Creación de certificados autofirmados con varias URL

Contenido

Introducción

Este documento describe cómo crear un certificado autofirmado que puede utilizar CloudCenter con varias URL.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados
- Linux

Componentes Utilizados

La información de este documento se basa en CentOS7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema

Los certificados que se suministran de forma estándar con CloudCenter, o que se pueden crear con el uso del asistente de configuración de Cisco Call Manager (CCM), no tienen un nombre alternativo de asunto (SAN) que determinados exploradores, como Google Chrome, tratan como un error y le advierten. Esto se puede invalidar, pero sin SAN, un certificado sólo puede ser válido desde una dirección URL específica.

Por ejemplo, si tiene un certificado válido para la dirección IP 10.11.12.13, si tiene un nombre de sistema de nombres de dominio (DNS) de www.opencart.com, recibe un error de certificado porque esa dirección URL no es para la que está el certificado (esto es cierto incluso si

www.opencart.com aparece en el archivo de hosts como el que pertenece a 10.11.1 2.13). Esto puede aparecer si los subarrendatarios de CloudCenter utilizan Single Sign On (SSO), ya que cada servidor SSO tiene su propia URL.

Solución

La forma más sencilla de solucionar este problema es crear un nuevo certificado autofirmado que tenga SAN que enumere cualquier URL que le dirija a la misma dirección IP. La guía es un intento de aplicar prácticas recomendadas a este proceso.

Paso 1. Navegue hasta el **directorio raíz** y cree una nueva carpeta para alojar los certificados:

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

Paso 2. Desplácese hasta la nueva carpeta y realice subcarpetas para organizar los certificados, las claves privadas y los registros.

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

Paso 3. Copie el contenido de **CAopenssl.conf a /root/ca/openssl.cnf**

> **Nota:** Este archivo contiene las opciones de configuración de una autoridad de certificación (CA) y las opciones predeterminadas que podrían ser apropiadas para CloudCenter.

Paso 4. Genere una clave privada y un certificado para la 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
```

Paso 5. Su CA es la forma definitiva de verificar que cualquier certificado es válido, a este certificado nunca se debe acceder por personas no autorizadas y nunca se debe exponer a Internet. Debido a esta restricción, debe crear una CA intermedia que firme el certificado final, lo que crea una interrupción en la que si el certificado de autoridad intermedia se ve comprometido, se puede revocar y emitir uno nuevo.

Paso 6. Cree un nuevo subdirectorio para la CA intermedia.

```
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
```

Paso 7. Copie el contenido de **Intermediateopenssl.conf** a **/root/ca/intermediate/openssl.cnf** .

> **Nota:** Este archivo contiene opciones de configuración casi idénticas para la CA, excepto algunos pequeños ajustes para que sea específico para un intermedio.

Paso 8. Genere la clave intermedia y el certificado.

```
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
```

Paso 9. Firme el certificado intermedio con el certificado CA, esto genera una cadena de confianza que el explorador utiliza para verificar la autenticidad de un certificado.

```
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
```

Paso 10. Cree una cadena de CA, ya que no desea que la CA esté en Internet, puede crear una cadena de CA que los exploradores utilicen para verificar la autenticidad hasta la 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
```

Paso 11. Cree una nueva clave y certificado para 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
```

Paso 12. Esto tiene todos los campos obligatorios en el comando y debe editarse manualmente.

- **/C=US** se refiere al país (límite de 2 caracteres)
- **/ST=NC** se refiere al estado y puede incluir espacios
- **/O=Cisco** hace referencia a la Organización
- **/CN=ccm.com** hace referencia al nombre común, que debe ser la dirección URL principal utilizada para acceder al CCM.
- **SAN\nsubjectAltName=** son los nombres alternativos, el nombre común debe estar en esta lista y no hay límite para la cantidad de SAN que tiene.

Paso 13. Firme el certificado final con el uso del certificado intermedio.

```
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
```

Paso 14. Verifique que el certificado se haya firmado correctamente.

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

Paso 15. Puede devolver un OK o un Fail.

Paso 16. Copie el nuevo certificado, su clave y la cadena CA en la carpeta **Catalina**.

```
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
```

Paso 17. Otorgue propiedad de cliqruser y establezca los permisos correctamente.

