.com.crt
3. 將**SSLCertificateKeyFile**更改為指向ccm.com.key
4. 將**SSLCACertificateFile**更改為指向ca-chain.crt

步驟20.重新啟動Tomcat。

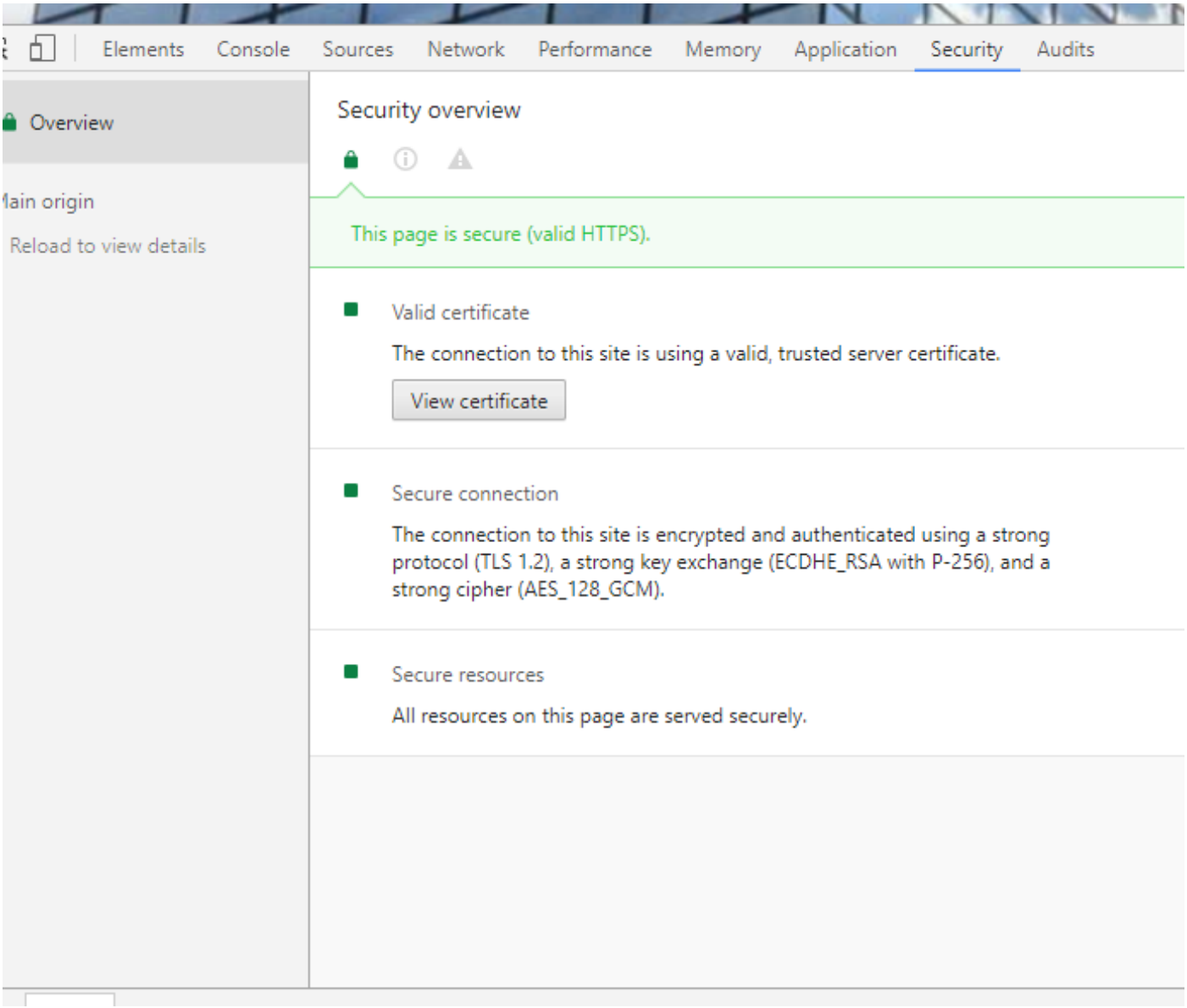
```
service tomcat stop
service tomcat start
```

