Dépanner l'installation de certificat sur WLC

Table des matières

Introduction

Ce document décrit les problèmes causés par l'utilisation de certificats tiers sur le contrôleur de réseau local sans fil (WLC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur LAN sans fil (WLC)
- Infrastructure à clé publique (PKI)
- Certificats X.509

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC 3504 avec version de microprogramme 8.10.105.0
- OpenSSL 1.0.2p pour l'outil de ligne de commande
- ordinateur Windows 10
- Chaîne de certificats de l'autorité de certification privée (CA) avec trois certificats (leaf, intermédiaire, racine)
- Serveur TFTP (Trivial File Transfer Protocol) pour le transfert de fichiers.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

Sur le WLC AireOS, vous pouvez installer des certificats tiers à utiliser pour WebAuth et WebAdmin. Lors de l'installation, le WLC attend un seul PEM (Privacy Enhanced Mail) avec tous les certificats de la chaîne jusqu'au certificat de l'autorité de certification racine et à la clé privée. Les détails sur cette procédure sont documentés dans Générer CSR pour des certificats tiers et Télécharger des certificats chaînés sur le WLC.

Ce document développe et montre plus en détail les erreurs d'installation les plus courantes avec des exemples de débogage et la résolution pour chaque scénario. Les sorties de débogage utilisées tout au long de ce document sont de **debug transfer all enable** et **debug pm pki enable** enabled sur le WLC. TFTP a été utilisé pour transférer le fichier de certificats.

Dépannage

Scénario 1. Le mot de passe fourni pour déchiffrer la clé privée est incorrect ou aucun mot de passe n'a été fourni

<#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.
```

Solution : Assurez-vous que le mot de passe correct est fourni afin que le WLC puisse le décoder pour l'installation.

Scénario 2. Aucun certificat CA intermédiaire dans la chaîne

<#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.
```

Solution : validez les champs **Émetteur** et **Identificateur de clé d'autorité X509v3** du certificat WLC pour valider le certificat CA qui a signé le certificat. Si le certificat d'autorité de certification intermédiaire a été fourni par l'autorité de certification, il peut être utilisé pour la validation. Sinon, demandez le certificat à votre autorité de certification.

Cette commande OpenSSL peut être utilisée pour valider ces détails sur chaque certificat :

<#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

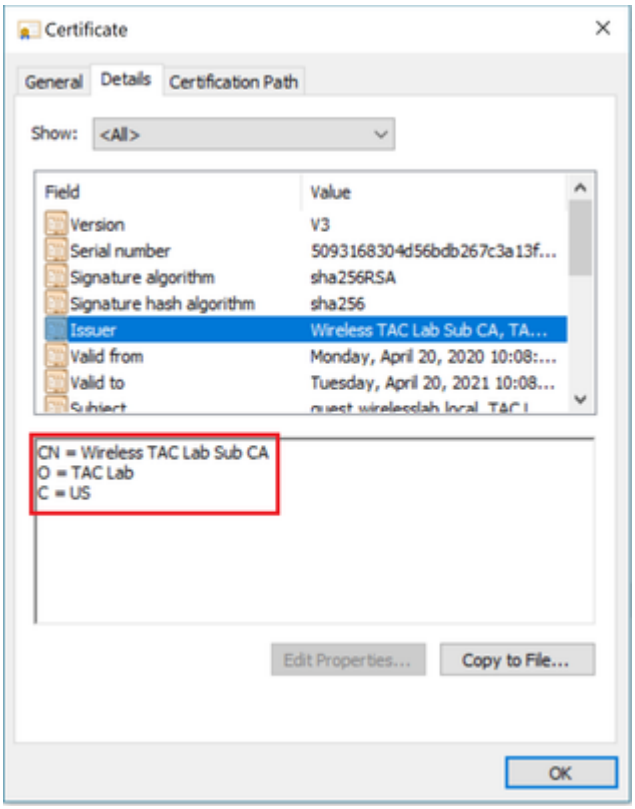
...

