Solución de problemas de instalación de certificados en WLC

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Troubleshoot](#)
[Escenario 1. La contraseña proporcionada para descifrar la clave privada es incorrecta o no se ha proporcionado ninguna contraseña](#)
[Situación hipotética 2. No hay certificado de CA intermedio en la cadena](#)
[Situación hipotética 3. No hay certificado de CA raíz en la cadena](#)
[Situación hipotética 4. No hay certificados de CA en la cadena](#)
[Situación hipotética 5. Sin clave privada](#)
[Información Relacionada](#)

Introducción

Este documento describe los problemas causados por el uso de certificados de terceros en el Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de LAN inalámbrica (WLC)
- Public Key Infrastructure (PKI)
- Certificados X.509

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC 3504 con versión de firmware 8.10.105.0
- OpenSSL 1.0.2p para la herramienta de línea de comandos
- máquina con Windows 10
- Cadena de certificados de la autoridad de certificación (CA) de laboratorio privada con tres certificados (hoja, intermedio, raíz)
- Servidor de protocolo de transferencia de archivos trivial (TFTP) para la transferencia de archivos.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En AireOS WLC, puede instalar certificados de terceros para ser utilizados por WebAuth y WebAdmin. En la instalación, el WLC espera un único PEM (Privacy Enhanced Mail) con todos los certificados de la cadena hasta el certificado de la CA raíz y la clave privada. Los detalles sobre este procedimiento se documentan en Generar CSR para Certificados de Terceros y Descargar Certificados Encadenados al WLC.

Este documento expande y muestra con más detalle los errores de instalación más comunes con ejemplos de depuración y resolución para cada escenario. Las salidas de depuración utilizadas a lo largo de este documento son de **debug transfer all enable** y **debug pm pki enable** en el WLC. Se utilizó TFTP para transferir el archivo de certificados.

Troubleshoot

Escenario 1. La contraseña proporcionada para descifrar la clave privada es incorrecta o no se ha proporcionado ninguna contraseña

<#root>

```
*TransferTask: Apr 21 03:51:20.737:

Add ID Cert: Adding certificate & private key using password check123


*TransferTask: Apr 21 03:51:20.737:

Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) to ID table using password check123


*TransferTask: Apr 21 03:51:20.737: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 03:51:20.737: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Apr 21 03:51:20.737: Decode & Verify PEM Cert: Cert/Key Length 6276 & VERIFY
*TransferTask: Apr 21 03:51:20.741: Decode & Verify PEM Cert: X509 Cert Verification return code: 1
*TransferTask: Apr 21 03:51:20.741: Decode & Verify PEM Cert: X509 Cert Verification result text: ok
*TransferTask: Apr 21 03:51:20.741:

Add Cert to ID Table: Decoding PEM-encoded Private Key using password check123


*TransferTask: Apr 21 03:51:20.799:

Decode PEM Private Key: Error reading Private Key from PEM-encoded PKCS12 bundle using password check123


*TransferTask: Apr 21 03:51:20.799: Add ID Cert: Error decoding / adding cert to ID cert table (verifyCh
*TransferTask: Apr 21 03:51:20.799: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 03:51:20.799:

RESULT_STRING: Error installing certificate.
```

Solución: asegúrese de que se proporcione la contraseña correcta para que el WLC pueda decodificarlo para la instalación.

