أستكشاف أخطاء تثبيت الشهادة وإصلاحها على WLC

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
استكشاف الأخطاء وإصلاحها
السيناريو 1. كلمة المرور المقدمة لفك تشفير المفتاح الخاص غير صحيحة أو لم يتم توفير كلمة مرور
السيناريو 2. الوجود الشهادة CA وسيطة في السلسلة
السيناريو 3. الوجود شهادة مرجع مصدق جذري في السلسلة
السيناريو 4. الوجود شهادات مرجع مصدق في السلسلة
السيناريو 5. الوجود مفتاح خاص
معلومات ذات صلة

المقدمة

يصف هذا المستند المشاكل الناجمة عن إستخدام شهادات جهة خارجية على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم في شبكة LAN اللاسلكية (WLC)
- البنية الأساسية للمفتاح العام (PKI)
- شهادات X.509

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- 3504 WLC مع البرنامج الثابت، الإصدار 8.10.105.0
- أداة سطر الأوامر OpenSSL 1.0.2p
- جهاز Windows 10
- سلسلة شهادات من هيئة شهادة المختبر الخاص (CA) مع ثلاث شهادات (طرفية أو

وسيطة أو جذرية)
- خادم بروتوكول نقل الملفات المبسط (TFTP) لنقل الملفات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

على AireOS WLC، يمكنك تثبيت شهادات جهة خارجية ليتم إستخدامها ل WebAuth و WebAdmin. أثناء التثبيت، تتوقع وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وحدة توسعة ذاكرة PEM واحدة (البريد المحسن للخصوصية) تم تنسيق الملف باستخدام كافة الشهادات الموجودة في السلسلة حتى شهادة المرجع المصدق الجذر والمفتاح الخاص. يتم توثيق تفاصيل حول هذا الإجراء في [إنشاء CSR لشهادات الطرف الثالث وتنزيل الشهادات المتسلسلة إلى WLC](#).

يتوسع هذا وثيقة ويبدي أكثر رثر تفصيل الأكثر أخطاء التثبيت شيوعا مع أمثلة تصحيح الأخطاء ودقة لكل سيناريو. مخرجات تصحيح الأخطاء المستخدمة في هذا المستند هي من debug transfer all enable وdebug pm pki enable على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تم إستخدام TFTP لنقل ملف الشهادات.

استكشاف الأخطاء وإصلاحها

السيناريو 1. كلمة المرور المقدمة لفك تشفير المفتاح الخاص غير صحيحة أو لم يتم توفير كلمة مرور

<#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 l
*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 check12
```

```
*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.

الحل: تأكد من توفير كلمة المرور الصحيحة بحيث يمكن ل WLC فك ترميزها للتثبيت.

السيناريو 2. لا توجد شهادة CA وسيطة في السلسلة

<#root>

```
*TransferTask: Apr 21 04:34:43.319: Add ID Cert: Adding certificate & private key using password Cisco1
*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.
```

الحل: التحقق من صحة حقلي معرف مفتاح المرجع Issuer وX509v3 Authority Key Identifier من شهادة WLC للتحقق من شهادة CA التي وقعت على الشهادة. إذا كانت شهادة CA الوسيطة مقدمة من قبل CA، يمكن إستخدامها للتحقق من الصحة. وإلا، اطلب الشهادة إلى المرجع المصدق.

يمكن إستخدام أمر OpenSSL هذا للتحقق من هذه التفاصيل على كل شهادة:

