Fehlerbehebung bei der Zertifikatsinstallation auf dem WLC

Inhalt

Einleitung

In diesem Dokument werden die Probleme beschrieben, die durch die Verwendung von Zertifikaten von Drittanbietern auf dem Wireless LAN Controller (WLC) verursacht werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Wireless LAN-Controller (WLC)
- Public Key Infrastructure (PKI)
- X.509-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 3504 WLC mit Firmware-Version 8.10.105.0
- OpenSSL 1.0.2p für Befehlszeilentool
- Windows 10-Computer
- Zertifikatskette von einer Zertifizierungsstelle (Certificate Authority, CA) im privaten Labor mit drei Zertifikaten (Leaf, Intermediate, Root)
- Trivial File Transfer Protocol (TFTP)-Server für die Dateiübertragung.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Auf dem AireOS WLC können Sie für WebAuth und WebAdmin Zertifikate von Drittanbietern installieren. Bei der Installation erwartet der WLC ein einziges PEM (Privacy Enhanced Mail) formatierte Datei mit allen Zertifikaten in der Kette bis hin zum Root-Zertifizierungsstellenzertifikat und dem privaten Schlüssel. Details zu diesem Verfahren sind unter CSR für Drittanbieterzertifikate generieren und Verkettete Zertifikate auf den WLC herunterladen dokumentiert.

In diesem Dokument werden die häufigsten Installationsfehler mit Debug-Beispielen und einer Auflösung für jedes Szenario ausführlicher erläutert. Debug-Ausgaben, die in diesem Dokument verwendet werden, sind vom **Debug-Transfer alle enable**- und **debug pm pki enable**-Funktionen, die auf dem WLC aktiviert sind. Die Zertifikatsdatei wurde über TFTP übertragen.

Fehlerbehebung

Szenario 1. Das Kennwort zum Entschlüsseln des privaten Schlüssels ist falsch, oder es wurde kein Kennwort angegeben.

<#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.
```

Lösung: Stellen Sie sicher, dass das richtige Kennwort eingegeben wird, damit der WLC es für die Installation decodieren kann.

Szenario 2. Kein Zwischenzertifikat der Zertifizierungsstelle in der Kette

<#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.
```

Lösung: Validieren Sie die Felder **Issuer** und **X509v3 Authority Key Identifier** aus dem WLC-Zertifikat, um das CA-Zertifikat zu validieren, das das Zertifikat signiert hat. Wenn das Zertifikat der Zwischen-Zertifizierungsstelle von der Zertifizierungsstelle bereitgestellt wurde, kann dies zur Validierung verwendet werden. Andernfalls fordern Sie das Zertifikat bei Ihrer Zertifizierungsstelle an.

Dieser OpenSSL-Befehl kann verwendet werden, um diese Details für jedes Zertifikat zu validieren:

<#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

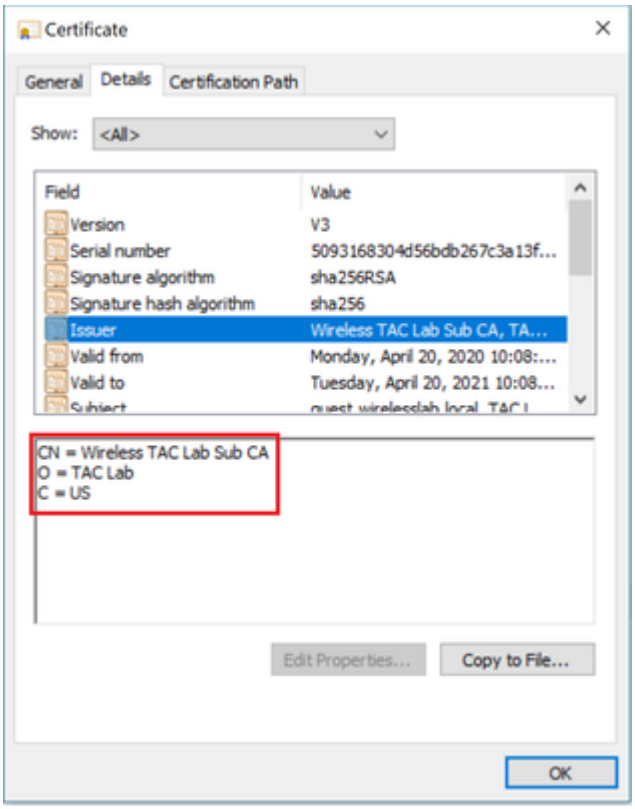
...

