自签名证书的创建与多个URL的

目录

简介

本文描述如何创建能由CloudCenter使用与多个URL的自签名证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 证书
- Linux

使用的组件

本文档中的信息根据CentOS7。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

来有CloudCenter的标准，或者可以创建与使用Cisco Call Manager (CCM)配置向导的证书，没有某些浏览器，例如谷歌镀铬物，对待错误并且警告您的一附属的替代方案名称(SAN)。这可以被改写，但是没有圣的，证书可以只是有效从一个特定URL。

例如，如果有为10.11.12.13的IP地址是有效的一证书，如果有www.opencart.com域名系统(DNS)名，您接收验证错误，因为该URL不是什么证书是为(这是真的，即使www.opencart.com在您的HOSTS文件列出作为属于到10.11.12.13)的那个。这能突然发生，如果CloudCenter转租人在使用单个符号打开(SSO)，因为每个SSO服务器有其自己的URL。

解决方案

调整此问题的简便的方法是创建有圣的列出所有URL处理您对同样IP地址的一新的自签名证书。指

南是尝试应用最佳实践到此进程。

步骤1.导航对**根目录**并且做新文件夹安置证书：

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

步骤2.导航到新文件夹并且做子文件夹组织证书、专用密钥和日志。

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

步骤3.复制**CAopenssl.conf**内容**对/root/ca/openssl.cnf**

> **注意**：此文件包含也许是适当的为CloudCenter的Certificate Authority (CA)和默认选项的配置选项。

步骤4.生成一专用密钥和证书CA的。

```
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
```

第五步：您的CA是最终方式验证所有证书有效，此证书必须由未授权的个人从未访问，并且必须从未显示在互联网。由于此限制，签署末端证书的您必须创建中间CA，这创建工间休息时间，如果半成品权限证书折衷它能取消和发出的新的。

第六步：做中间CA的一个新的子目录。

```
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
```

步骤7.复制**Intermediateopenssl.conf**内容**对**/root/ca/intermediate/openssl.cnf**。**

> **注意**：此文件包含CA的几乎完全相同的配置选项除一些个小调整之外使特定对中间。

步骤8.生成半成品密钥和证书。

```
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
```

步骤9.签署与CA证书的中间证书，这构件浏览器使用验证证书的真实性信任的一系列。

```
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
```

步骤10.请创建CA一系列，因为您不想要在互联网的CA，您能做浏览器使用一直验证真实性至CA的CA一系列。

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

步骤11.创建一新密钥和证书CCM的。

```
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
```

步骤 12这有所有必填字段在命令，并且必须手工编辑。

- /C =US是指国家(2字符限制)
- /ST =NC是指状态，并且也许包括空间
- /O =Cisco是指组织
- /CN =ccm.com是指公用名称，这应该是用于的主URL访问CCM。
- SAN \ nsubjectAltName=是代替名称，公用名称应该在此列表，并且没有限制对多少圣的您有。

步骤 13签署与使用的最终证书中间证书。

```
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
```

步骤 14验证证书正确地签了字。

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

步骤 15它能返回OK或失败。

步骤 16复制新证书，它是关键和对卡塔利娜文件夹的CA一系列。

```
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
```

步骤 17格兰特cliqruser正确所有权和集权限。

```
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
```

步骤18。在您做所有变动前，请备份server.xml文件。

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

步骤19。编辑server.xml ：

1. 找出从<Connector port="10443" maxHttpHeaderSize="8192"开始的部分
2. 更改SSLCertificateFile指向ccm.com.crt
3. 更改SSLCertificateKeyFile指向ccm.com.key
4. 更改SSLCACertificateFile指向CAchain.crt