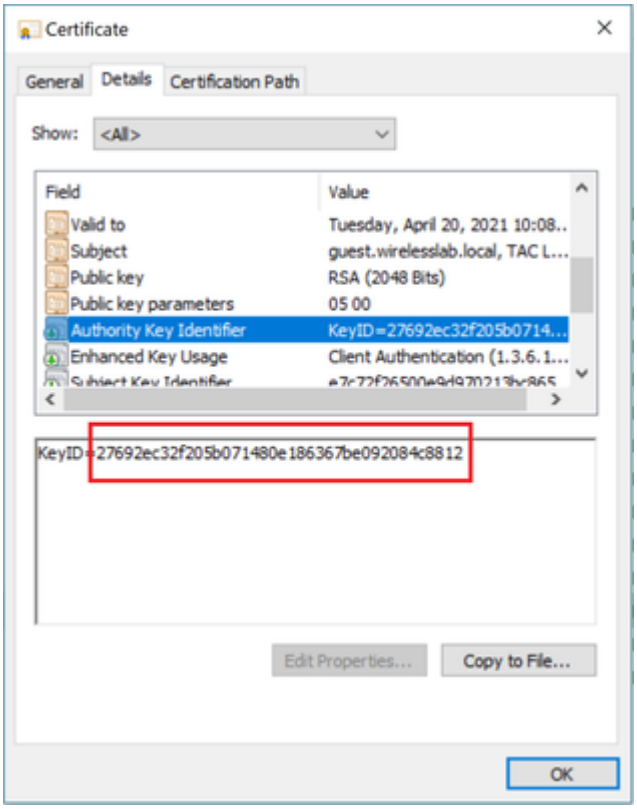
X509v3 Subject Key Identifier:

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

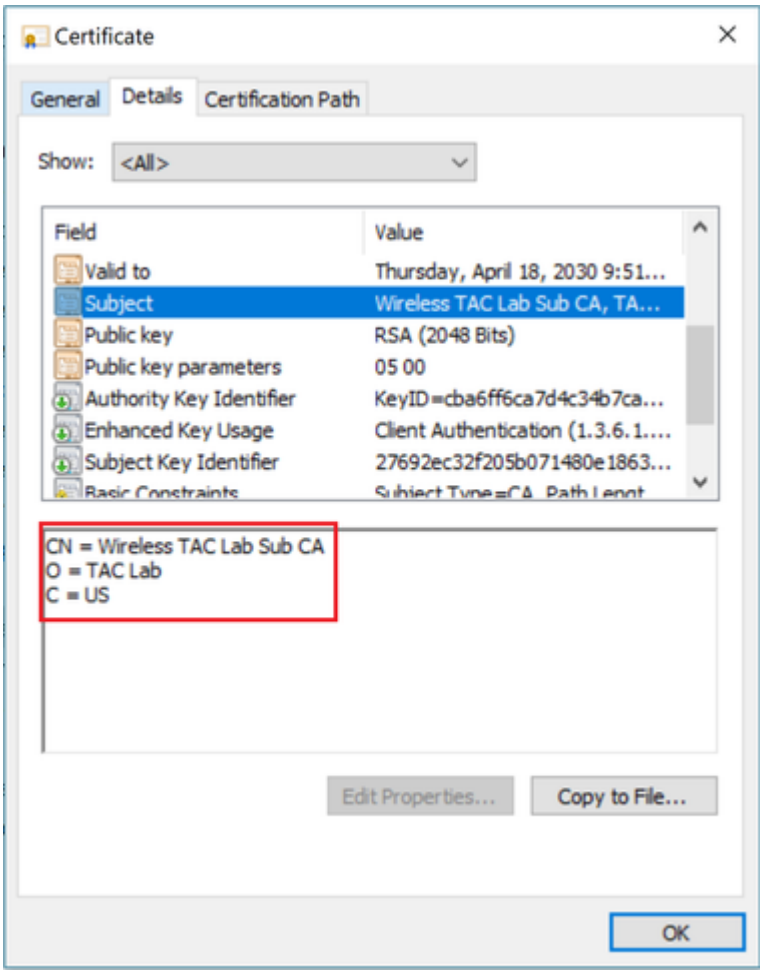
Si vous utilisez Windows, vous pouvez également attribuer au certificat une extension **.crt** et double-cliquer pour valider ces détails.