步驟21. CCM現在使用對於步驟13中指定的所有DNS名稱和IP地址有效的新證書。

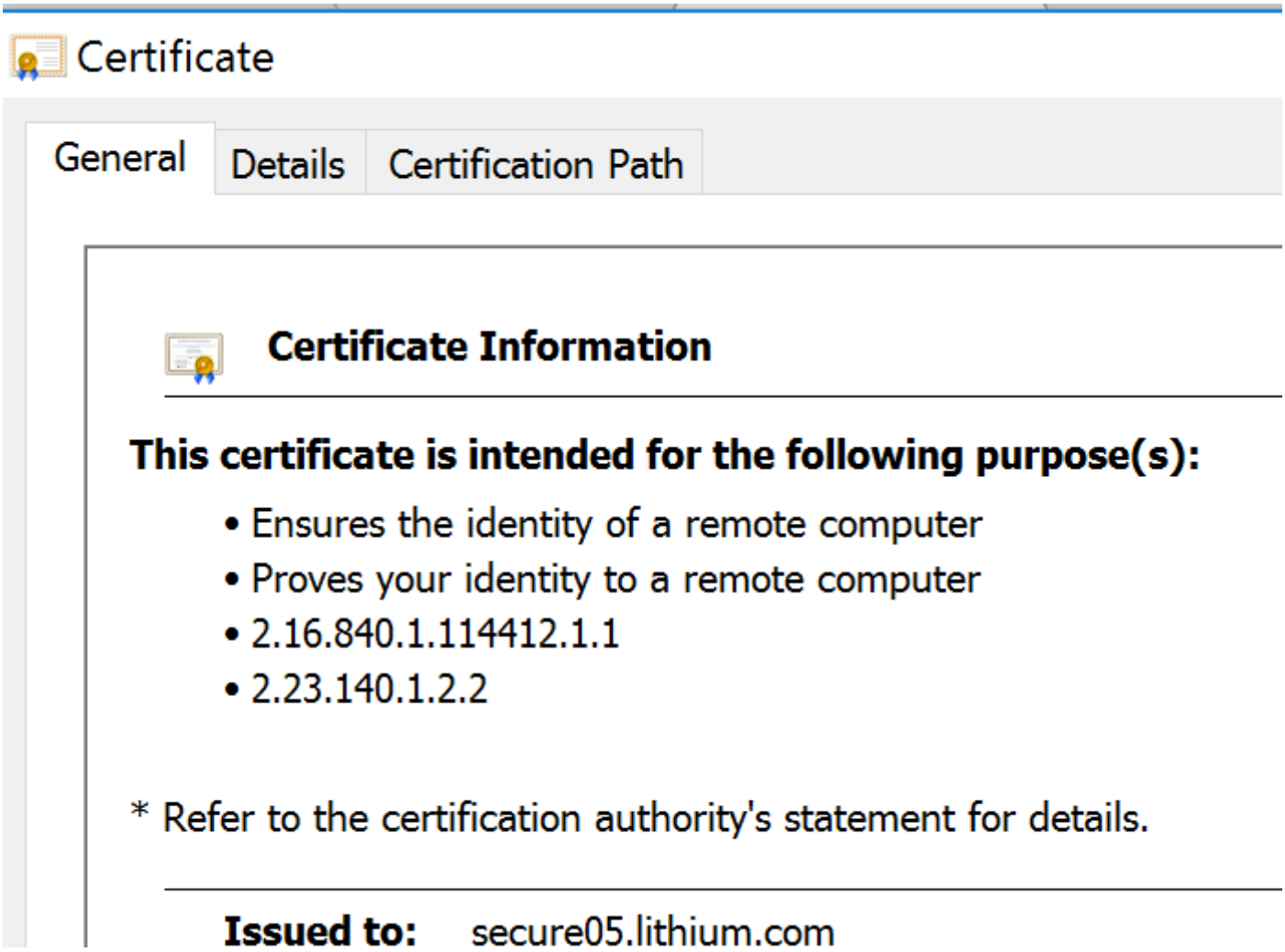
步驟22.由於在編寫指南時建立了CA，因此瀏覽器在預設情況下不會將其識別為有效，您必須手動匯入證書。