步骤20。重新启动Tomcat。

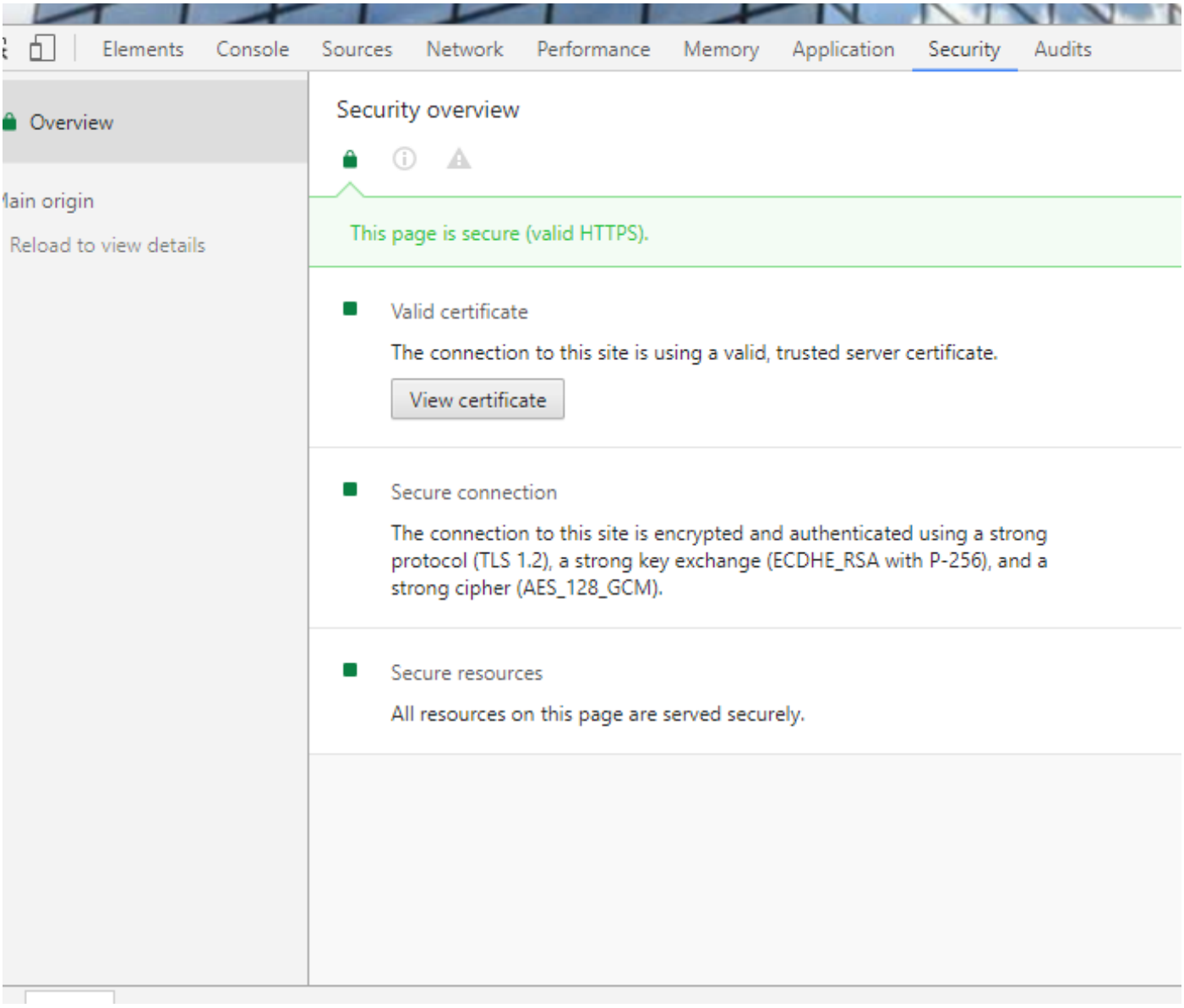
```
service tomcat stop
service tomcat start
```