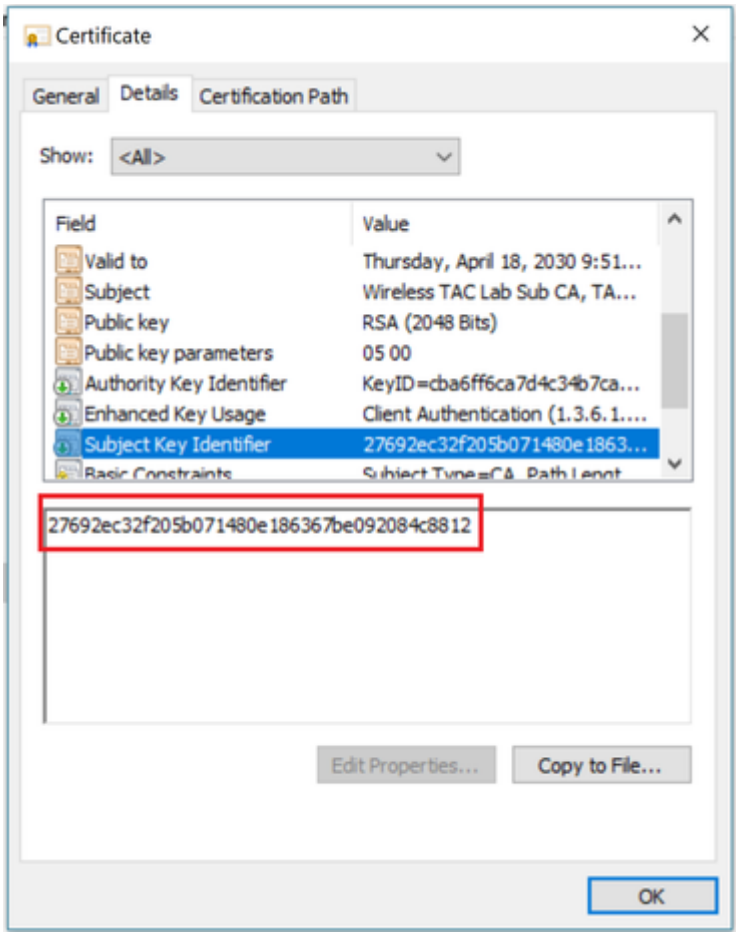
Certificat WLC :





Certificat CA intermédiaire :


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

Une fois le certificat de CA intermédiaire identifié, poursuivez la chaîne en conséquence et réinstallez.