```
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
```

Paso 18. Realice una copia de seguridad del archivo **server.xml** antes de realizar cambios.

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

Paso 19. Editar **server.xml:**

1. Busque la sección que comienza con **<Connector port="10443" maxHttpHeaderSize="8192"**
2. Cambie el **archivo SSLCcertificate** para que apunte a ccm.com.crt
3. Cambie **SSLCcertificateKeyFile** para que señale a ccm.com.key
4. Cambie **SSLCACcertificateFile** para señalar a ca-chain.crt

Paso 20. Reinicie Tomcat.

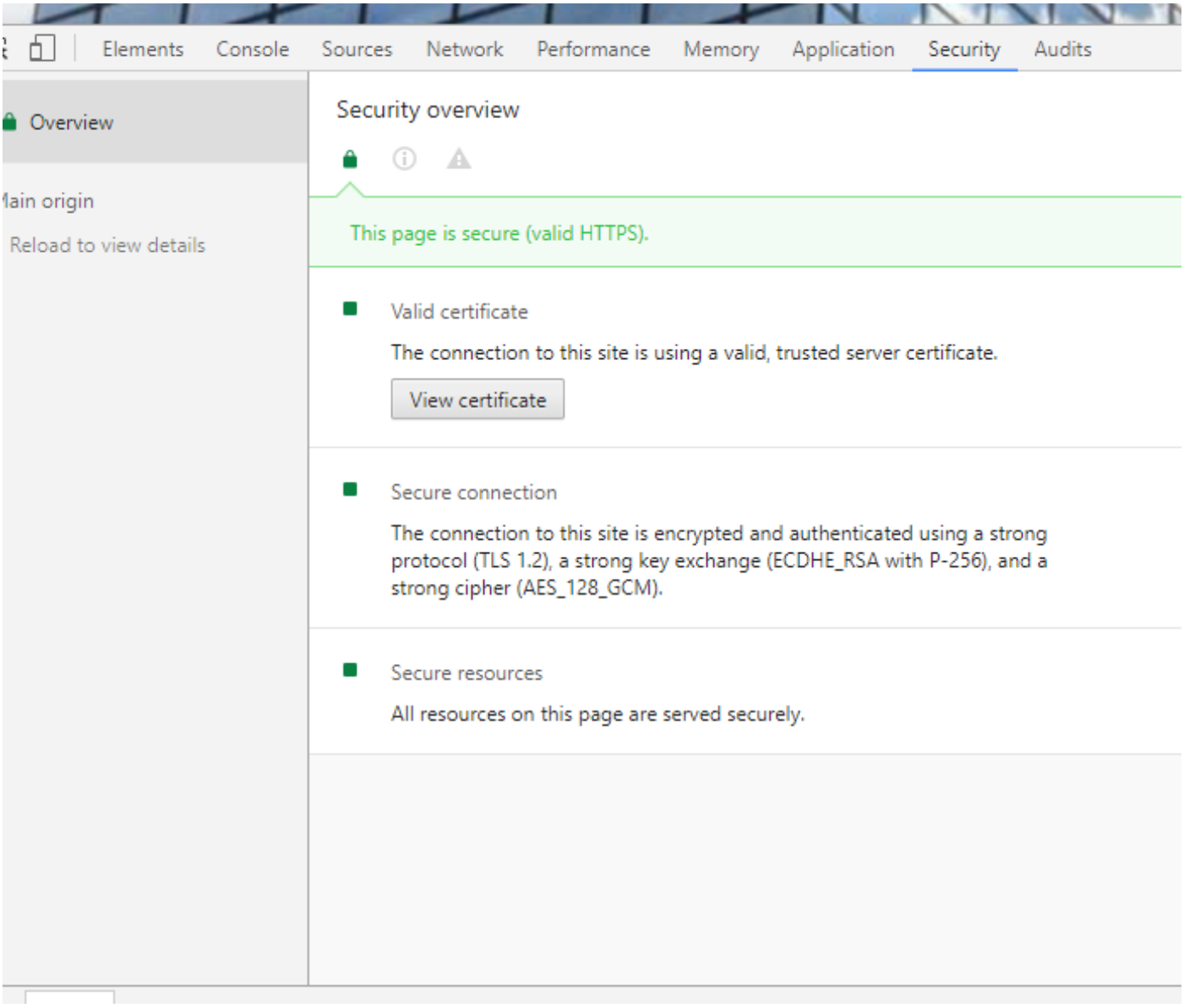
```
service tomcat stop
service tomcat start
```

Paso 21. El CCM ahora utiliza el nuevo certificado que es válido para todos los nombres DNS y direcciones IP especificados en el Paso 13.

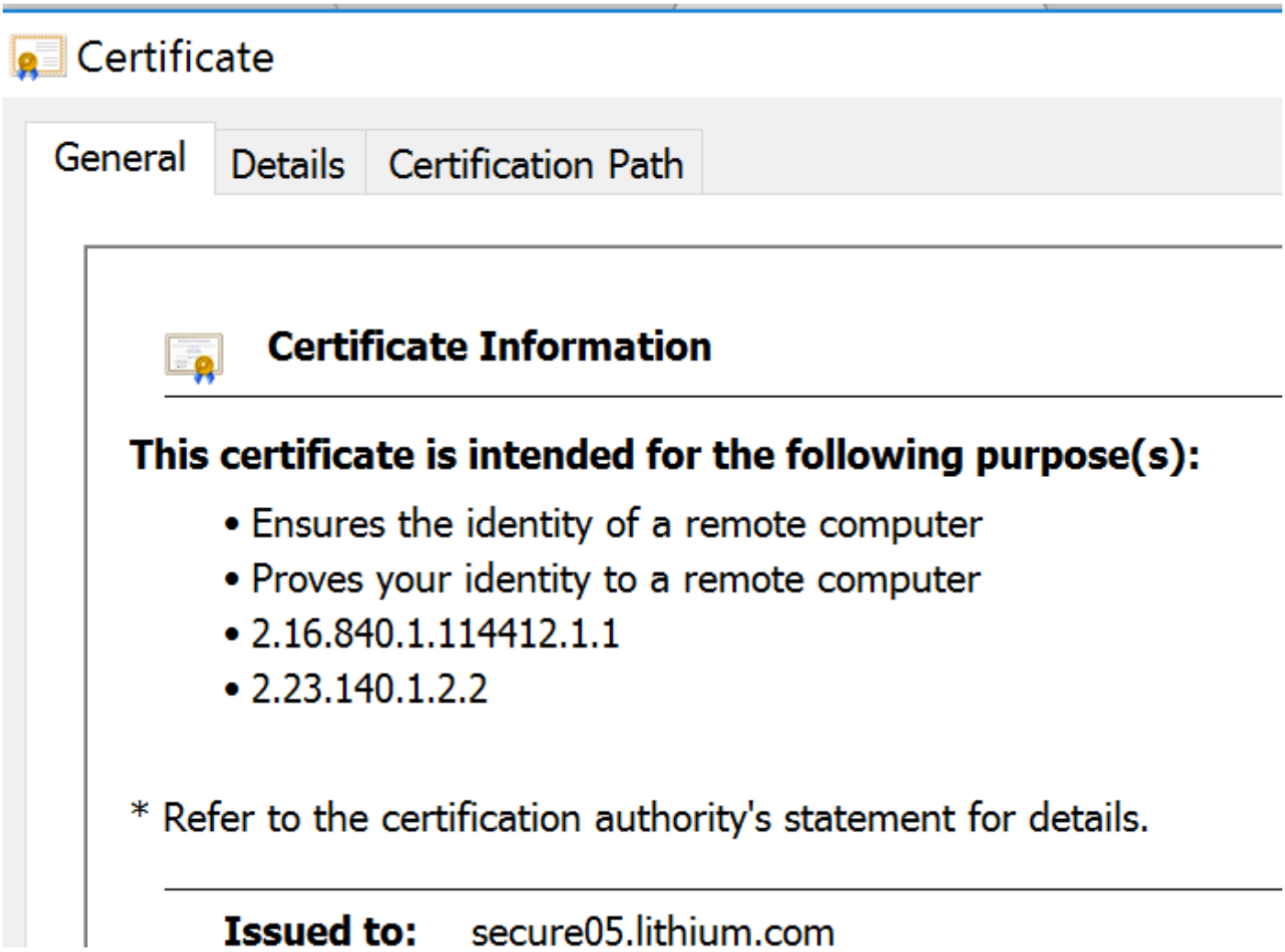
Paso 22. Como la CA se creó en el momento de la guía, los exploradores no la reconocerán como válida de forma predeterminada, por lo que debe importar manualmente el certificado.