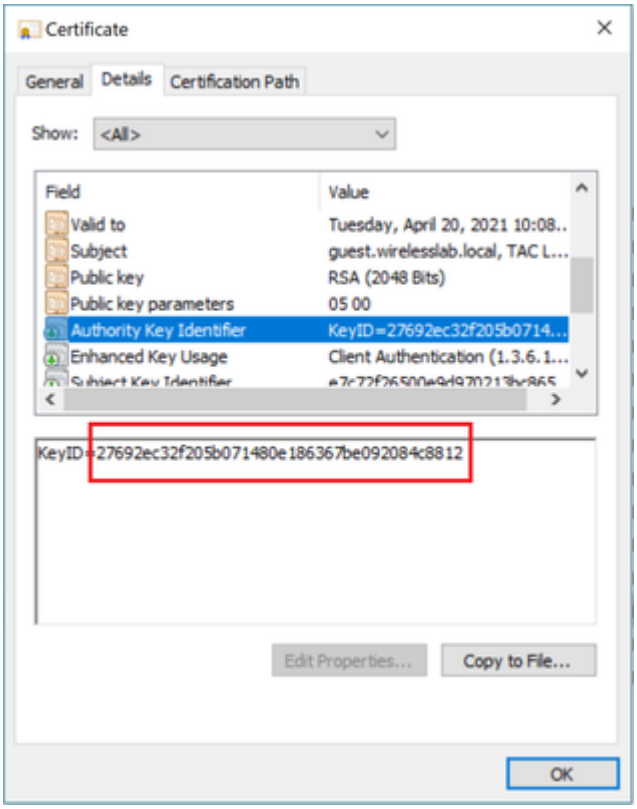
X509v3 Subject Key Identifier:

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

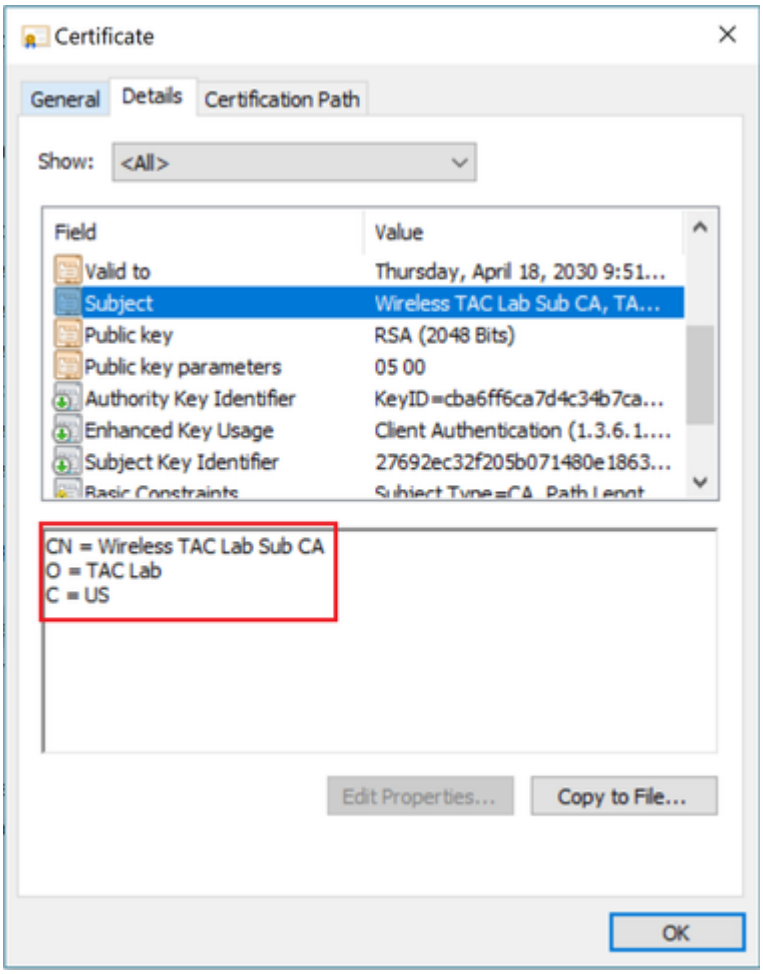
Wenn Sie Windows verwenden, geben Sie dem Zertifikat die Erweiterung **.crt**, und doppelklicken Sie darauf, um diese Details zu validieren.