<#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

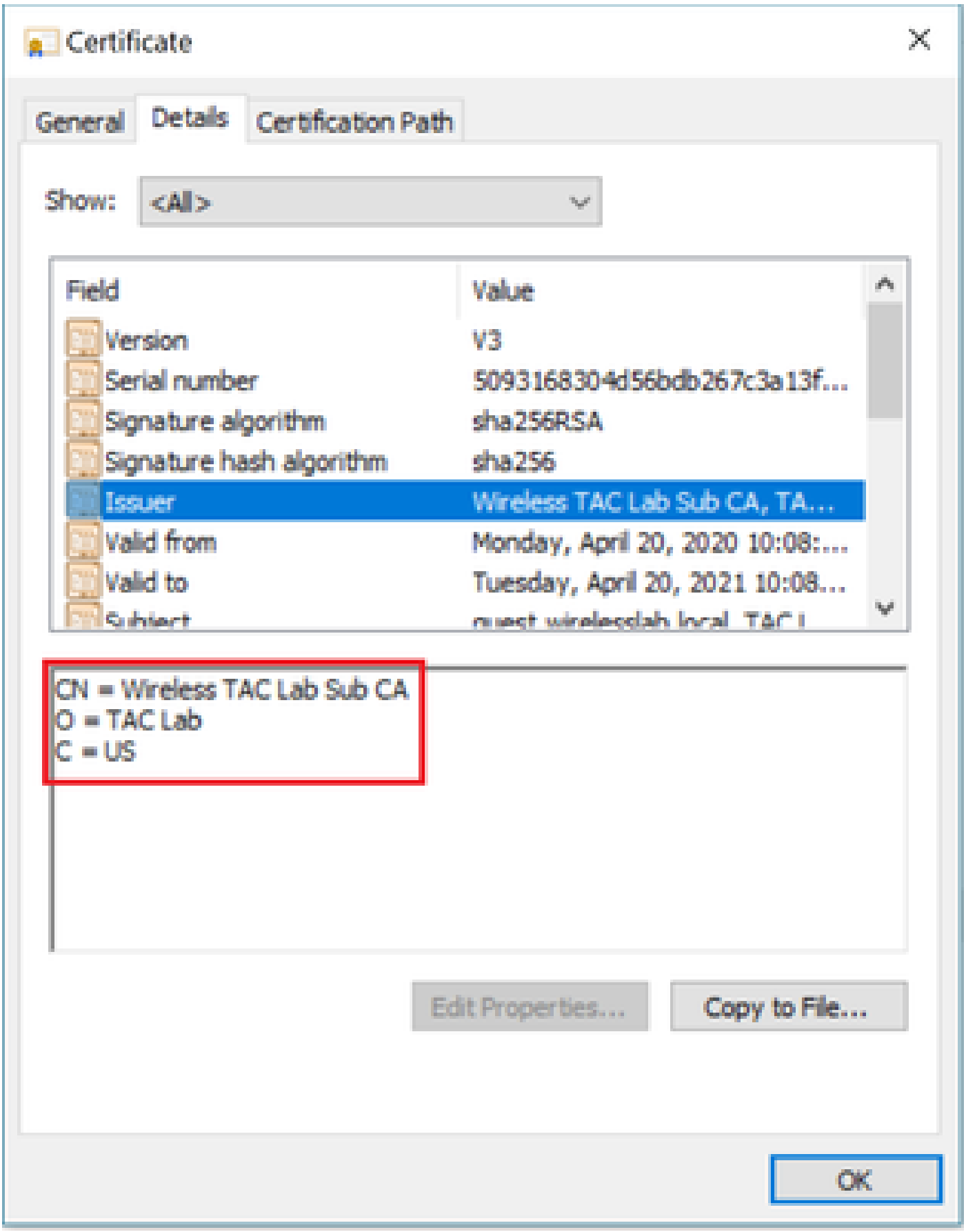
...

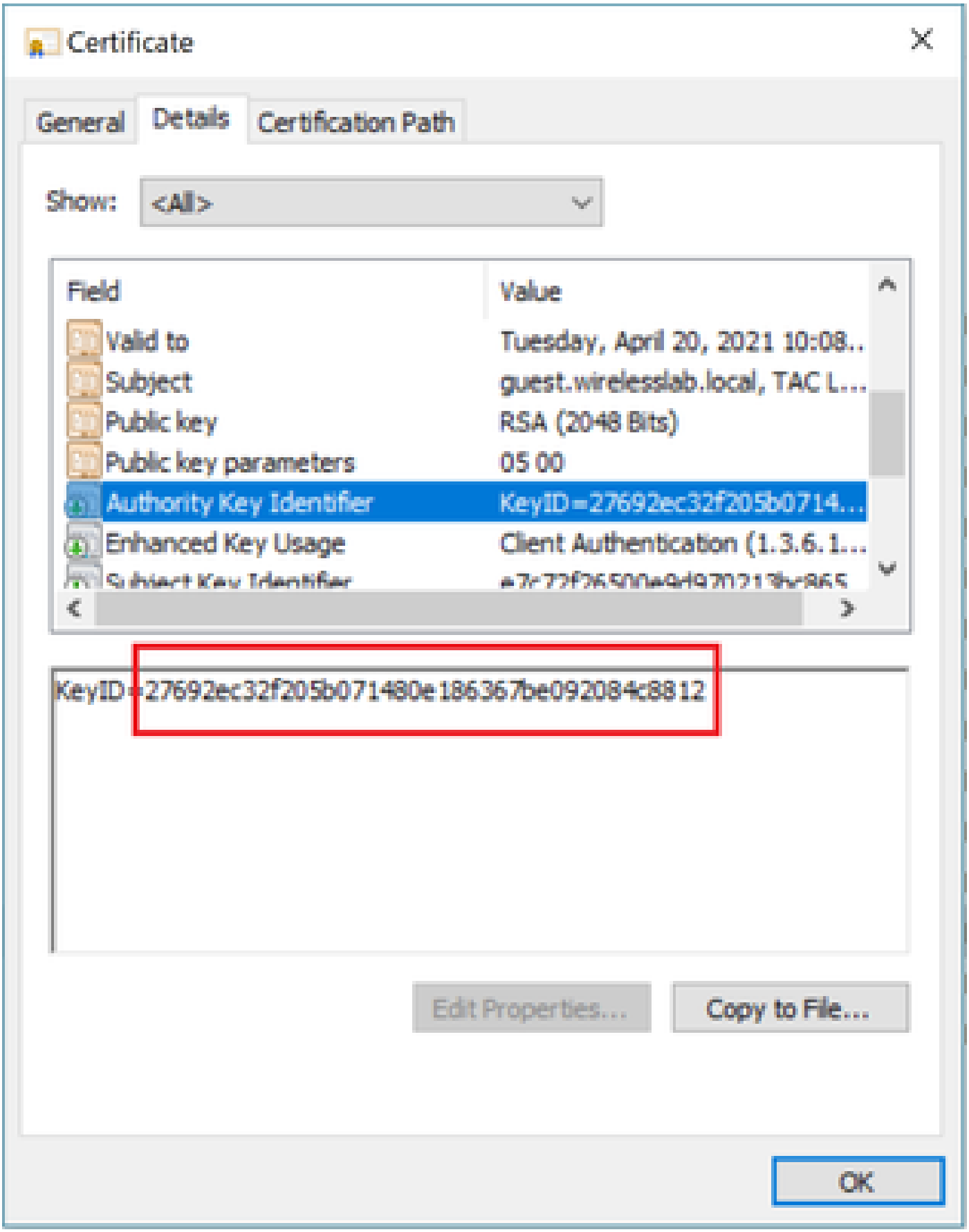
X509v3 Subject Key Identifier:

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

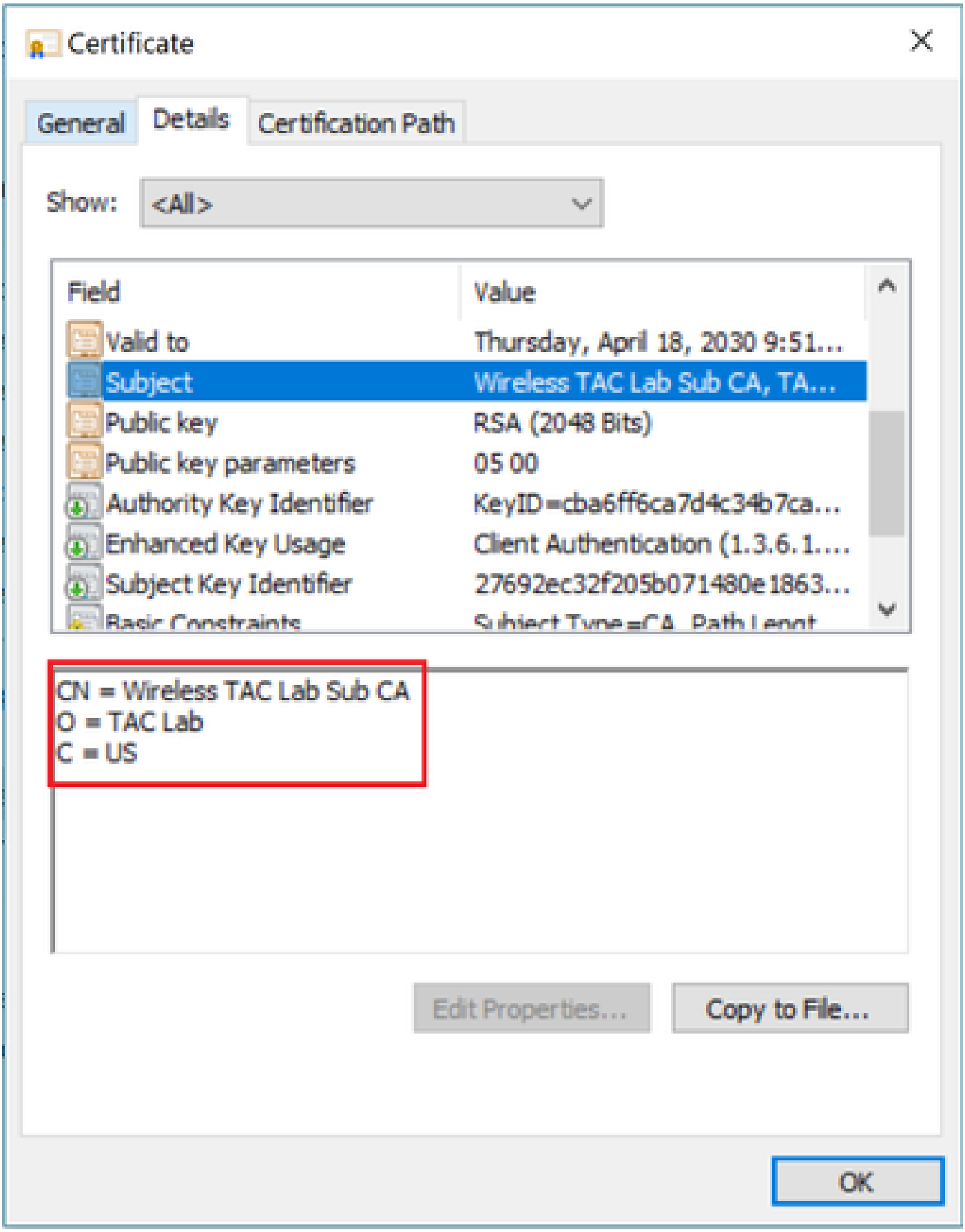
بدلا من ذلك، إذا كنت تستخدم Windows، فعليك بنقر .crt على الشهادة لتدقيق هذه التفاصيل.