步骤21。CCM当前使用为在步骤和IP地址是有效指定的所有DNS名13的新证书。

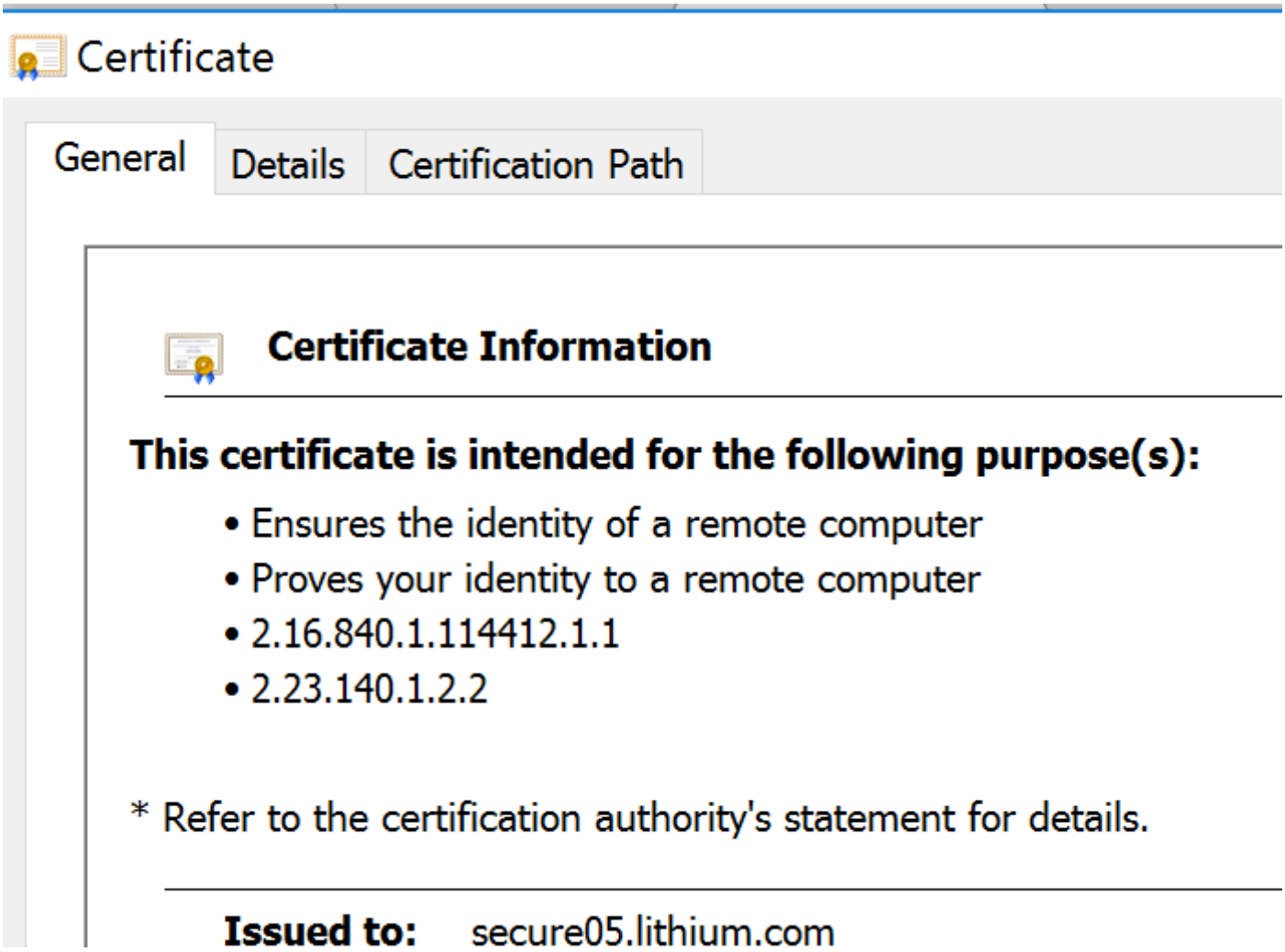
步骤22。因为CA在指南时创建，您的浏览器不会认可它和有效默认情况下，您必须手工导入证书。