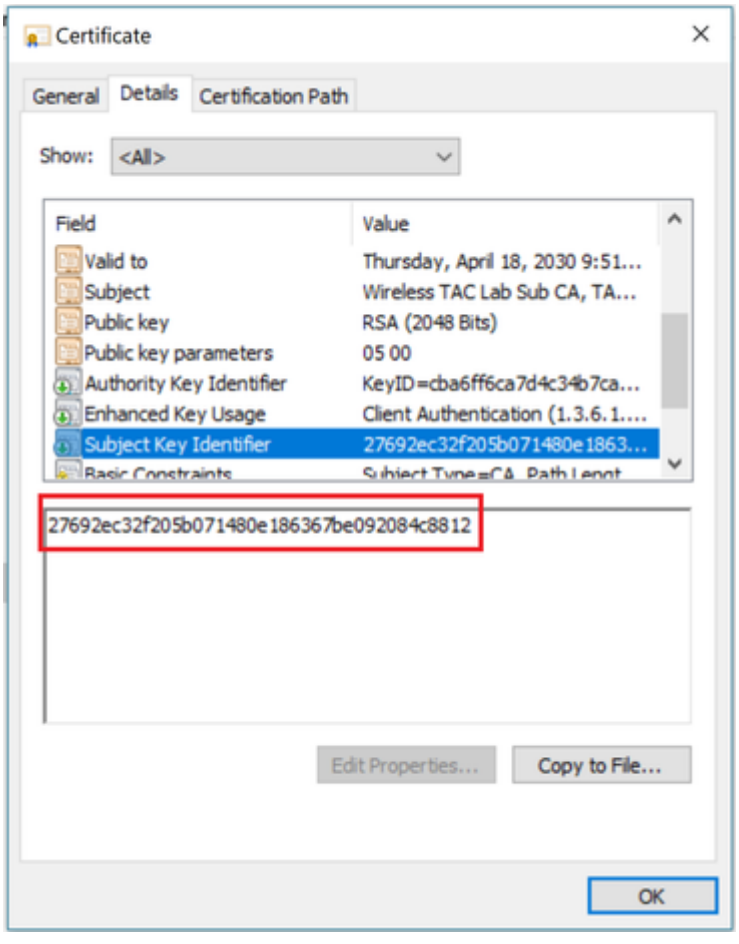
WLC-Zertifikat:





Zwischenzertifikat:


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

Sobald das Zertifikat der Zwischen-Zertifizierungsstelle identifiziert wurde, fahren Sie mit der Kette entsprechend fort, und installieren Sie es erneut.