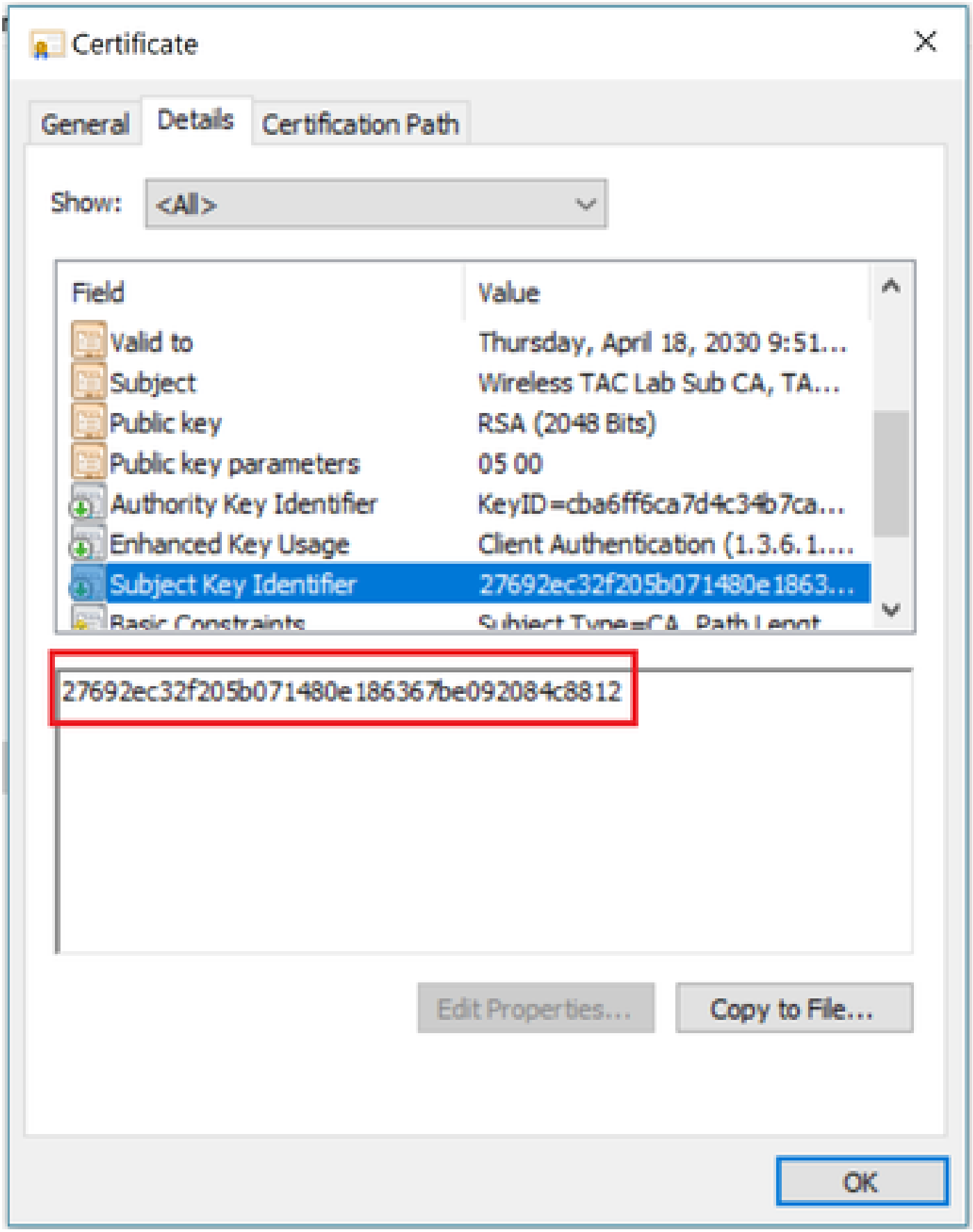
شهادة WLC:





شهادة المرجع المصدق الوسيط:


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



بمجرد تحديد شهادة المرجع المصدق الوسيط، استمر في إستخدام السلسلة وفقا لذلك وأعد التثبيت.

السيناريو 3. لا توجد شهادة مرجع مصدق جذري في السلسلة

<#root>

```
*TransferTask: Apr 21 04:28:09.643: Add ID Cert: Adding certificate & private key using password Cisco1
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*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 l
*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 (verifyC
```

حل: هذا السيناريو مشابه للسيناريو 2، ولكن هذه المرة مقابل الشهادة الوسيطة عند التحقق من صحة المصدر (المرجع المصدق الجذر). يمكن اتباع نفس التعليمات مع التحقق من صحة حقل مصدر مفتاح المرجع ومعرف مفتاح المرجع المصدق X509v3 على شهادة المرجع المصدق الوسيطة للتحقق من المرجع المصدق الجذر.

يمكن إستخدام أمر OpenSSL هذا للتحقق من هذه التفاصيل على كل شهادة:

<#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

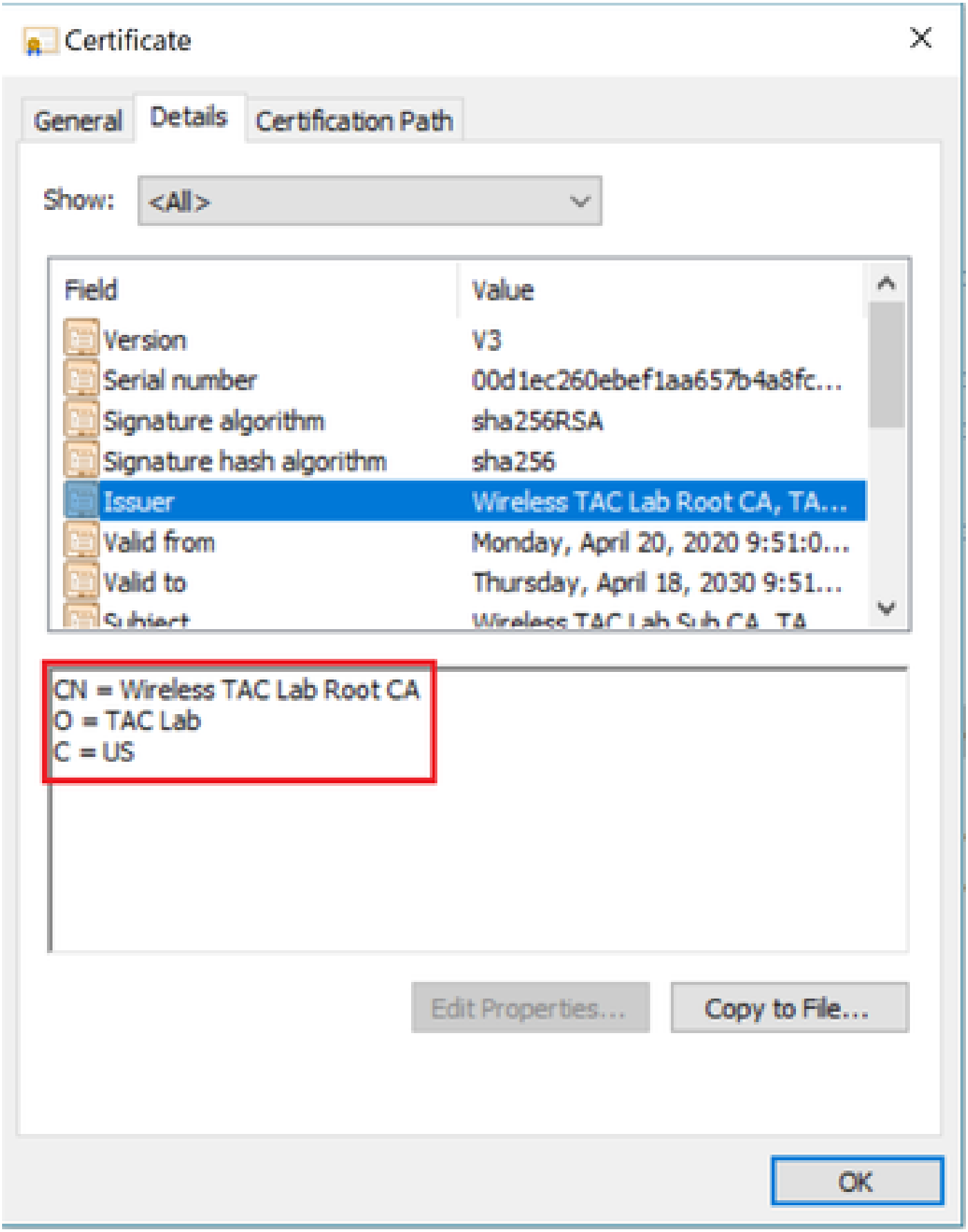
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

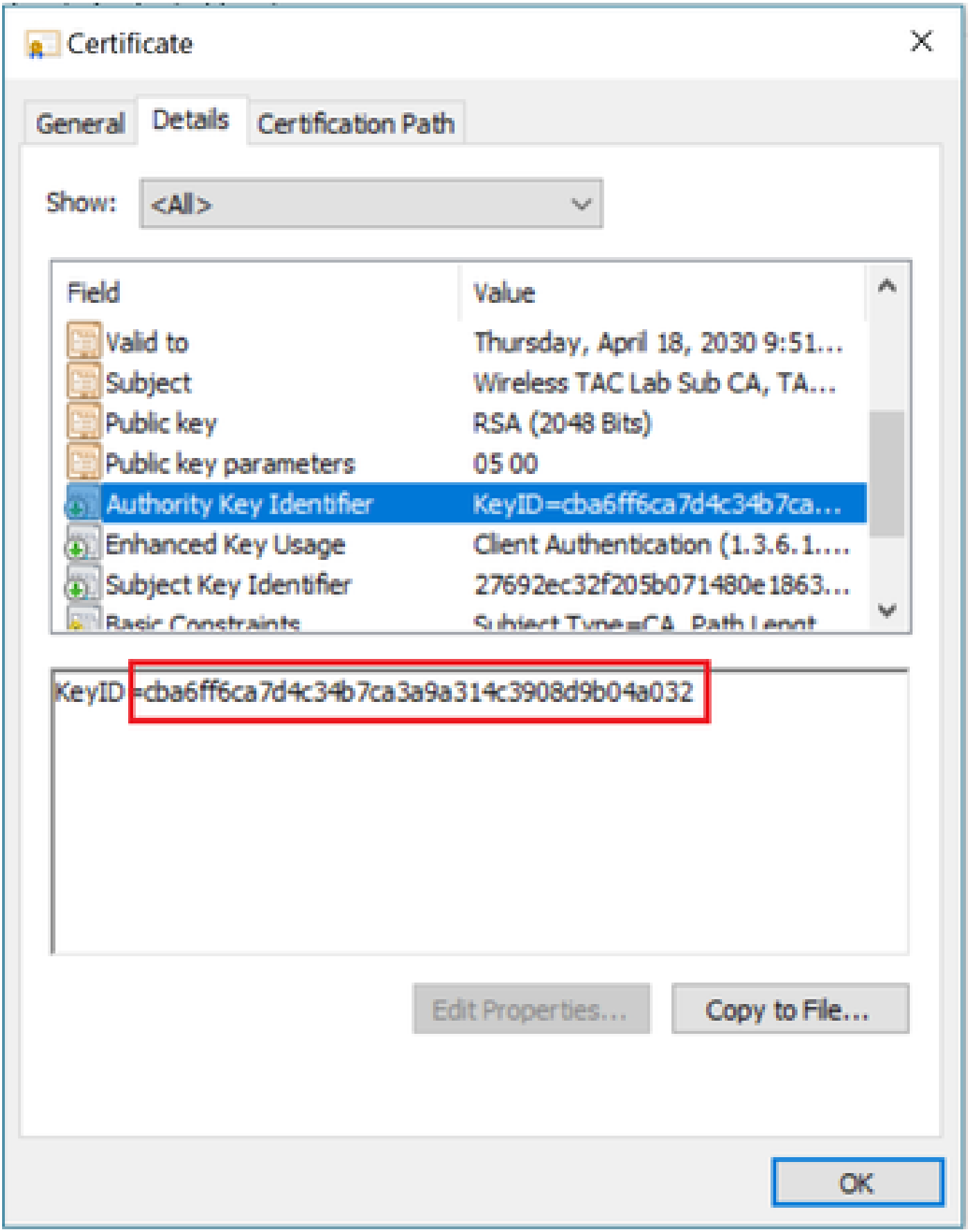
...