步骤23。导航对与使用的**CCM**所有有效URL并且按**Ctrl+Shift+i**，这打开开发者工具。

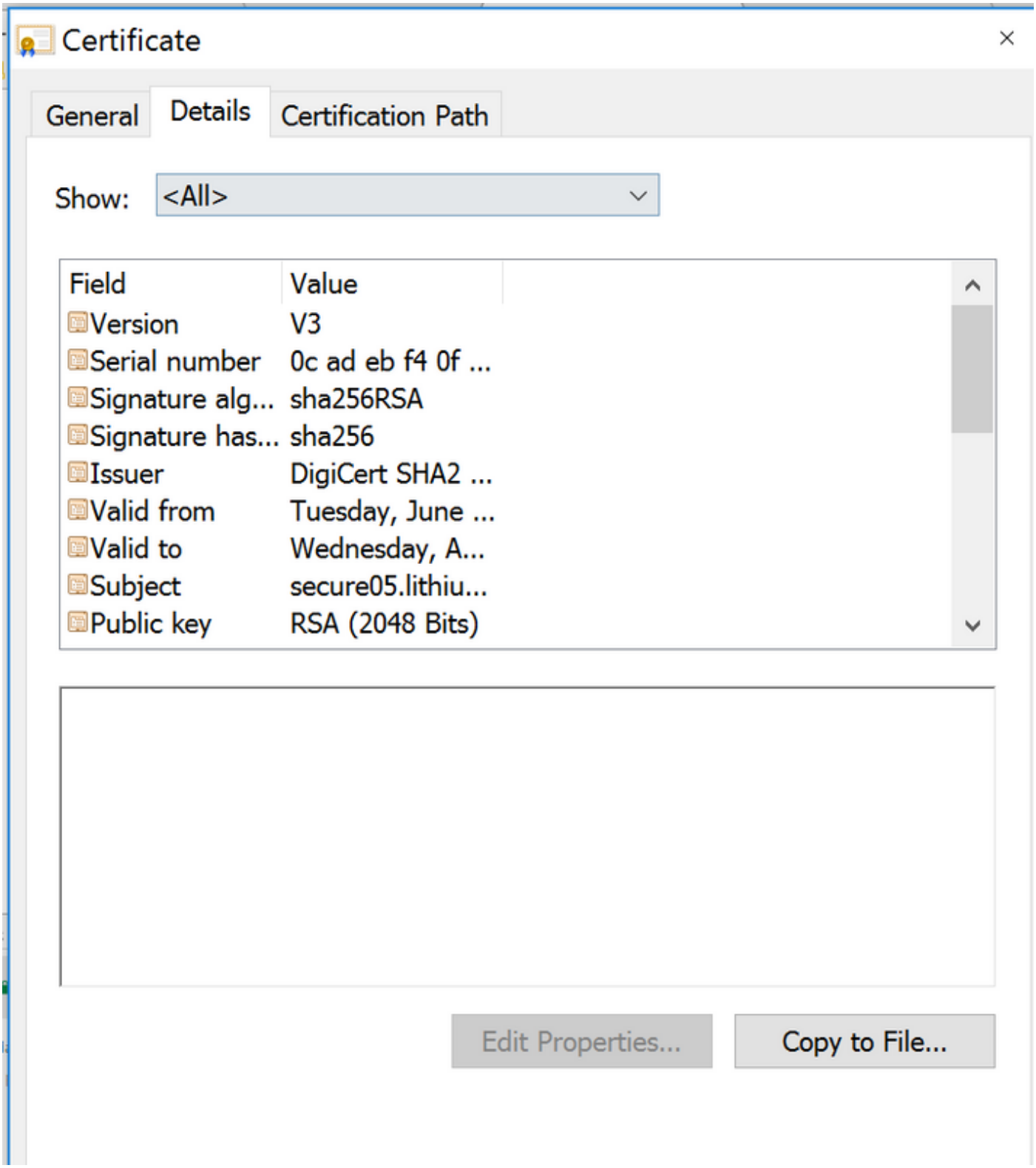
步骤24。如镜像所显示，选择**查看证书**。



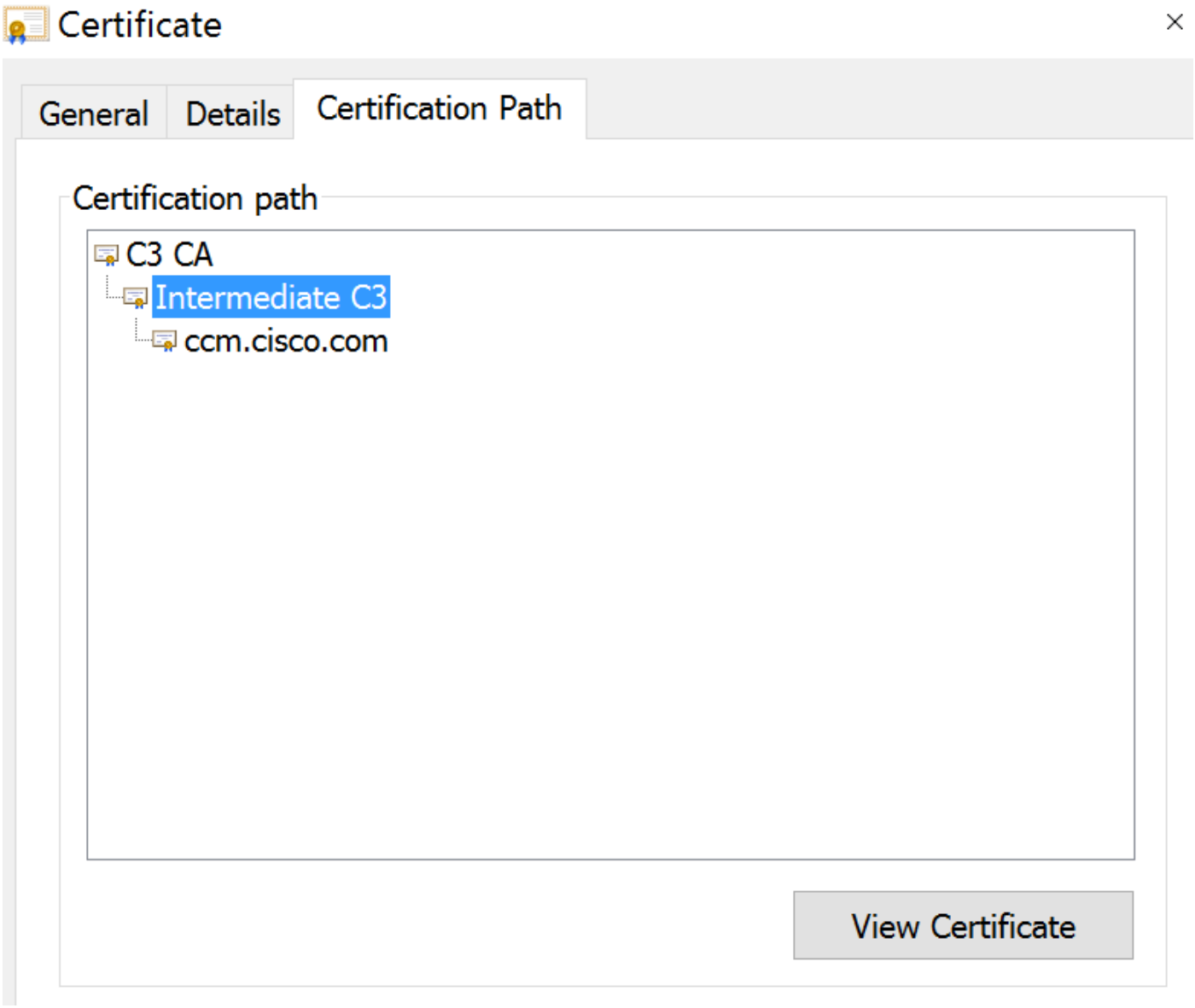
步骤25。如镜像所显示，选择**详细信息**。



步骤26。如镜像所显示，选择**复制到文件**。



步骤27。如果收到关于不信任CA的错误，则请导航到**证书路径**查看中间和根证明。如镜像所显示，您能点击他们和查看他们的证书并且复制那些到文件。



步骤28。一旦安排证书下载，请遵从您的操作系统的(OS)或浏览器的说明安装这些证书作为委托权限和中间权限。