Szenario 3. Kein Zertifikat der Stammzertifizierungsstelle in der Kette

<#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
```

Lösung: Dieses Szenario ähnelt Szenario 2, diesmal jedoch im Vergleich zum Zwischenzertifikat, wenn Sie den Aussteller (Root CA) validieren. Die gleichen Anweisungen gelten für die Überprüfung der **X509v3-** und **X509v3-Autoritätsschlüssel-ID-**Felder auf dem Zwischenzertifikat der Zertifizierungsstelle zur Validierung der Stammzertifizierungsstelle.

Dieser OpenSSL-Befehl kann verwendet werden, um diese Details für jedes Zertifikat zu validieren:

<#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

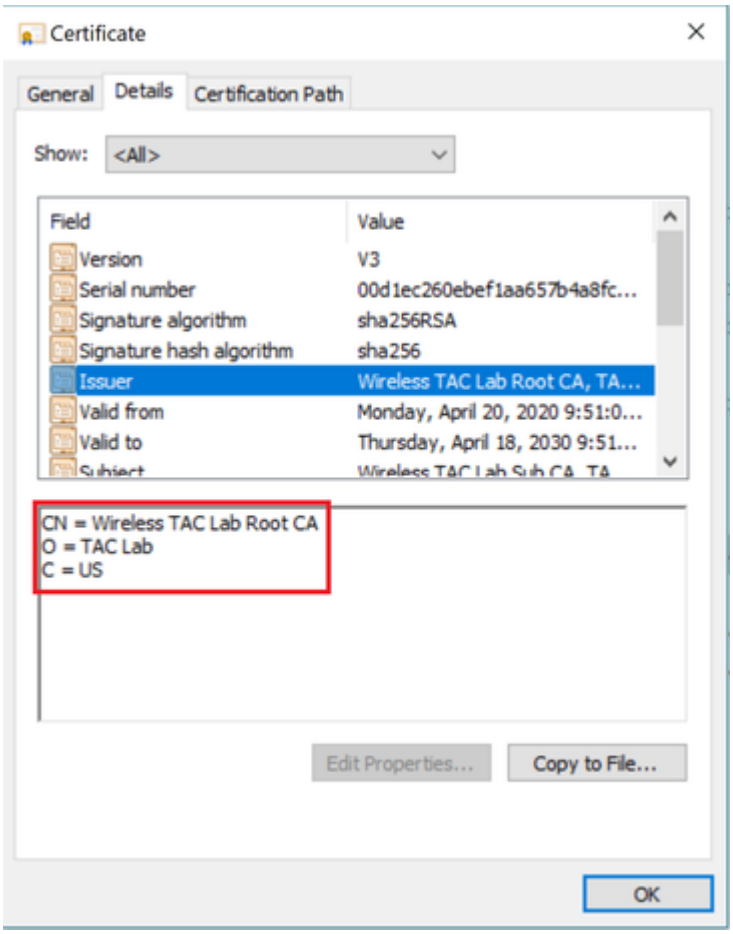
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

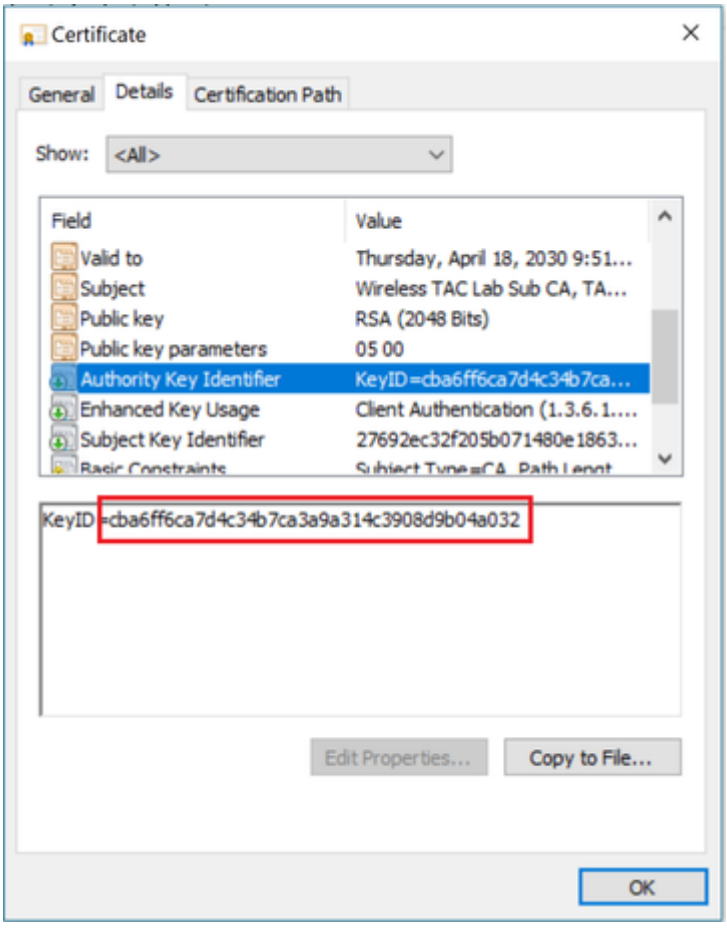
...

X509v3 Subject Key Identifier:

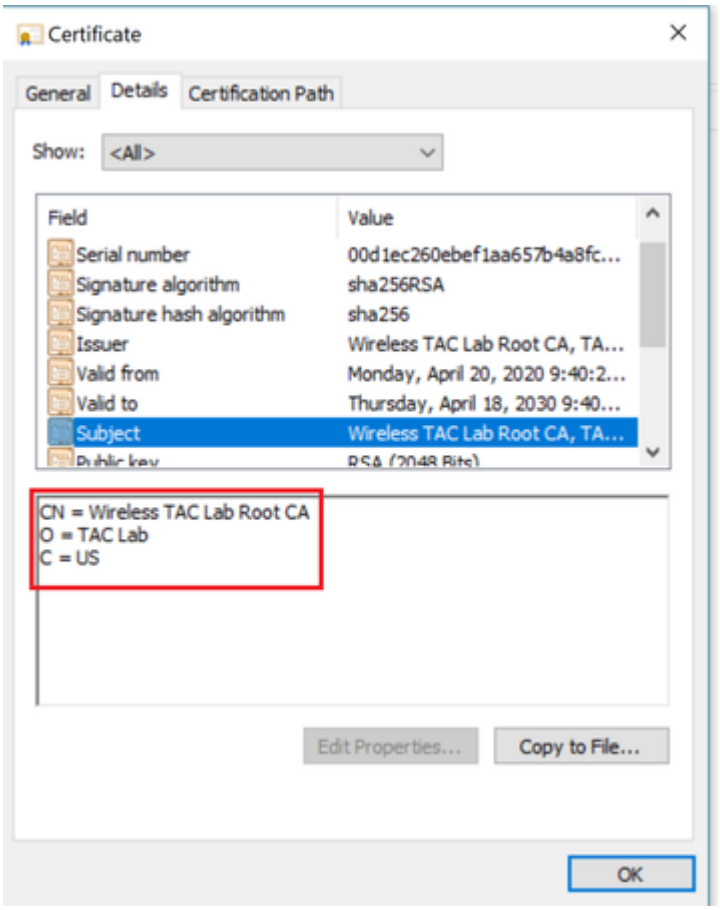
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