X509v3 Subject Key Identifier:

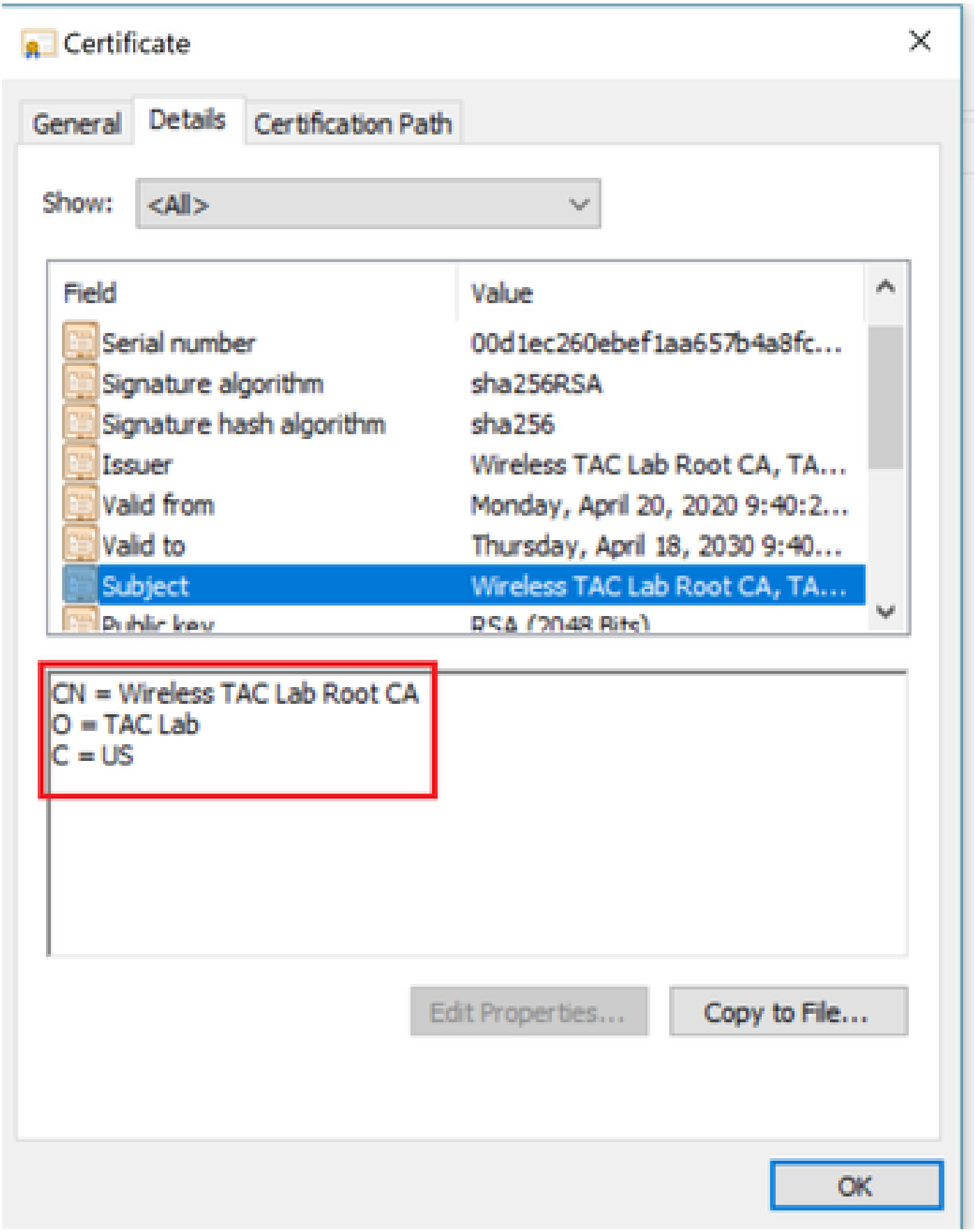
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