Paso 23. Navegue hasta **CCM** con cualquier URL válida y presione **Ctrl+Mayús+i**, esto abre las herramientas del desarrollador.

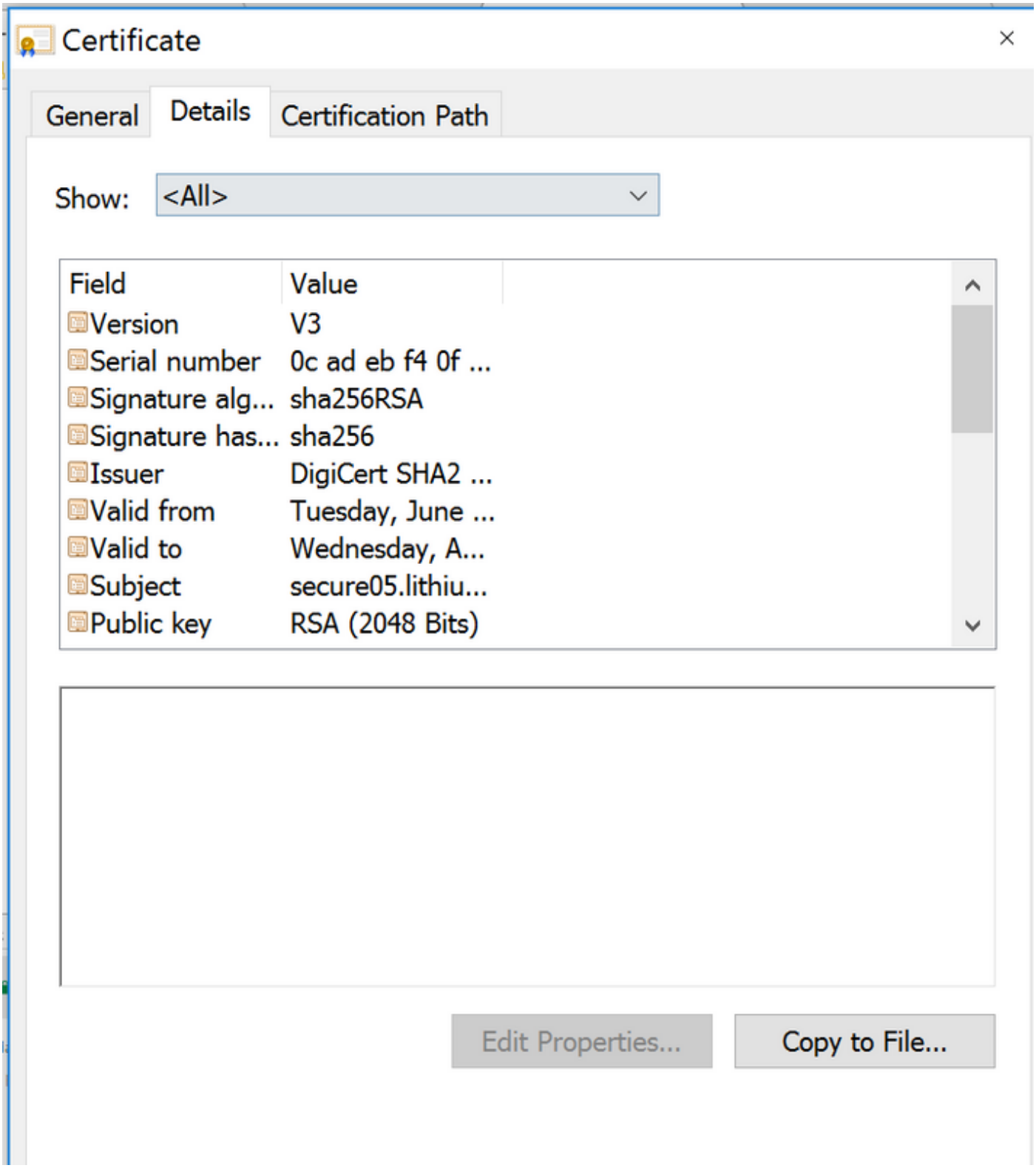
Paso 24. Seleccione **Ver certificado** como se muestra en la imagen.



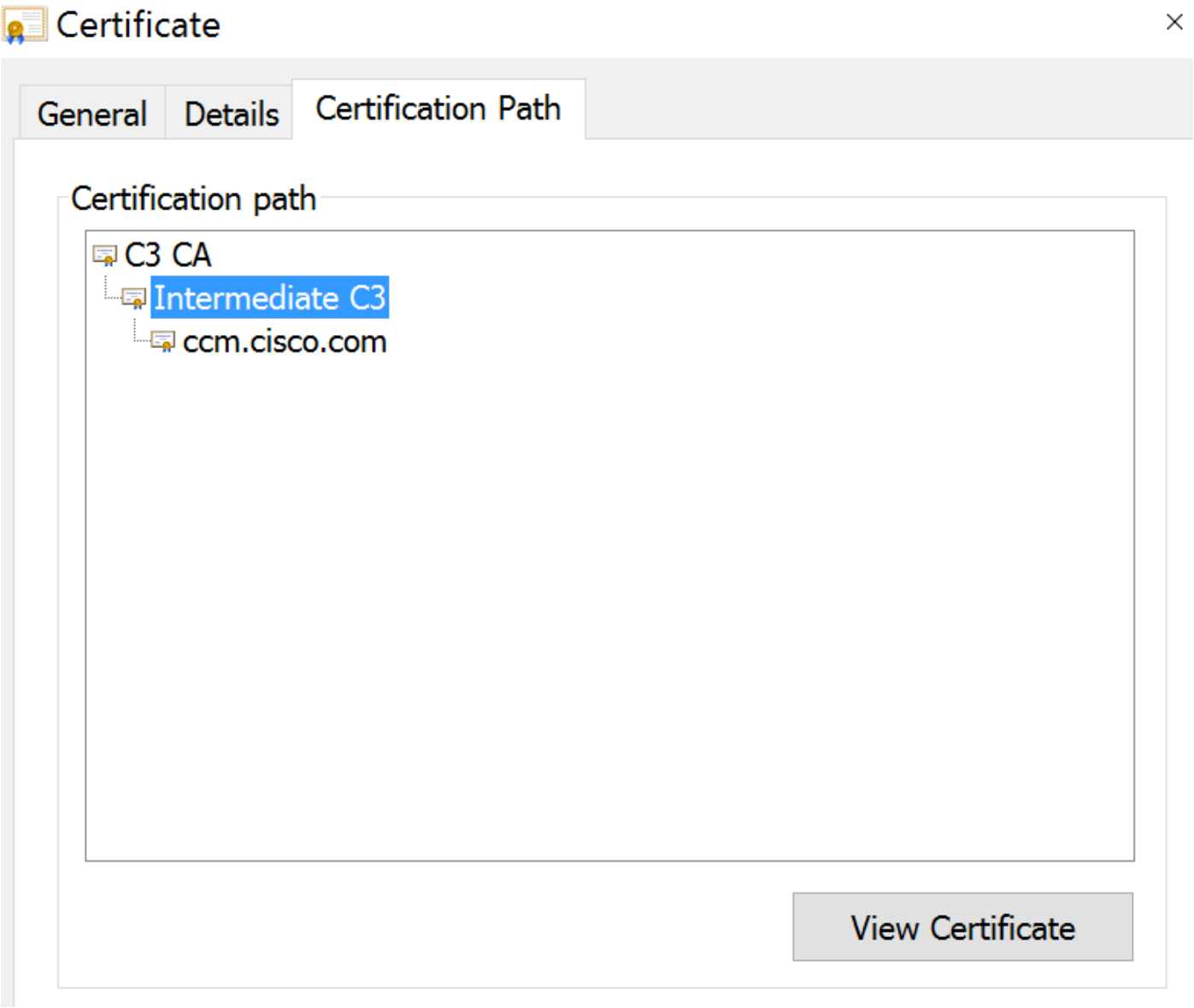
Paso 25. Seleccione **Detalles** como se muestra en la imagen.



Paso 26. Seleccione **Copiar a archivo** como se muestra en la imagen.



Paso 27. Si obtiene errores sobre una CA no confiable, navegue hasta **Trayectoria de certificación** para ver el certificado intermedio y raíz. Puede hacer clic en ellos y ver su certificado, así como copiarlos en los archivos como se muestra en la imagen.



Paso 28. Una vez descargados los certificados, siga las instrucciones del sistema operativo (OS) o del navegador para instalar estos certificados como autoridad de confianza y autoridades intermedias.