Scénario 3. Aucun certificat CA racine dans la chaîne

<#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
```

Solution : ce scénario est similaire au scénario 2, mais cette fois avec le certificat intermédiaire lorsque vous validez l'émetteur (autorité de certification racine). Les mêmes instructions peuvent être suivies avec la vérification des champs **Émetteur** et **Identificateur de clé d'autorité X509v3** sur le certificat d'autorité de certification intermédiaire pour valider l'autorité de certification racine.

Cette commande OpenSSL peut être utilisée pour valider ces détails sur chaque certificat :

<#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

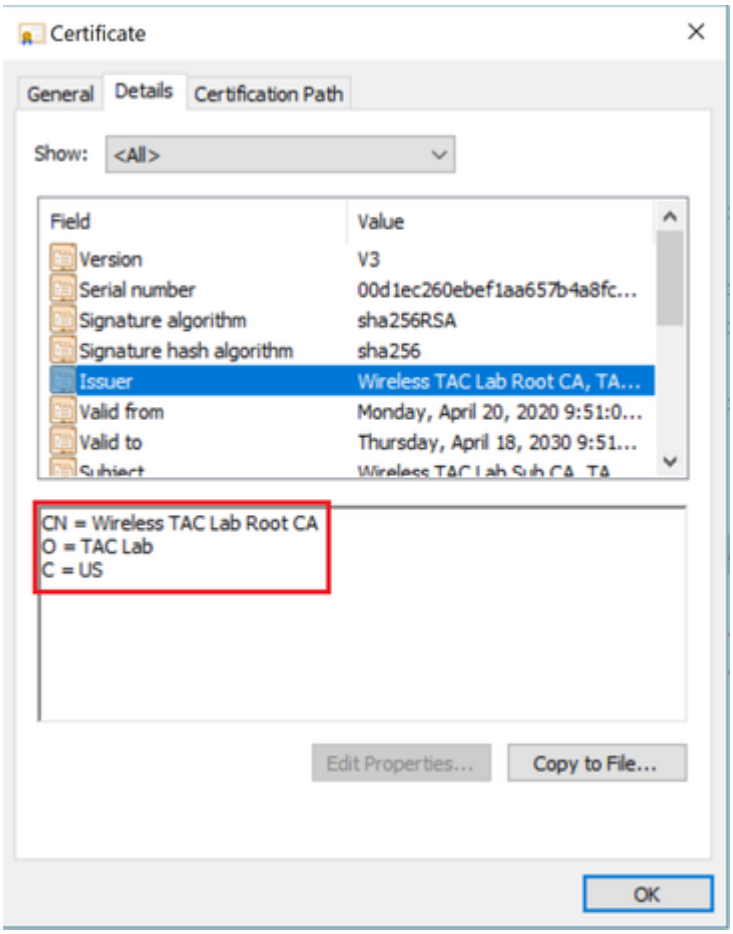
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

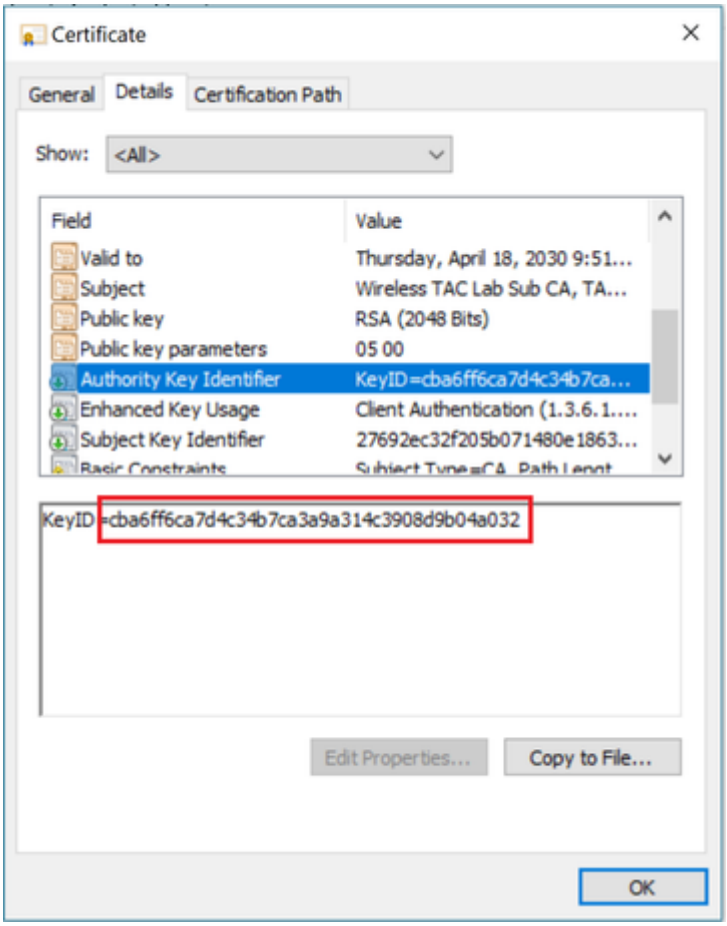
...

X509v3 Subject Key Identifier:

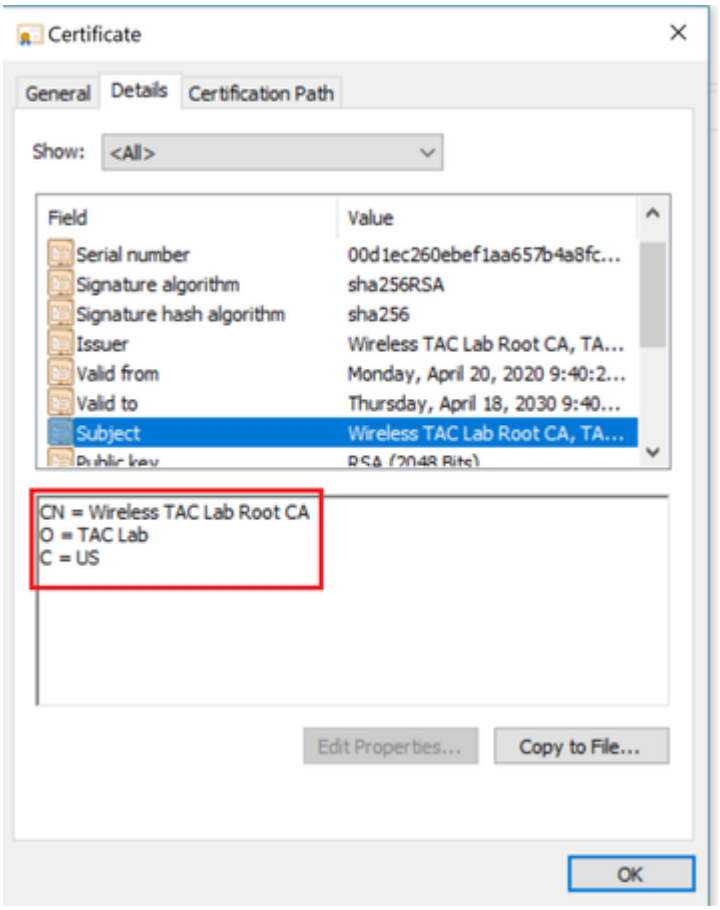
