Создание подписанных сертификатов со множественным URL

Содержание

Введение

Этот документ описывает, как создать подписанный сертификат, который может использоваться CloudCenter со множественным URL.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Сертификаты
- Linux

Используемые компоненты

Сведения в этом документе основываются на CentOS7.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

Сертификаты, которые прибывают стандарт с CloudCenter, или которые могут быть созданы с использованием Мастер настройки Cisco Call Manager (CCM), не имейте альтернативного имени субъекта (SAN), какие определенные браузеры, такие как Google Chrome, обработки как ошибка и предупреждает вас. Это может быть отвергнуто, но без SAN, сертификат может только быть допустимым от одного определенного URL.

Например, если у вас есть сертификат, который допустим для IP-адреса 10.11.12.13, если у вас есть Имя системы доменных имен (DNS) www.opencart.com, вы получаете ошибку

сертификата, потому что тот URL не то, что сертификат для (это истинно, даже если www.opencart.com перечислен в вашем файле hosts как тот, который принадлежит 10.11.12.13). Это может неожиданно возникнуть, если субарендаторы CloudCenter в употреблении Единой точки входа (SSO), поскольку каждый сервер SSO имеет свой собственный URL.

Решение

Самый легкий способ устранить эту проблему состоит в том, чтобы создать новый подписанный сертификат, который имеет SAN, который перечисляет любой URL, который направляет вас к тому же IP-адресу. Руководство является попыткой применить оптимальные методы к этому процессу.

Шаг 1. Перейдите к **корневому каталогу** и сделайте новую папку для корпуса сертификатов:

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

Шаг 2. Перейдите в новую папку и сделайте подпапки для организации сертификатов, секретных ключей и журналов.

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

Шаг 3. Скопируйте содержание **CAopenssl.conf к/root/ca/openssl.cnf**

> **Примечание:** Этот файл содержит параметры конфигурации для Центра сертификации (CA) и параметров по умолчанию, которые могли бы быть соответствующими CloudCenter.

Шаг 4. . Генерируйте секретный ключ и сертификат для CA.

```
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
```

Шаг 5. . Ваш CA является окончательным способом проверить, что любой сертификат допустим, к этому сертификату никогда не должны обращаться неавторизованные частные лица и никогда нельзя представлять Интернету. Из-за этого ограничения, необходимо создать промежуточное звено CA , которое подписывает конечный сертификат, это создает разрыв, где, если промежуточный сертификат полномочий поставился под угрозу, это может быть отозвано, и выполнен новый.

Шаг 6. Сделайте новый подкаталог для промежуточного CA.

```
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
```

Шаг 7. Скопируйте содержание **Intermediateopenssl.conf** к**/root/ca/intermediate/openssl.cnf**.

> **Примечание:** Этот файл содержит почти опции одинаковой конфигурации для CA кроме нескольких маленьких тонких настроек для создания его определенным для промежуточного звена.

Шаг 8. Генерируйте промежуточный ключ и сертификат.

```
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
```

Шаг 9. Подпишите промежуточный сертификат с сертификатом CA, это создает цепочку доверия что использование браузера для проверки подлинности сертификата.

```
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
```

Шаг 10. Создайте цепочку CA, так как вы не хотите CA в Интернете, можно сделать цепочку CA что использование браузеров для проверки подлинности полностью до 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
```

Шаг 11. Создайте новый ключ и сертификат для CCM.

```
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
```

Шаг 12. Это имеет все обязательные поля в команде и должно быть отредактировано вручную.

- **/C=US** обращается к стране (2 символьных предела)
- **/ST=NC** обращается к Состоянию и мог бы включать пробелы
- **/O=Cisco** обращается к Организации
- **/CN=ccm.com** обращается к Общему имени, это должно быть основным URL, используемым для доступа к CCM.
- **SAN\nsubjectAltName =** являются альтернативными названиями, общее имя должно быть в этом списке и нет никакого предела тому, сколько SAN вы имеете.

Шаг 13. Подпишите заключительный сертификат с использованием промежуточного сертификата.

```
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
```

Шаг 14. Проверьте, что сертификат был подписан правильно.

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

Шаг 15. Это может возвратить или OK или Сбой.

Шаг 16. Скопируйте новый сертификат, это является ключевым, и цепочка CA к папке

Каталины.

```
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
```

Шаг 17. Предоставьте cliqruser владение и установите разрешения правильно.