Situación hipotética 2. No hay certificado de CA intermedio en la cadena

<#root>

```
*TransferTask: Apr 21 04:34:43.319: Add ID Cert: Adding certificate & private key using password Cisco12
*TransferTask: Apr 21 04:34:43.319: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) t
*TransferTask: Apr 21 04:34:43.319: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 04:34:43.319: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Apr 21 04:34:43.319: Decode & Verify PEM Cert: Cert/Key Length 4840 & VERIFY
*TransferTask: Apr 21 04:34:43.321: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:34:43.321:
```

Decode & Verify PEM Cert: X509 Cert Verification result text: unable to get local issuer certificate

```
*TransferTask: Apr 21 04:34:43.321:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth: unable to get local issuer certifi

```
*TransferTask: Apr 21 04:34:43.321: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:34:43.321: Add ID Cert: Error decoding / adding cert to ID cert table (verifyCh
*TransferTask: Apr 21 04:34:43.321: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 04:34:43.321: RESULT_STRING: Error installing certificate.
```

Solución: valide los campos **Emisor** y **Identificador de clave de autoridad X509v3** del certificado de WLC para validar el certificado de CA que firmó el certificado. Si la CA proporcionó el certificado de CA intermedia, se puede utilizar para realizar la validación. De lo contrario, solicite el certificado a su CA.

Este comando OpenSSL se puede utilizar para validar estos detalles en cada certificado:

<#root>

```
>
```

openssl x509 -in

wlc.crt

-text -noout

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
50:93:16:83:04:d5:6b:db:26:7c:3a:13:f3:95:32:7e
Signature Algorithm: sha256WithRSAEncryption
```

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA

```
Validity
Not Before: Apr 21 03:08:05 2020 GMT
Not After : Apr 21 03:08:05 2021 GMT
Subject: C=US, O=TAC Lab, CN=guest.wirelesslab.local

...

X509v3 extensions:
```

X509v3 Authority Key Identifier:

keyid:27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12

<#root>

>

openssl x509 -in

int-ca.crt

-text -noout

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:97
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA
Validity
Not Before: Apr 21 02:51:03 2020 GMT
Not After : Apr 19 02:51:03 2030 GMT
```

Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA

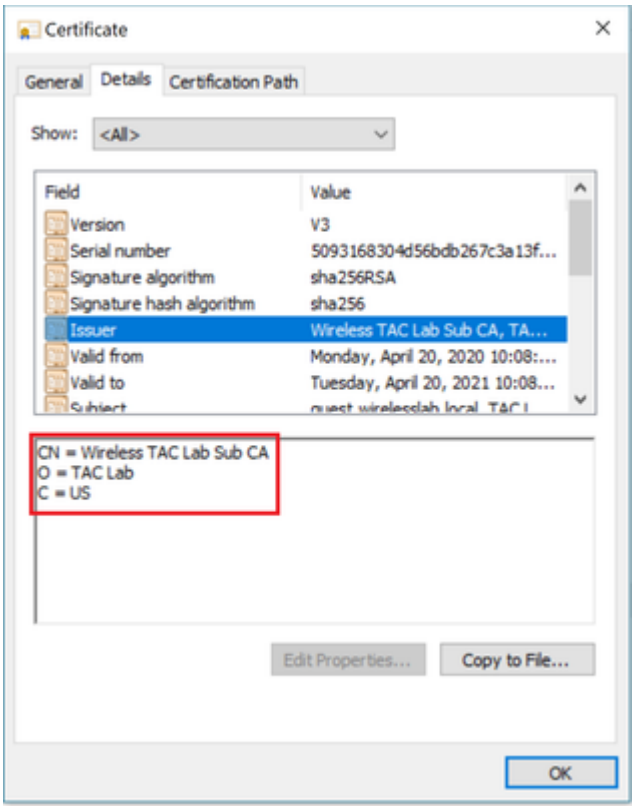
...

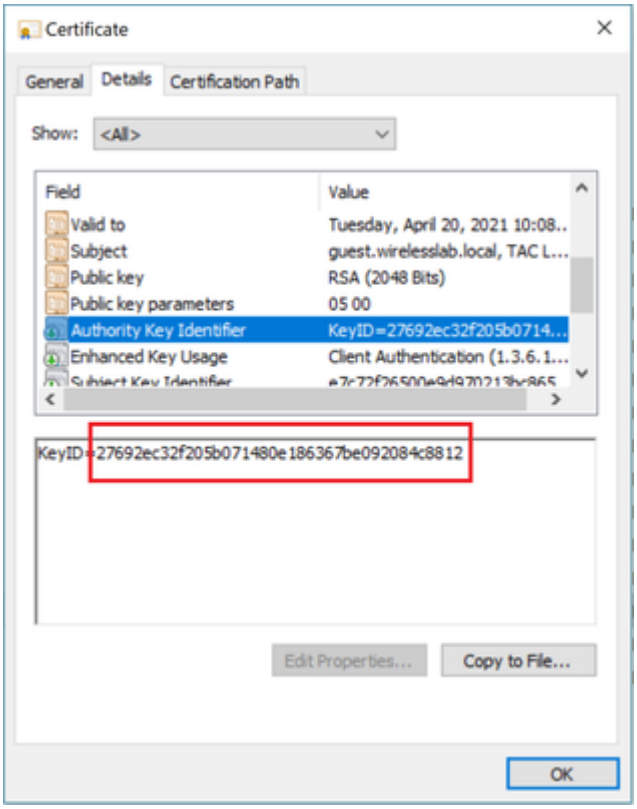
X509v3 Subject Key Identifier:

27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12

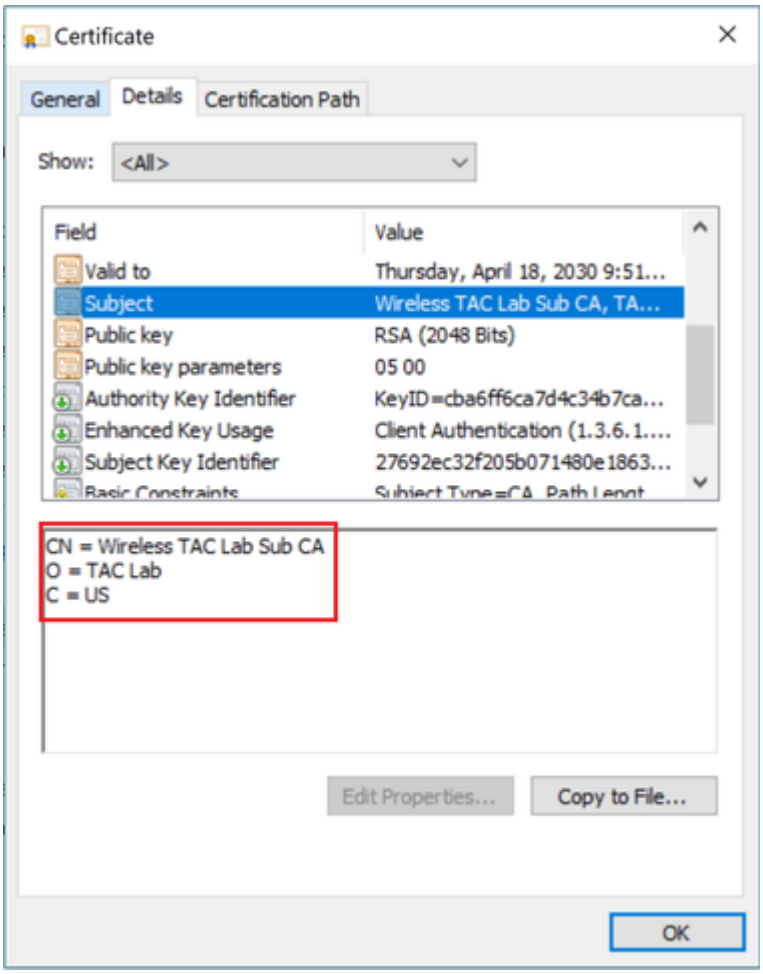
Como alternativa, si utiliza Windows, asigne al certificado una extensión **.crt** y haga doble clic para validar estos detalles.

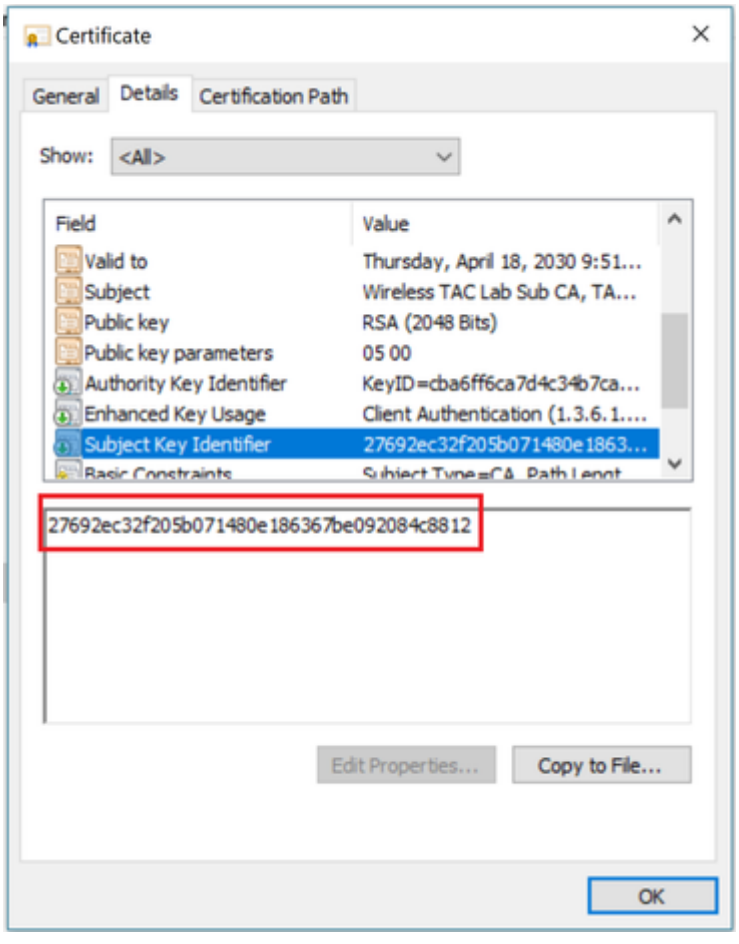
Certificado WLC:





Certificado de CA intermedio:


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Thursday, April 18, 2030 9:51...
Subject
Wireless TAC Lab Sub CA, TA...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
KeyID=cba6ff6ca7d4c34b7ca...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Subject Key Identifier
27692ec32f205b071480e1863...
CN = Wireless TAC Lab Sub CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Thursday, April 18, 2030 9:51...
Subject
Wireless TAC Lab Sub CA, TA...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
KeyID=cba6ff6ca7d4c34b7ca...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Subject Key Identifier
27692ec32f205b071480e1863...
27692ec32f205b071480e186367be092084c8812
Edit Properties...
Copy to File...
OK

Una vez identificado el certificado de CA intermedia, continúe con la cadena según corresponda y vuelva a instalar.

Situación hipotética 3. No hay certificado de CA raíz en la cadena

<#root>