步驟23.使用任何有效的URL導航到**CCM**，然後按**Ctrl+Shift+i**，這將開啟開發人員工具。

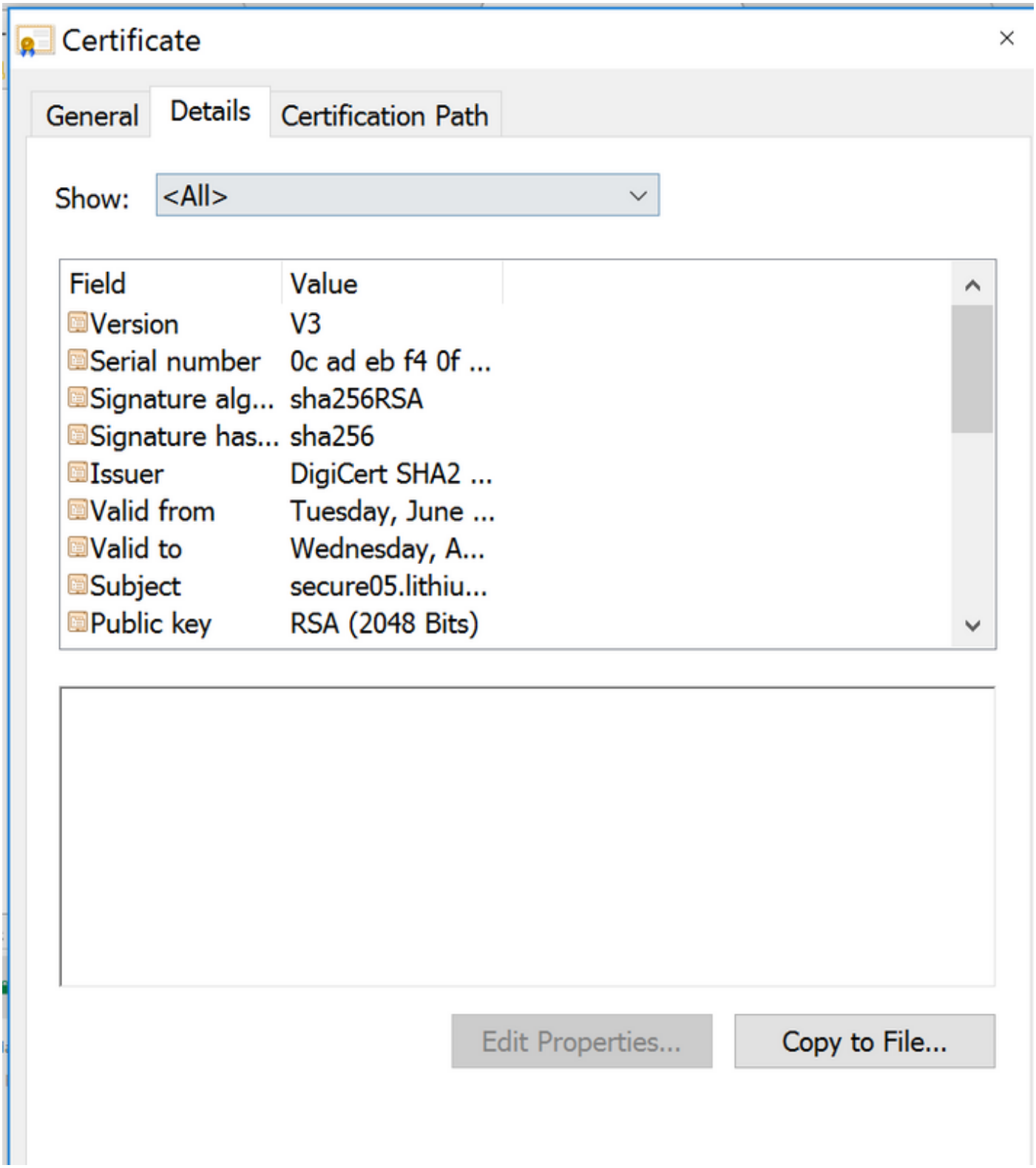
步驟24.選擇**View Certificate**，如下圖所示。



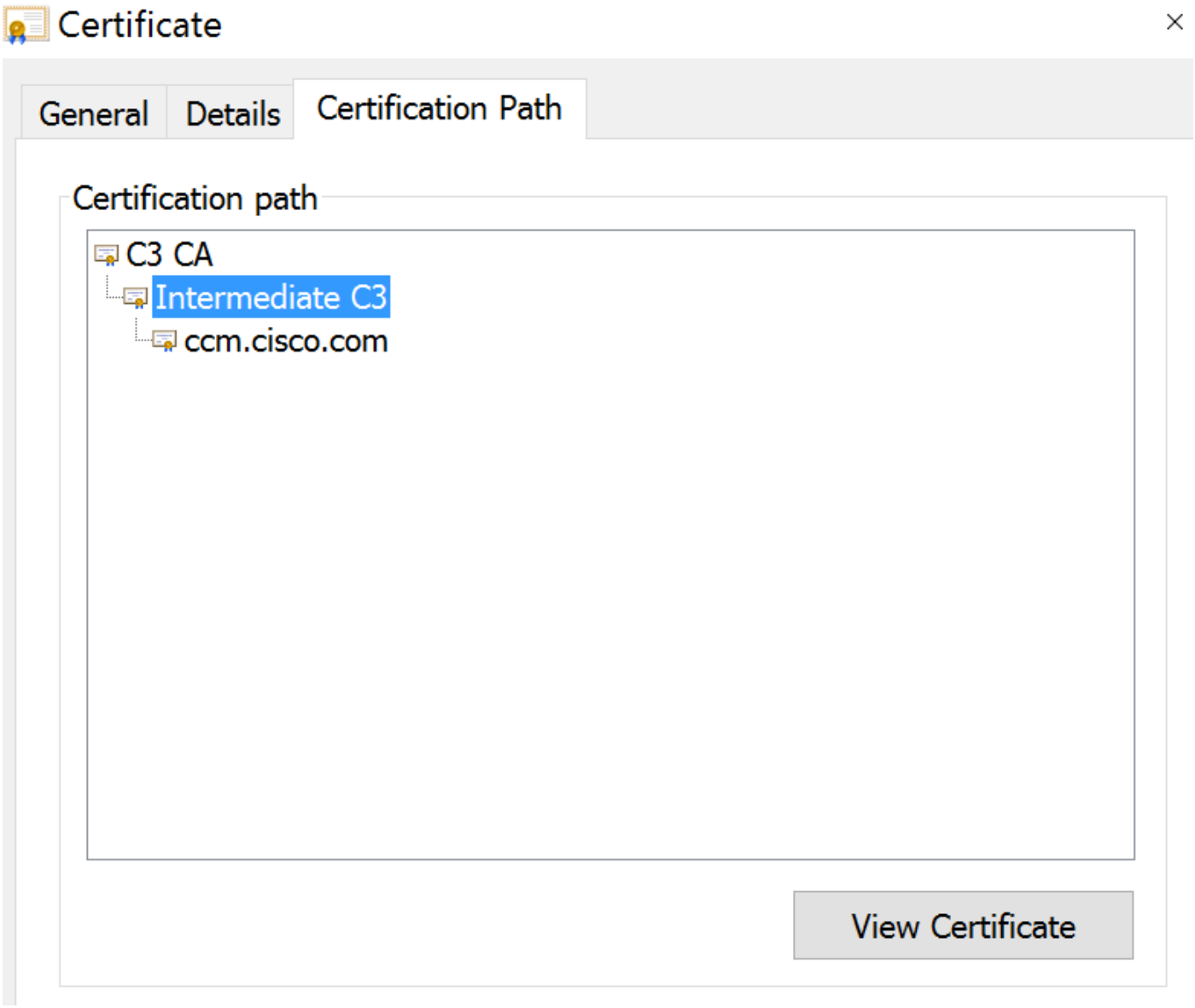

步驟25.選擇**Details**，如下圖所示。




步驟26.選擇Copy To File，如下圖所示。




步驟27.如果收到有關不受信任的CA的錯誤，請導航到**證書路徑**以檢視中間證書和根證書。您可以按一下這些憑證，並檢視其憑證，然後將其複製到檔案中，如下圖所示。




步驟28.下載證書後，按照作業系統(OS)或瀏覽器的說明安裝這些證書作為受信任的機構和中間機構。