```
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
```

Шаг 18. Резервируйте **server.xml** файл перед внесением любых изменений.

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

Шаг 19. Отредактируйте **server.xml:**

1. Найдите раздел, который запускается с **<Порт разъёма = "10443" maxHttpHeaderSize = "8192"**
2. Измените **SSLCertificateFile** для обращения к ccm.com.crt
3. Измените **SSLCertificateKeyFile** для обращения к ccm.com.key
4. Измените **SSLCACertificateFile** для обращения ca-chain.crt

Шаг 20. Tomcat перезапуска.

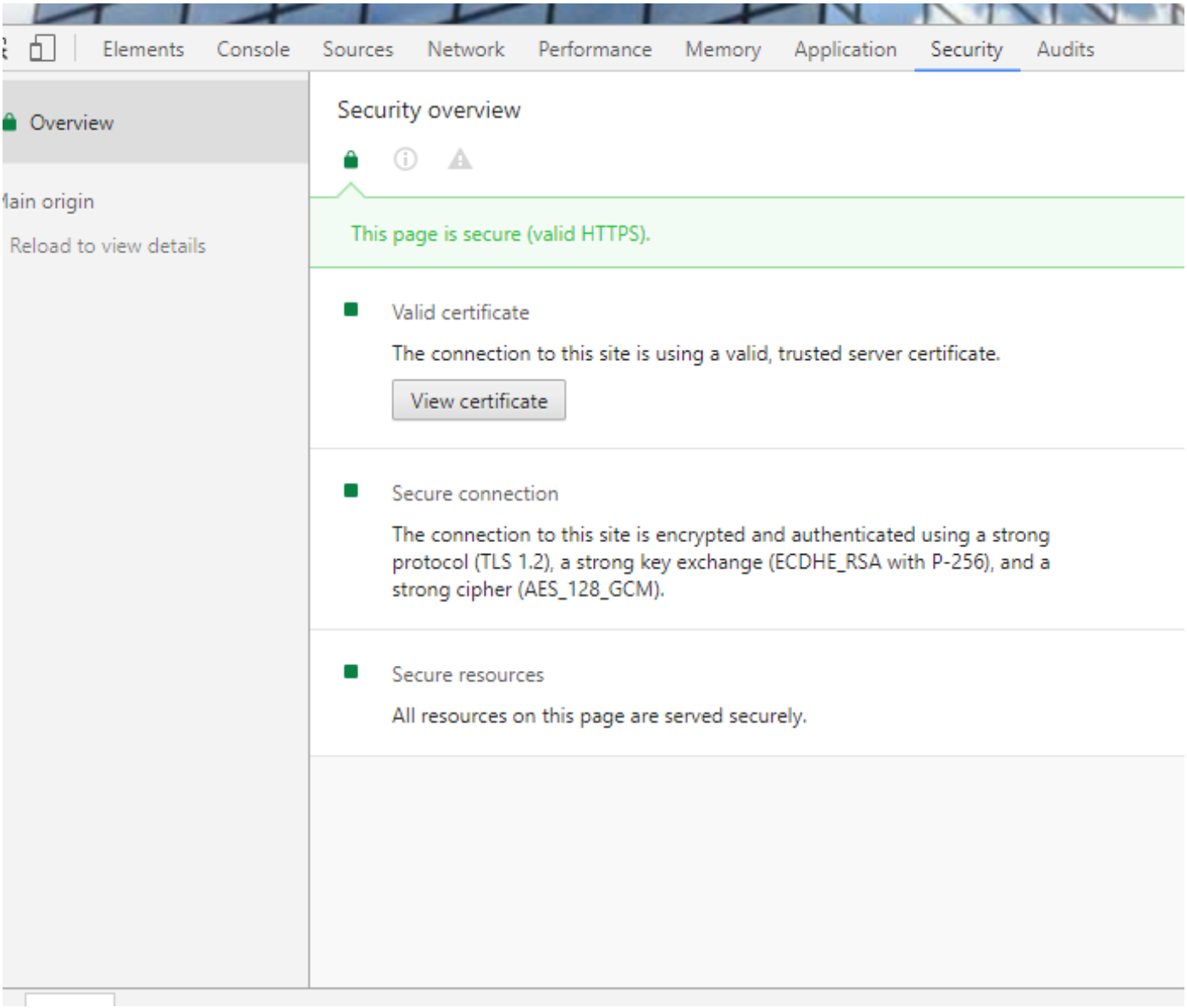
```
service tomcat stop
service tomcat start
```

Шаг 21. CCM теперь использует новый сертификат, который допустим для всех имен DNS и IP-адресов, заданных в Шаге 13.

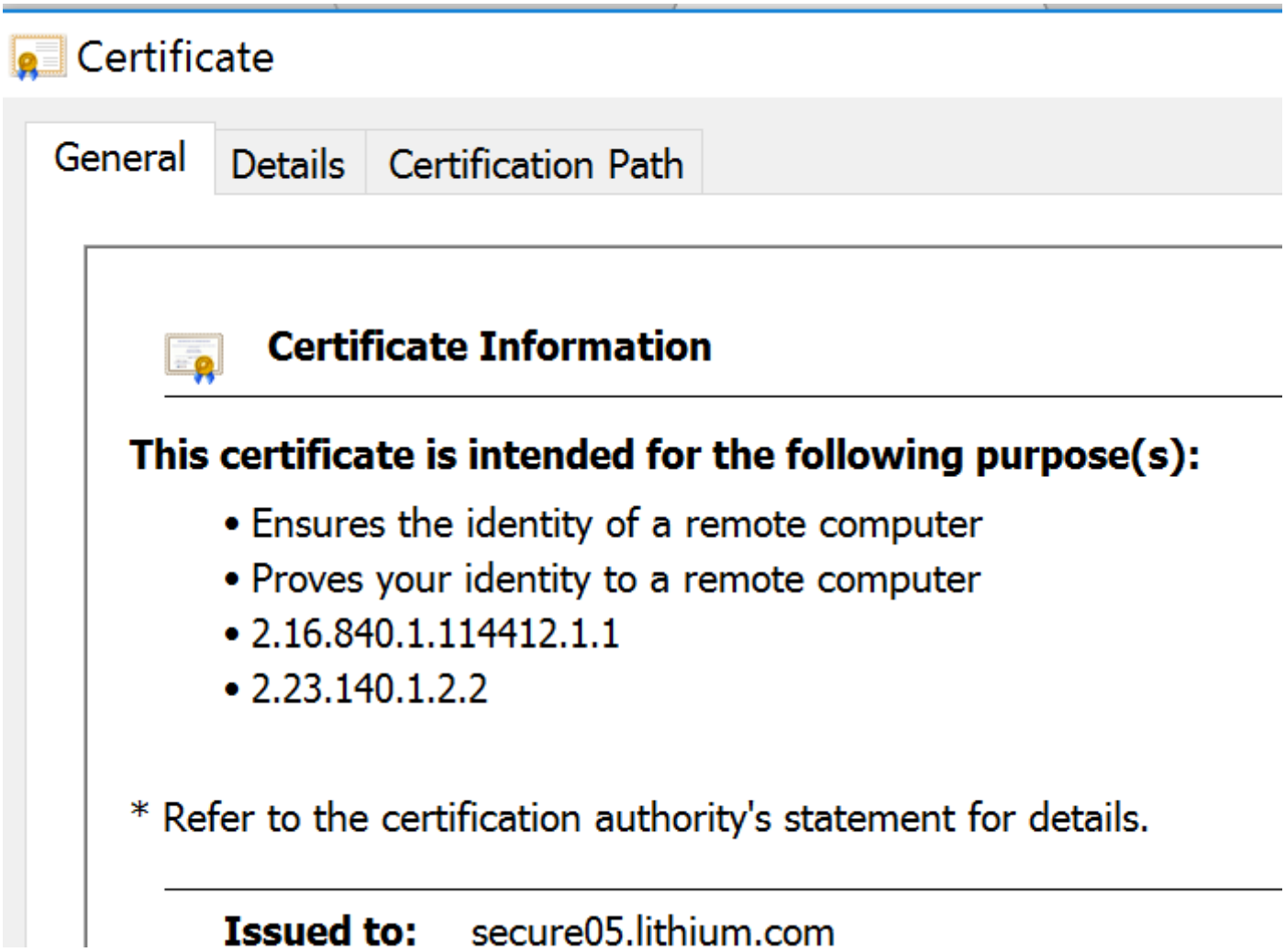
Шаг 22. Поскольку CA был создан во время руководства, ваши браузеры не распознают его как допустимый по умолчанию, необходимо вручную импортировать сертификат.