```
*TransferTask: Apr 21 04:28:09.643: Add ID Cert: Adding certificate & private key using password Cisco12
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) t
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 04:28:09.643: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Apr 21 04:28:09.643: Decode & Verify PEM Cert: Cert/Key Length 4929 & VERIFY
*TransferTask: Apr 21 04:28:09.645: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:28:09.645:
```

Decode & Verify PEM Cert: X509 Cert Verification result text: unable to get issuer certificate

```
*TransferTask: Apr 21 04:28:09.645:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 1 depth: unable to get issuer certificate

```
*TransferTask: Apr 21 04:28:09.646: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:28:09.646: Add ID Cert: Error decoding / adding cert to ID cert table (verifyCh
```

Solución: Este escenario es similar al escenario 2, pero esta vez con el certificado intermedio cuando se valida el emisor (CA raíz). Se pueden seguir las mismas instrucciones con la verificación de los campos **Emisor** y **Identificador de clave de autoridad X509v3** en el certificado de CA intermedio para validar la CA raíz.

Este comando OpenSSL se puede utilizar para validar estos detalles en cada certificado:

<#root>

>

openssl x509 -in

int-ca.crt

-text -noout

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:97
Signature Algorithm: sha256WithRSAEncryption
```

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

```
Validity
Not Before: Apr 21 02:51:03 2020 GMT
Not After : Apr 19 02:51:03 2030 GMT
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA
```

...

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

<#root>

>

openssl x509 -in

root-ca.crt

-text -noout

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:96
Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

Validity
Not Before: Apr 21 02:40:24 2020 GMT
Not After : Apr 19 02:40:24 2030 GMT

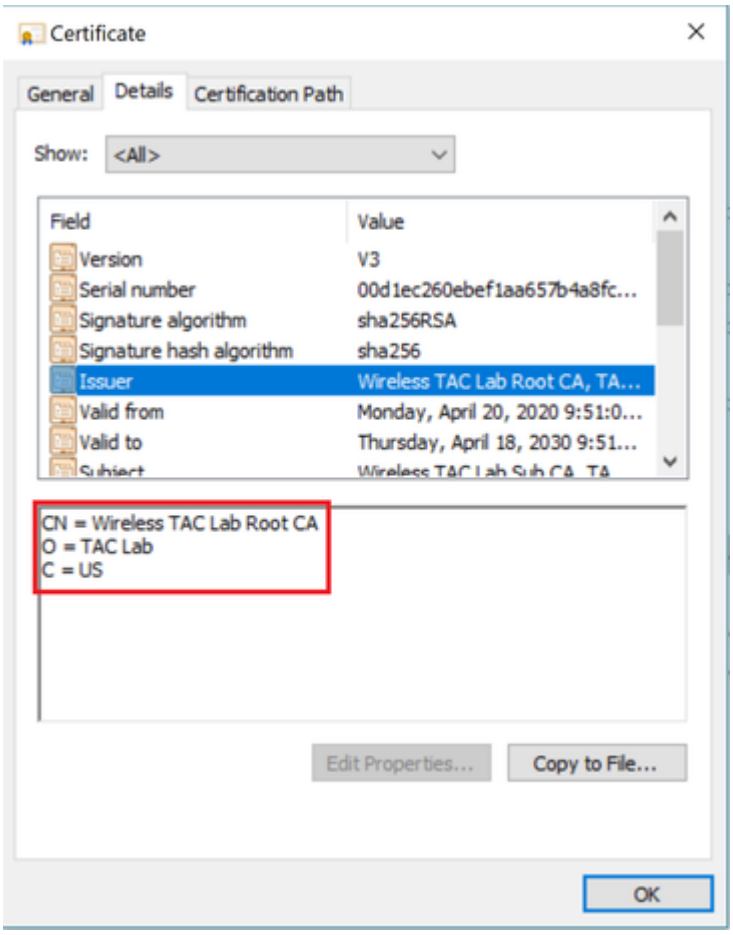
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

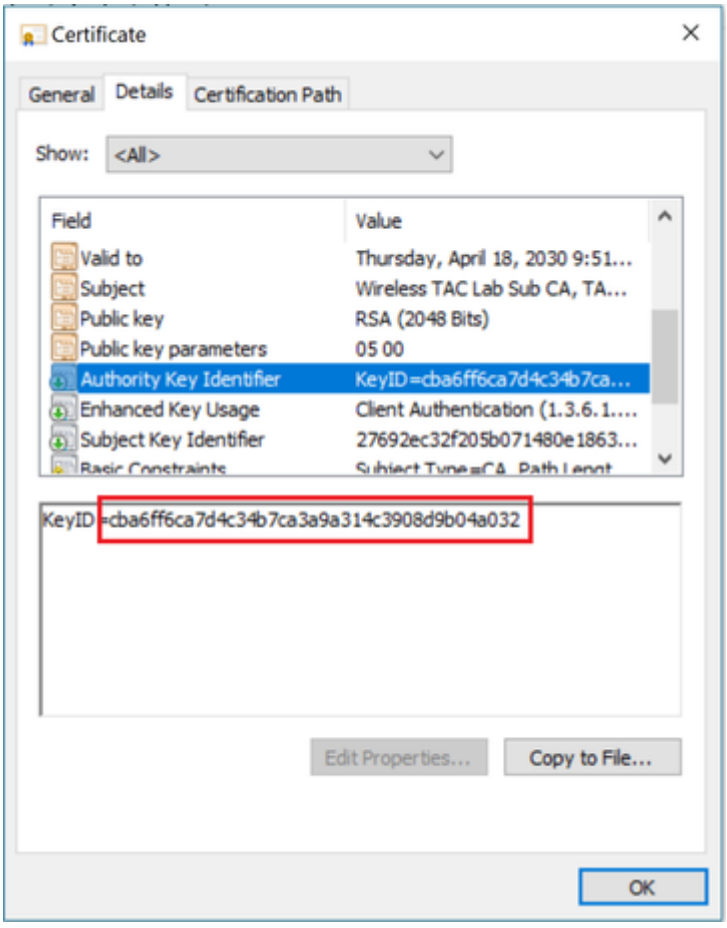
...

X509v3 Subject Key Identifier:

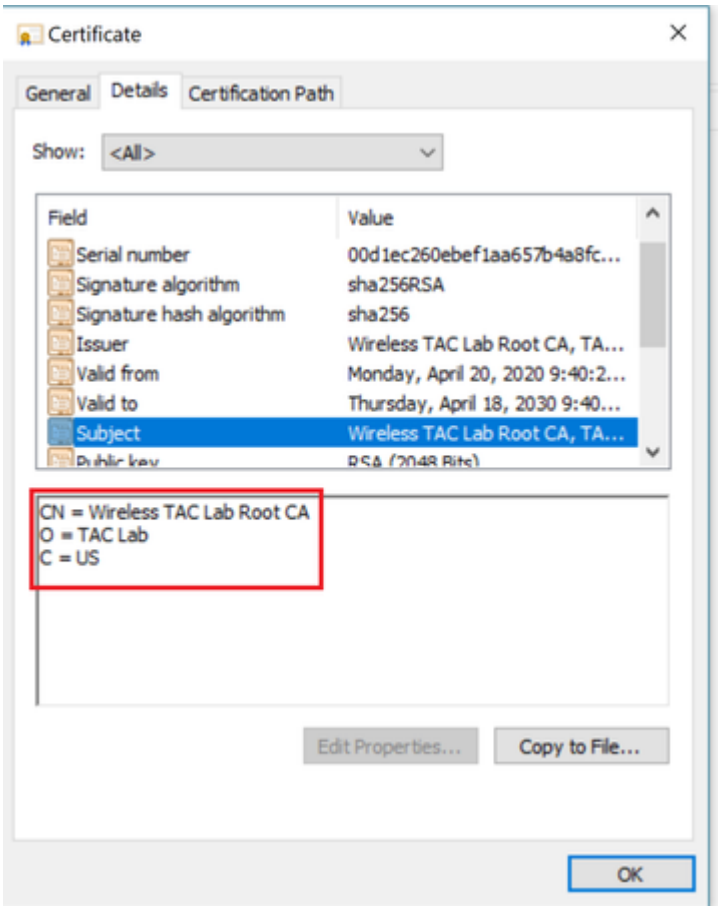