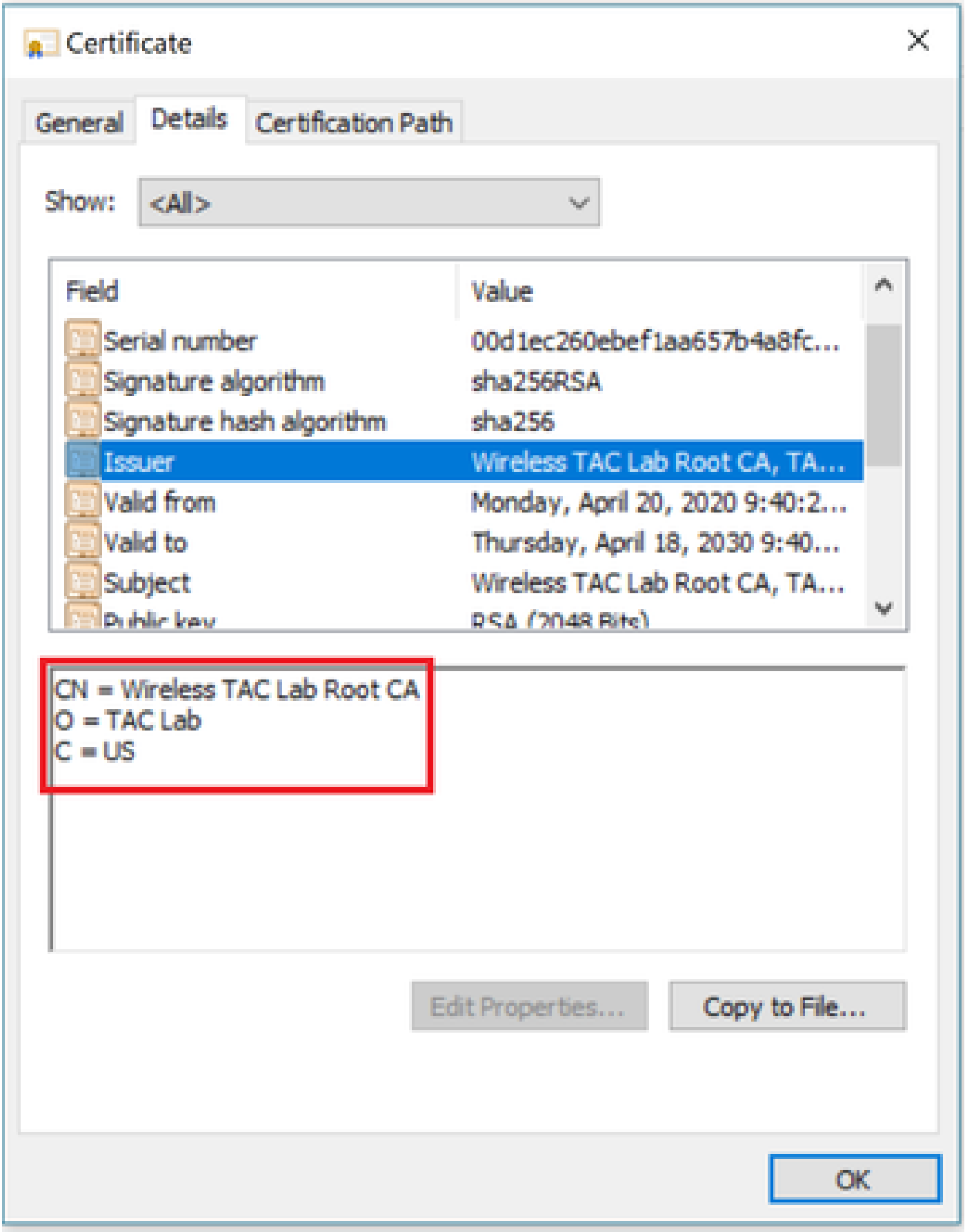
شهادة CA الرئيسية

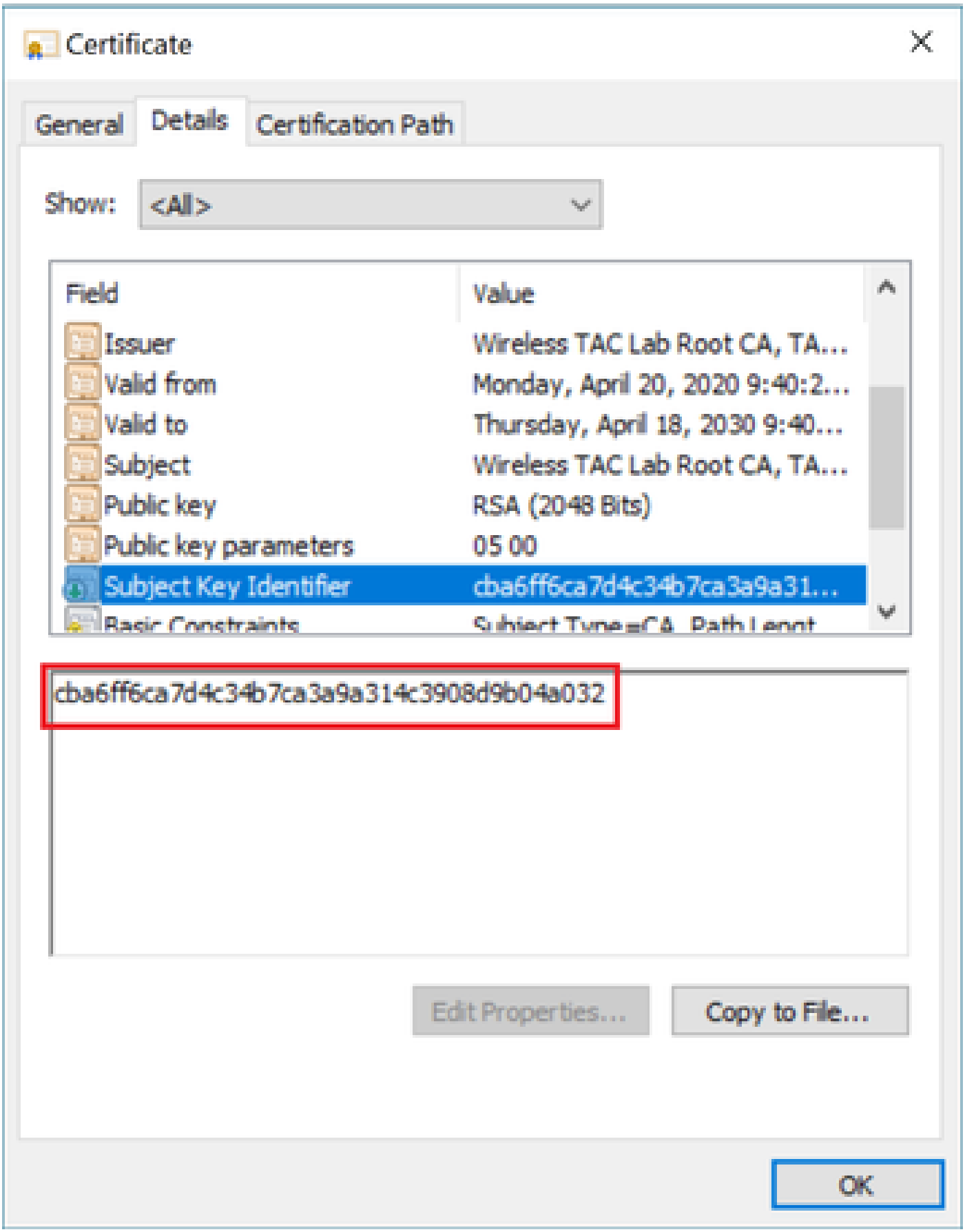

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:51:0...
Valid to
Thursday, April 18, 2030 9:51...
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK



شهادة المرجع المصدق الجذر:


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...
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...
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK



بمجرد تحديد شهادة المرجع المصدق الجذر (المصدر والموضوع كالهما متشابهان)، استمر في استخدام السلسلة وفقا لذلك وأعد التثبيت.

ملاحظة: يستخدم هذه المستند ثلاث سلاسل شهادات (طرفية أو متوسطة أو درجة جذر)، وهو السيناريو الأكثر شيوعا. يمكن أن يكون هناك سيناريوهين مختلفين. يمكن إستخدام نفس المبدأ التوجيهي من عندما يكون هناك شهادتي CA متوسطتين. يجب أن يتم العثور على شهادة المرجع المصدق الجذر هذه السيناريو حتى.

السيناريو 4. لا توجد شهادات مرجع مصدق في السلسلة

<#root>

```
*TransferTask: Apr 21 04:56:50.272: Add ID Cert: Adding certificate & private key using password Cisco1
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*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 l
*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.
```

الحل: بدون أي شهادة أخرى في الملف غير شهادة WLC، يفشل التحقق عند التحقق من صحته. يمكن تابع الصحة عند عمق 0. يمكن فتح الملف في محرر نصي ليتم التحقق من صحته. يمكن تابع الإرشادات الواردة في السيناريو 3 و 2 لتحديد السلسلة حتى تصل إلى المرجع المصدق (CA) الجذري وإعادة السلاسل وفقا لذلك وإعادة التثبيت.

السيناريو 5. لا يوجد مفتاح خاص

<#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)
*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 l
*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 passwo
*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 (verifyC
*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.
```

الحل: تتوقع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تضمين المفتاح الخاص في الملف إذا تم إنشاء طلب توقيع الشهادة (CSR) خارجيا ويلزم تقييده في الملف. في حالة إنشاء CSR في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، تأكد من عدم إعادة تحميل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) قبل التثبيت، وإلا فسيفقد المفتاح الخاص.

معلومات ذات صلة

- الدعم التقني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).