Шаг 23. Перейдите к **CCM** с использованием любого допустимого URL и нажмите **Ctrl+Shift+i**, это открывает программные средства разработчика.

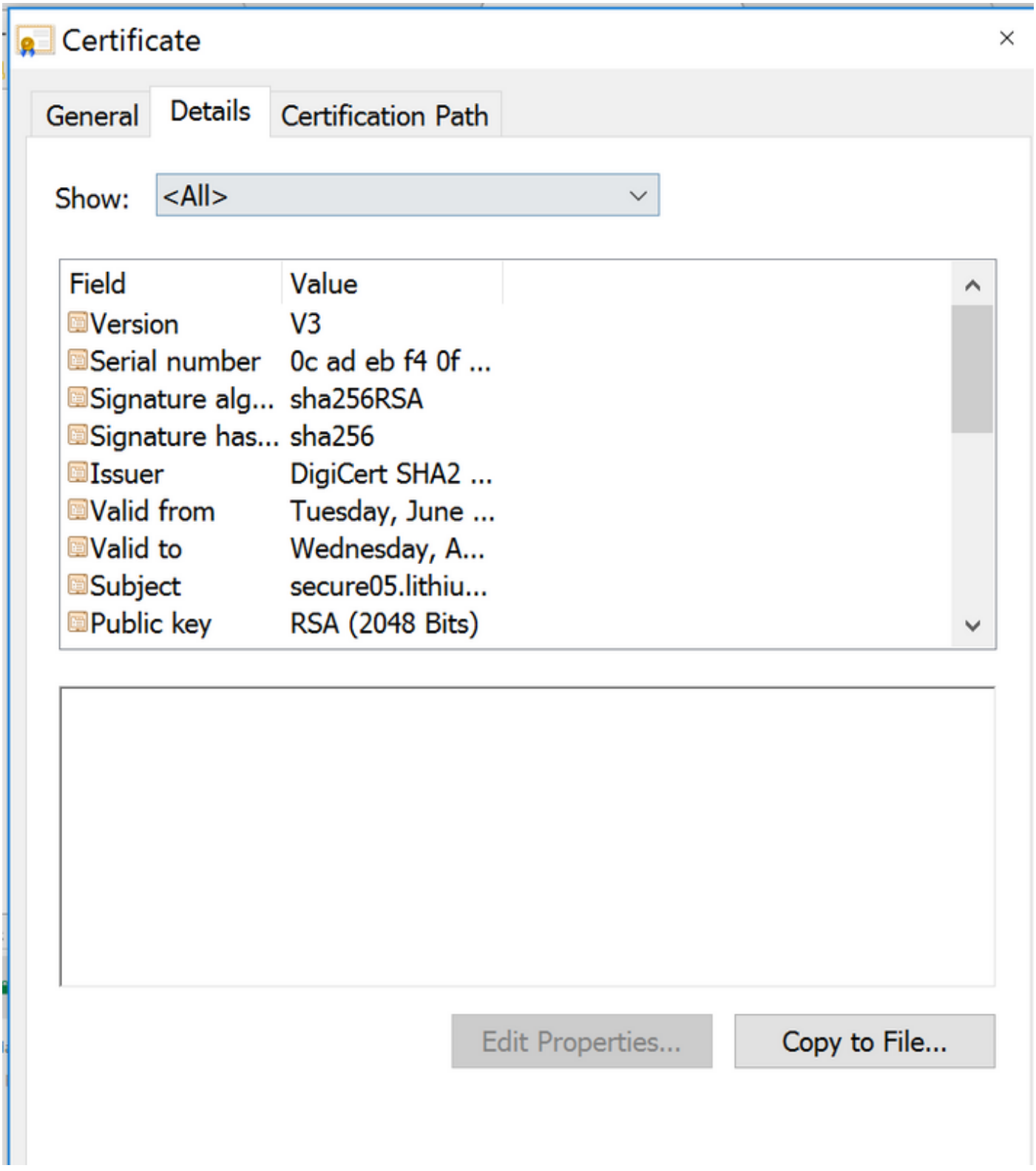
Шаг 24. Выберите **View Certificate** как показано в образе.



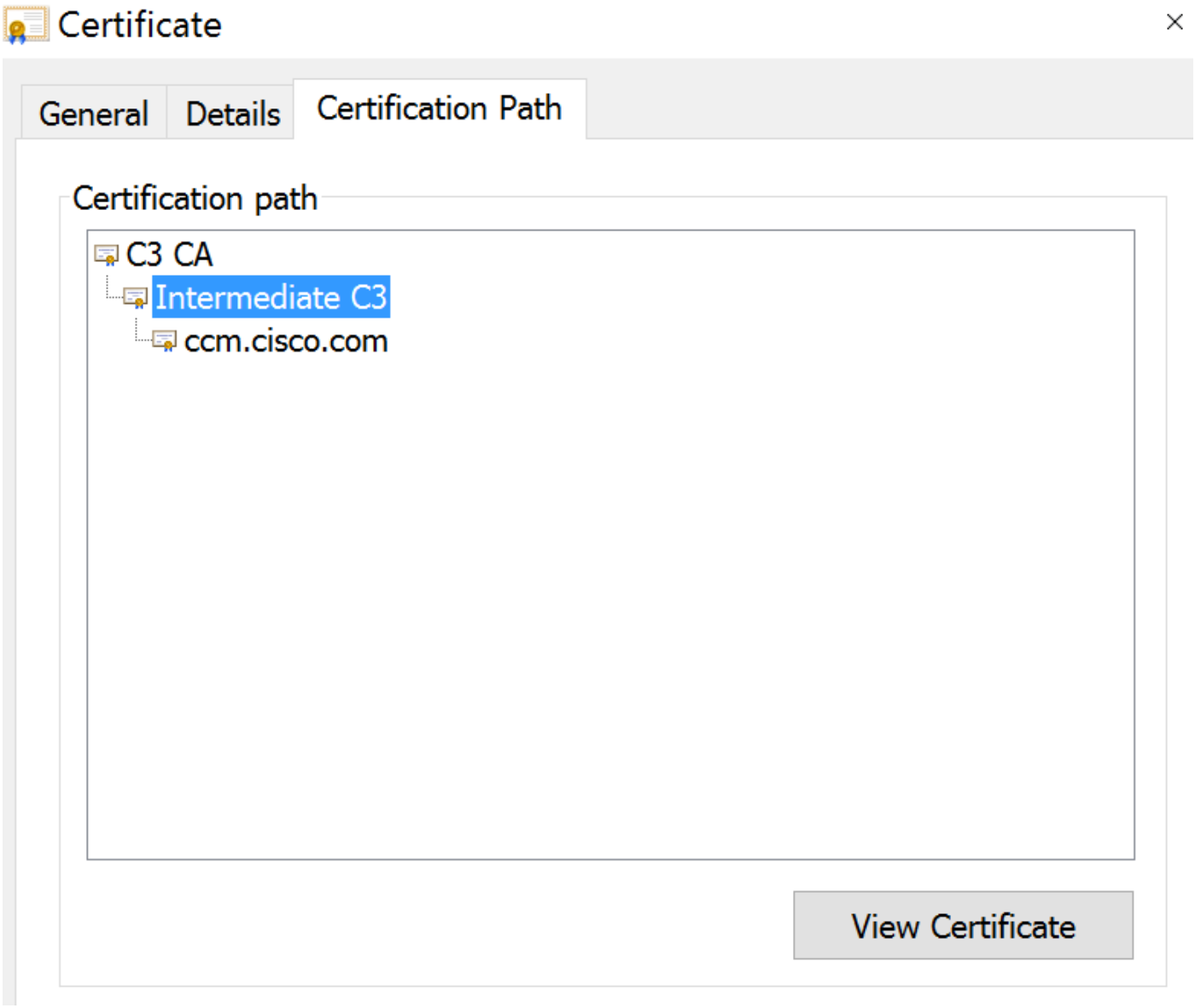
Шаг 25. Выберите **Details** как показано в образе.



Шаг 26. Выберите **Copy To File** как показано в образе.



Шаг 27. Если вы получаете ошибки о недоверяемом CA, то перешли к **Пути сертификации** для просмотра Промежуточного звена и Корневого сертификата. Можно щелкнуть по ним и просмотреть их сертификат и также скопировать тех к файлам как показано в образе.



Шаг 28. Как только вам загрузили сертификаты, следуете инструкциям вашей Операционной системы (OS) или Браузера для установки этих сертификатов как полномочий, которым доверяют, и промежуточных полномочий.