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

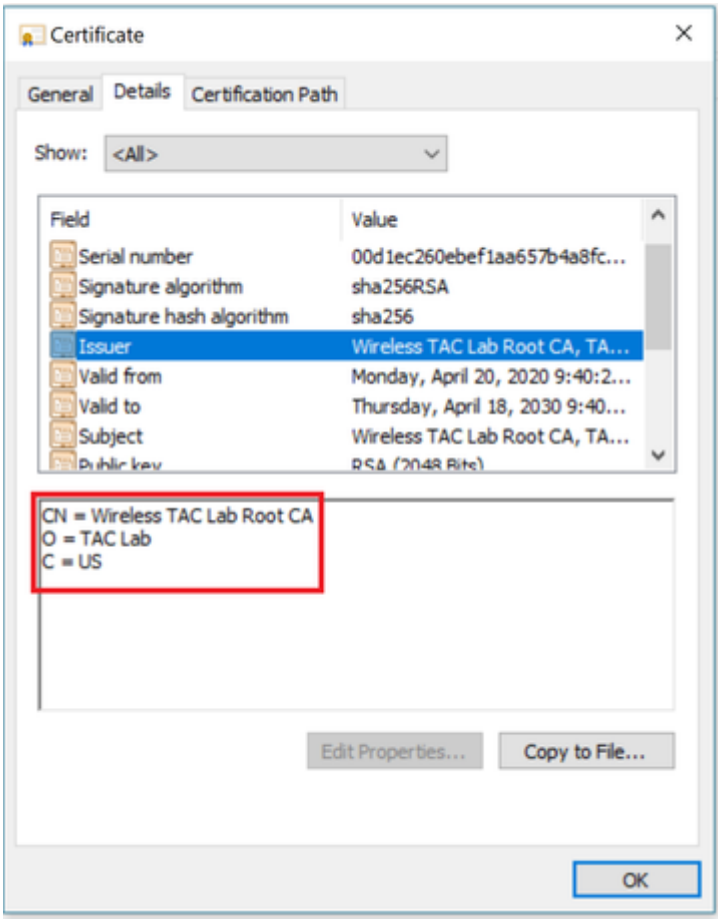
Certificat CA intermédiaire

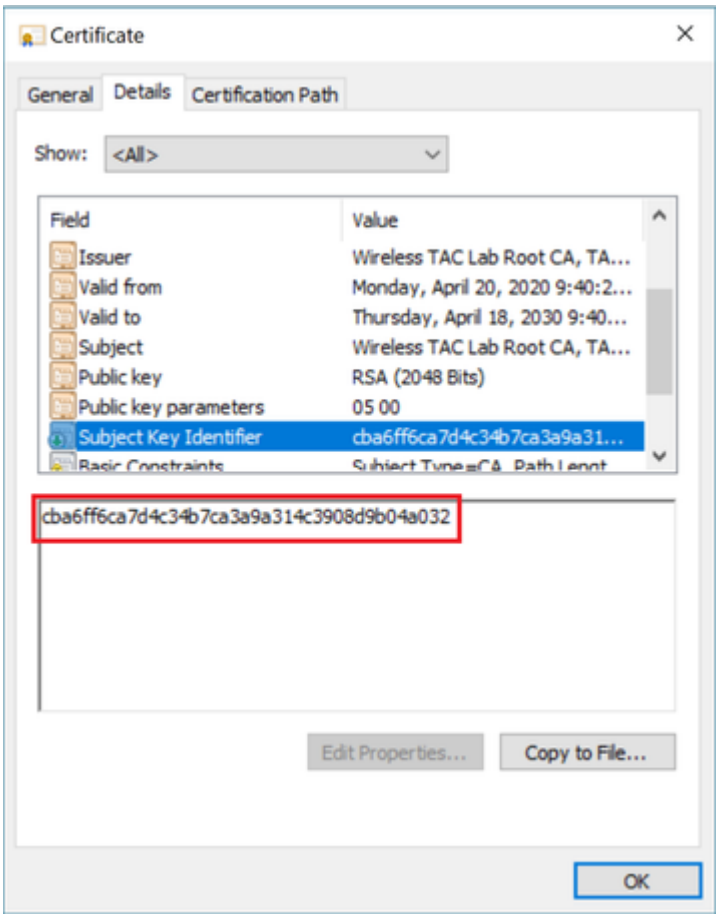




Certificat de CA racine :


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



Une fois le certificat de l'autorité de certification racine identifié (l'émetteur et l'objet sont identiques), poursuivez la chaîne en conséquence et réinstallez.

> **Remarque** : ce document utilise trois chaînes de certificats (leaf, CA intermédiaire, CA racine), ce qui est le scénario le plus courant. Il peut y avoir des scénarios dans lesquels 2 certificats CA intermédiaires sont impliqués. La même directive de ce scénario peut être utilisée jusqu'à ce que le certificat de l'autorité de certification racine soit trouvé.

Scénario 4 . Aucun certificat CA dans la chaîne

<#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.
```

Solution : Avec aucun autre certificat dans le fichier autre que le certificat WLC, la validation échoue à la **vérification à la profondeur 0**. Le fichier peut être ouvert dans un éditeur de texte à valider. Les instructions des scénarios 2 et 3 peuvent être suivies pour identifier la chaîne jusquâ€™à lâ€™autorité de certification racine, puis pour la réorganiser en conséquence et la réinstaller.

Scénario 5. Pas de clé privée

<#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.
```

Solution : le WLC s'attend à ce que la clé privée soit incluse dans le fichier si la demande de signature de certificat (CSR) a été générée en externe et doit être chaînée dans le fichier. Si le CSR a été généré dans le WLC, assurez-vous que le WLC n'est pas rechargé avant l'installation, sinon la clé privée est perdue.

Informations connexes

- **Assistance technique et téléchargements Cisco**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.