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

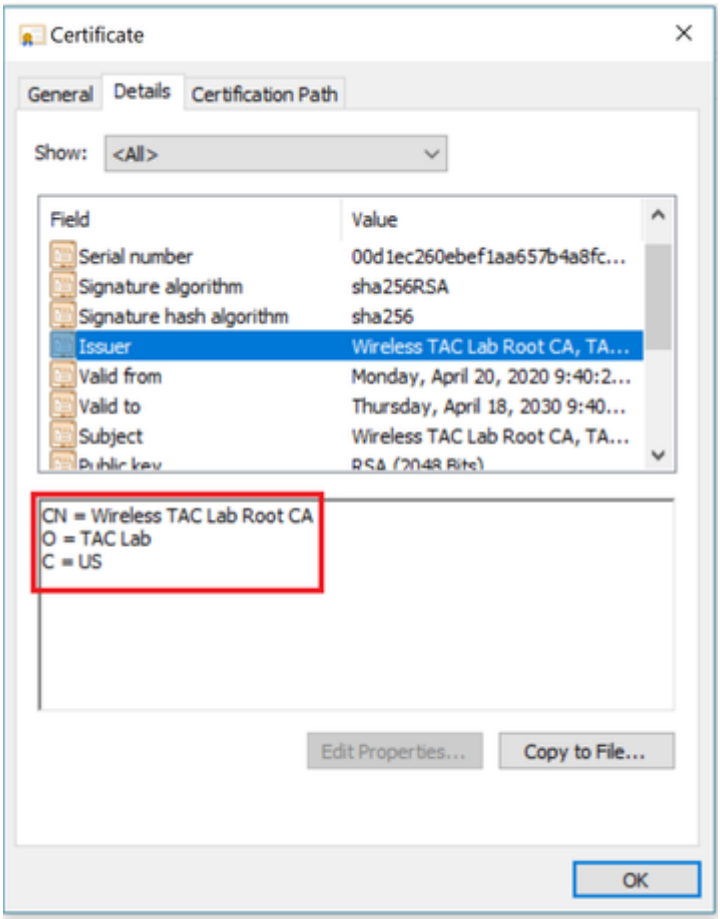
Certificado CA intermedio

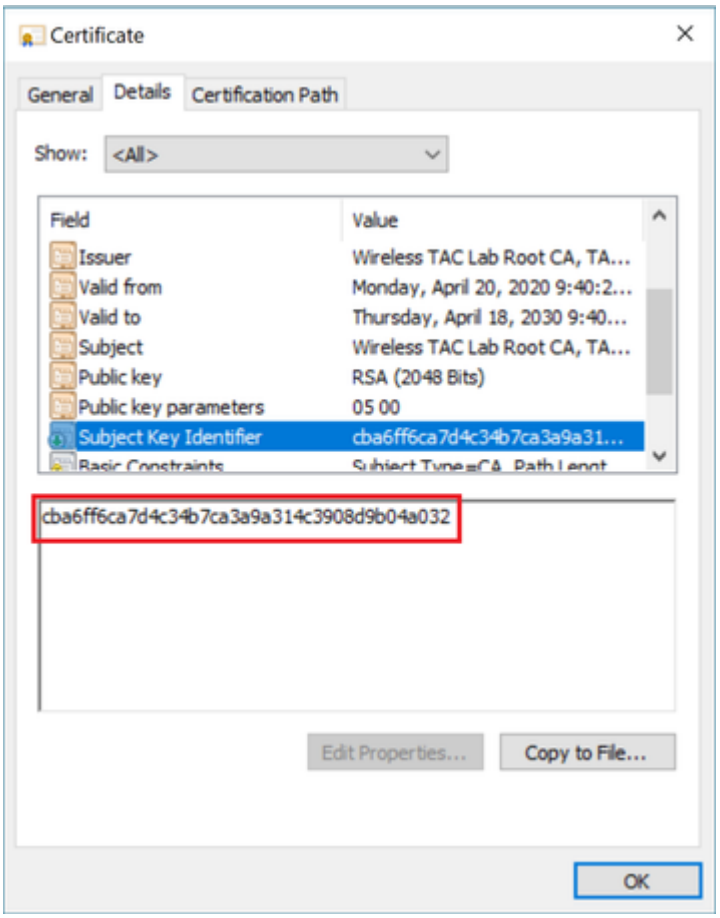




Certificado de CA raíz:


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:40:2...
Valid to
Thursday, April 18, 2030 9:40...
Subject
Wireless TAC Lab Root CA, TA...
Public key
RSA (2048 Bits)
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:40:2...
Valid to
Thursday, April 18, 2030 9:40...
Subject
Wireless TAC Lab Root CA, TA...
Public key
RSA (2048 Bits)
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK



Una vez identificado el certificado de CA raíz (el emisor y el sujeto son iguales), continúe con la cadena en consecuencia y vuelva a instalar.

> **Nota**: Este documento utiliza tres cadenas de certificados (hoja, CA intermedia, CA raíz), que es el escenario más común. Puede haber situaciones en las que estén involucrados 2 certificados de CA intermedios. Se puede utilizar la misma directriz de este escenario hasta que se encuentre el certificado de CA raíz.

Situación hipotética 4. No hay certificados de CA en la cadena

<#root>