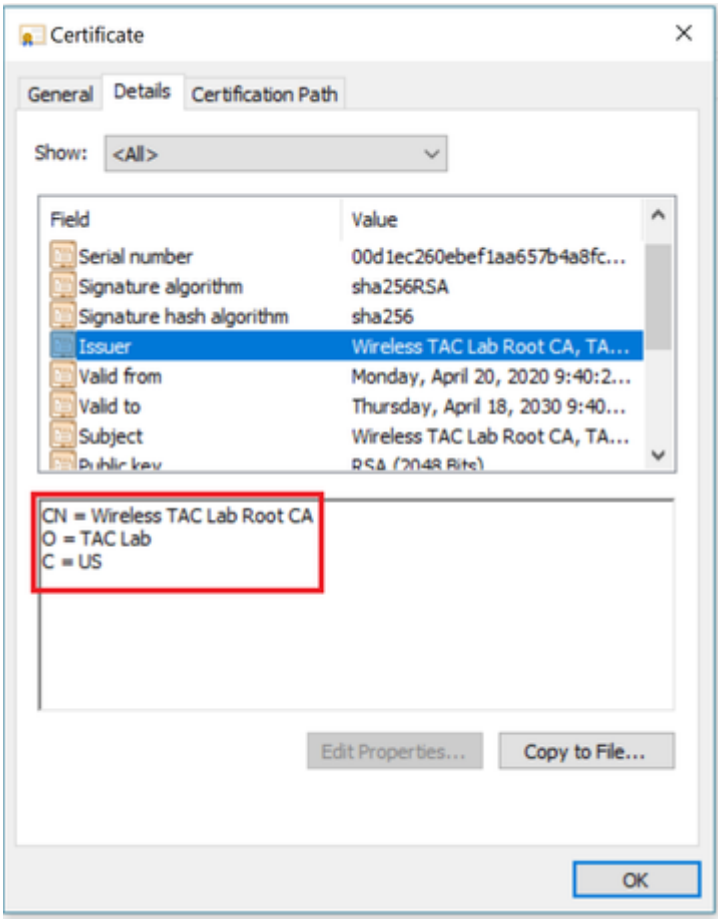
Zwischenzertifikat

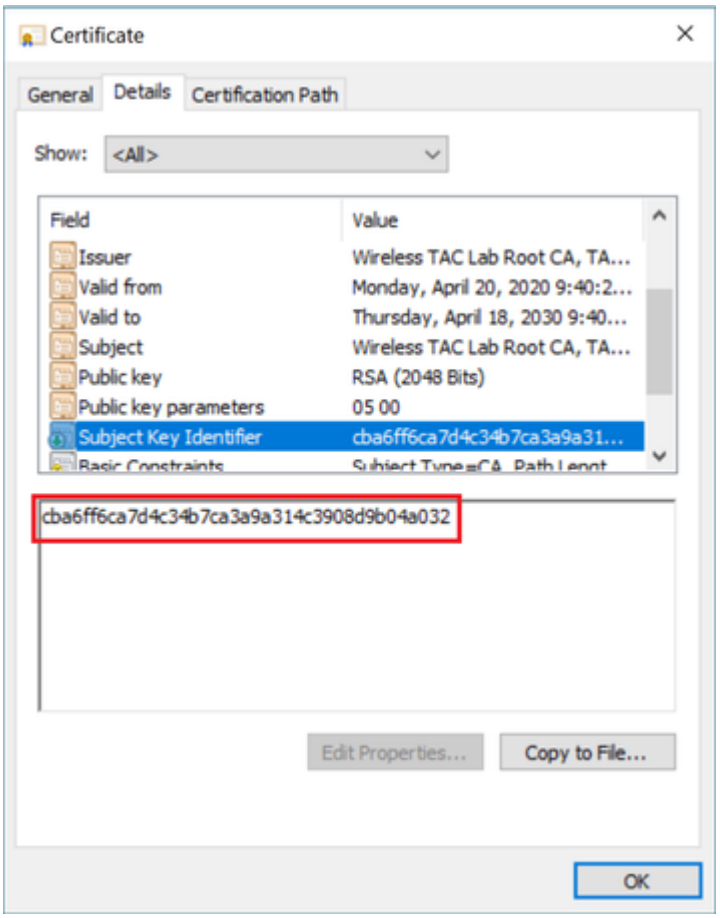




Stammzertifizierungsstelle:


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



Sobald das Zertifikat der Stammzertifizierungsstelle identifiziert wurde (Aussteller und Betreff sind identisch), fahren Sie mit der Kette entsprechend fort und installieren Sie das Zertifikat erneut.

> **Hinweis**: Dieses Dokument verwendet drei Zertifikatsketten (Leaf, Zwischen-CA, Root-CA). Dies ist das häufigste Szenario. Es kann Szenarien geben, in denen 2 Zertifikate für eine Zwischen-Zertifizierungsstelle betroffen sind. Dieselbe Richtlinie aus diesem Szenario kann verwendet werden, bis das Zertifikat der Stammzertifizierungsstelle gefunden wird.

Szenario 4. Keine Zertifizierungsstellenzertifikate in der Kette

<#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.
```

Lösung: Wenn sich kein anderes Zertifikat in der Datei befindet, als das WLC-Zertifikat, schlägt die Validierung bei der **Überprüfung in der Tiefe 0 fehl**. Die Datei kann zur Validierung in einem Texteditor geöffnet werden. Anhand der Richtlinien aus Szenario 2 und 3 kann die Kette bis zur Root-Zertifizierungsstelle identifiziert und entsprechend neu verkettet und neu installiert werden.

Szenario 5. Kein privater Schlüssel

<#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.
```

Lösung: Der WLC erwartet, dass der private Schlüssel in die Datei aufgenommen wird, wenn eine Zertifikatsanforderung (Certificate Signing Request, CSR) extern generiert wurde und in der Datei verkettet werden muss. Falls der CSR im WLC generiert wurde, stellen Sie sicher, dass der WLC vor der Installation nicht neu geladen wird, da sonst der private Schlüssel verloren geht.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.