```
*TransferTask: Apr 21 04:56:50.272: Add ID Cert: Adding certificate & private key using password Cisco12
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) t
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 04:56:50.272: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Apr 21 04:56:50.272: Decode & Verify PEM Cert: Cert/Key Length 3493 & VERIFY
*TransferTask: Apr 21 04:56:50.273: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:56:50.273:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth: unable to get local issuer certifi

```
*TransferTask: Apr 21 04:56:50.274: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:56:50.274: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 04:56:50.274: RESULT_STRING: Error installing certificate.
```

Solución: sin ningún otro certificado en el archivo que no sea el certificado WLC, la validación falla en la **Verificación a 0 de profundidad**. El archivo se puede abrir en un editor de texto para validarlo. Se pueden seguir las pautas de los escenarios 2 y 3 para identificar la cadena hasta la CA raíz y volver a encadenar en consecuencia y reinstalar.

Situación hipotética 5. Sin clave privada

<#root>

```
*TransferTask: Apr 21 05:02:34.764: Add WebAuth Cert: Adding certificate & private key using password
*TransferTask: Apr 21 05:02:34.764: Add ID Cert: Adding certificate & private key using password
*TransferTask: Apr 21 05:02:34.764: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) t
*TransferTask: Apr 21 05:02:34.764: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 05:02:34.764: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Apr 21 05:02:34.764: Decode & Verify PEM Cert: Cert/Key Length 3918 & VERIFY
*TransferTask: Apr 21 05:02:34.767: Decode & Verify PEM Cert: X509 Cert Verification return code: 1
*TransferTask: Apr 21 05:02:34.767: Decode & Verify PEM Cert: X509 Cert Verification result text: ok
*TransferTask: Apr 21 05:02:34.768: Add Cert to ID Table: Decoding PEM-encoded Private Key using passwor
*TransferTask: Apr 21 05:02:34.768:

Retrieve CSR Key: can't open private key file for ssl cert.



*TransferTask: Apr 21 05:02:34.768:

Add Cert to ID Table: No Private Key



*TransferTask: Apr 21 05:02:34.768: Add ID Cert: Error decoding / adding cert to ID cert table (verifyCh
*TransferTask: Apr 21 05:02:34.768: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 05:02:34.768: RESULT_STRING: Error installing certificate.
```

Solución: el WLC espera que la clave privada se incluya en el archivo si la solicitud de firma de certificado (CSR) se generó externamente y debe encadenarse en el archivo. En el caso de que el CSR fue generado en el WLC, asegúrese de que el WLC no se recarga antes de la instalación, de lo contrario la clave privada se pierde.

Información Relacionada

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).