Solucionar problemas de instalação de certificado no WLC

Contents

Introduction

Este documento descreve os problemas causados pelo uso de certificados de terceiros na controladora Wireless LAN (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 3504 WLC com versão de firmware 8.10.105.0
- OpenSSL 1.0.2p para a ferramenta de linha de comando
- Máquina com Windows 10
- Cadeia de certificados da Autoridade de Certificação (CA) do laboratório privado com três certificados (folha, intermediário, raiz)
- Servidor TFTP (Trivial File Transfer Protocol) para transferência de arquivos.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

No AireOS WLC, você pode instalar certificados de terceiros para serem usados para WebAuth e WebAdmin. Na instalação, a WLC espera um único PEM (Privacy Enhanced Mail) arquivo formatado com todos os certificados da cadeia até o certificado de CA raiz e a chave privada. Os detalhes sobre esse procedimento estão documentados em Gerar CSR para certificados de terceiros e Baixar certificados em cadeia para o WLC.

Este documento expande e mostra em mais detalhes os erros de instalação mais comuns com exemplos de depuração e resolução para cada cenário. As saídas de depuração usadas em todo este documento são de **debug transfer all enable** e **debug pm pki enable** habilitado na WLC. O TFTP foi usado para transferir o arquivo de certificados.

Troubleshoot

Cenário 1. A senha fornecida para descriptografar a chave privada está incorreta ou nenhuma senha foi fornecida

<#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.
```

Solução: certifique-se de que a senha correta seja fornecida para que a WLC possa decodificá-la para instalação.

Cenário 2. Nenhum Certificado de Autoridade de Certificação Intermediária na Cadeia

<#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.
```

Solução: valide os campos **Emissor** e **Identificador de chave de autoridade X509v3 do certificado WLC para validar o certificado CA que assinou o certificado.** Se o certificado CA intermediário foi fornecido pela CA, ele pode ser usado para validação. Caso contrário, solicite o certificado à sua CA.

Este comando OpenSSL pode ser usado para validar estes detalhes em 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

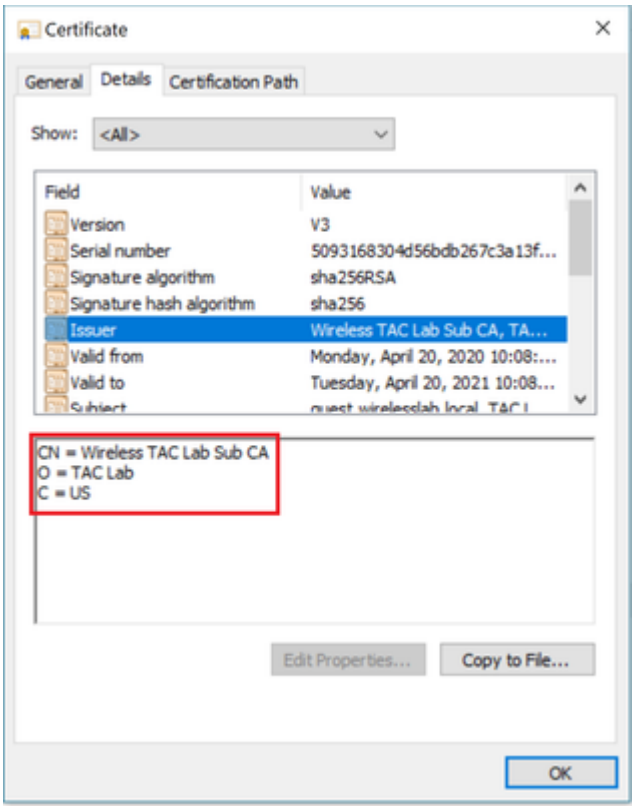
...

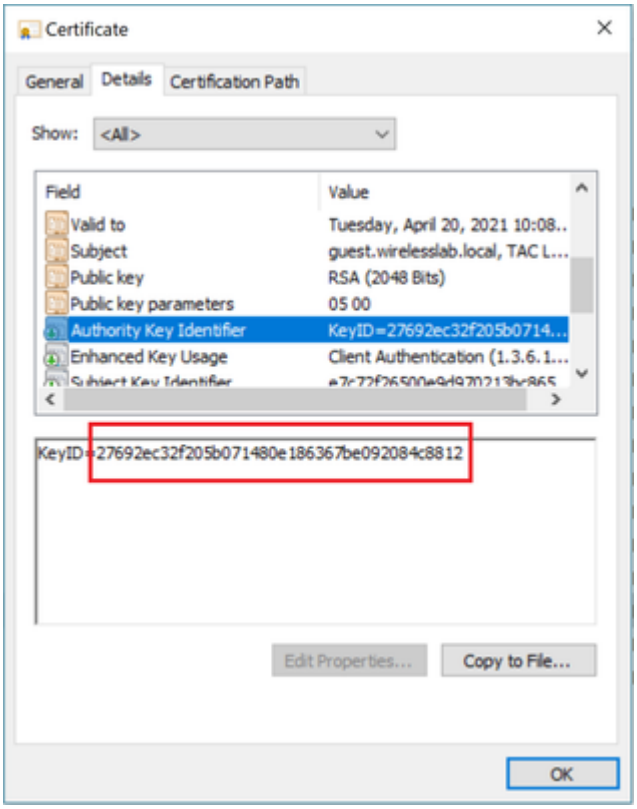
X509v3 Subject Key Identifier:

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

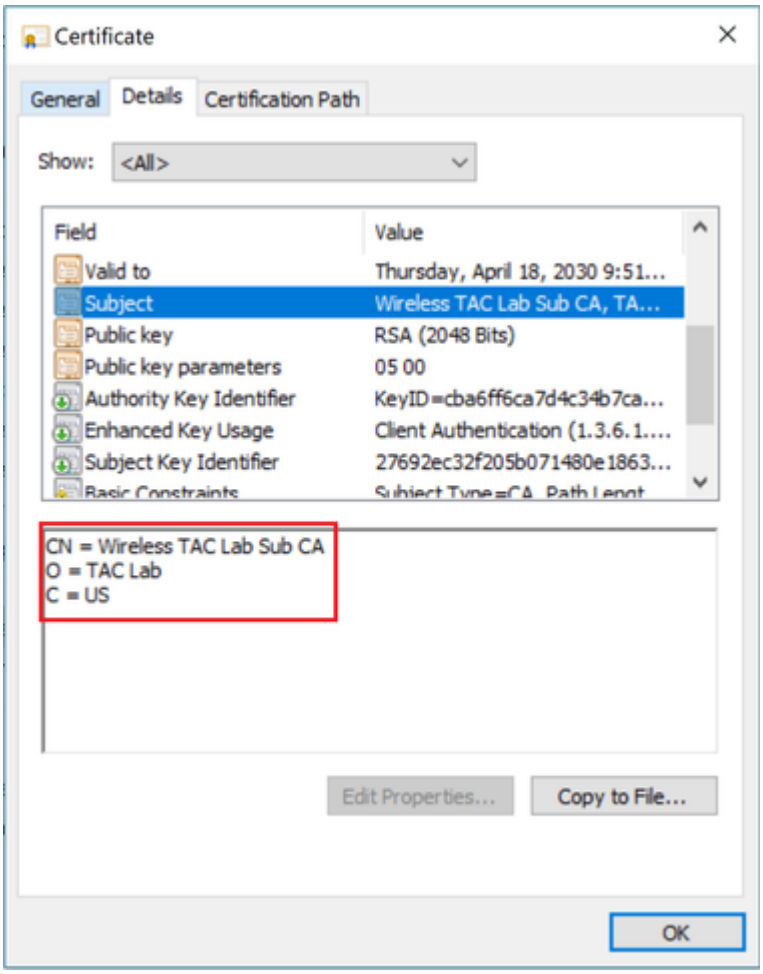
Se preferir, se você usar o Windows, forneça ao certificado uma extensão **.crt** e clique duas vezes para validar esses detalhes.

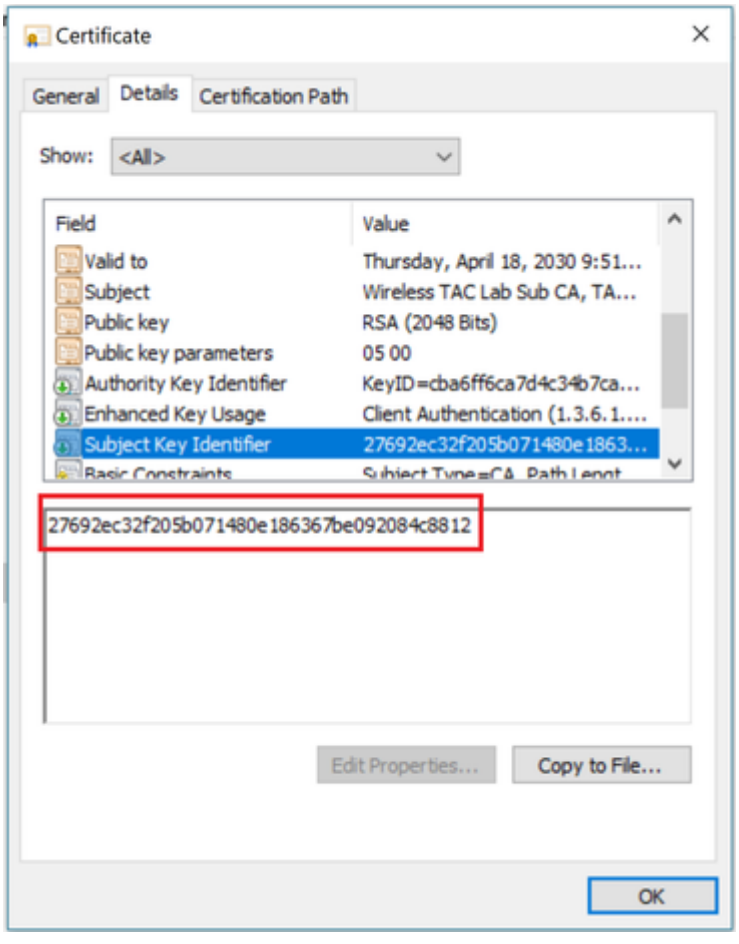
Certificado WLC:





Certificado CA intermediário:


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

Depois que o certificado CA intermediário for identificado, prossiga com a cadeia e reinstale.

Cenário 3. Nenhum Certificado CA Raiz na Cadeia

<#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
```

Solução: este cenário é semelhante ao cenário 2, mas desta vez em relação ao certificado intermediário quando você valida o emissor (CA raiz). As mesmas instruções podem ser seguidas com a verificação dos campos **Issuer** e **X509v3 Authority Key Identifier** no certificado intermediário da CA para validar a CA raiz.

Este comando OpenSSL pode ser usado para validar estes detalhes em 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

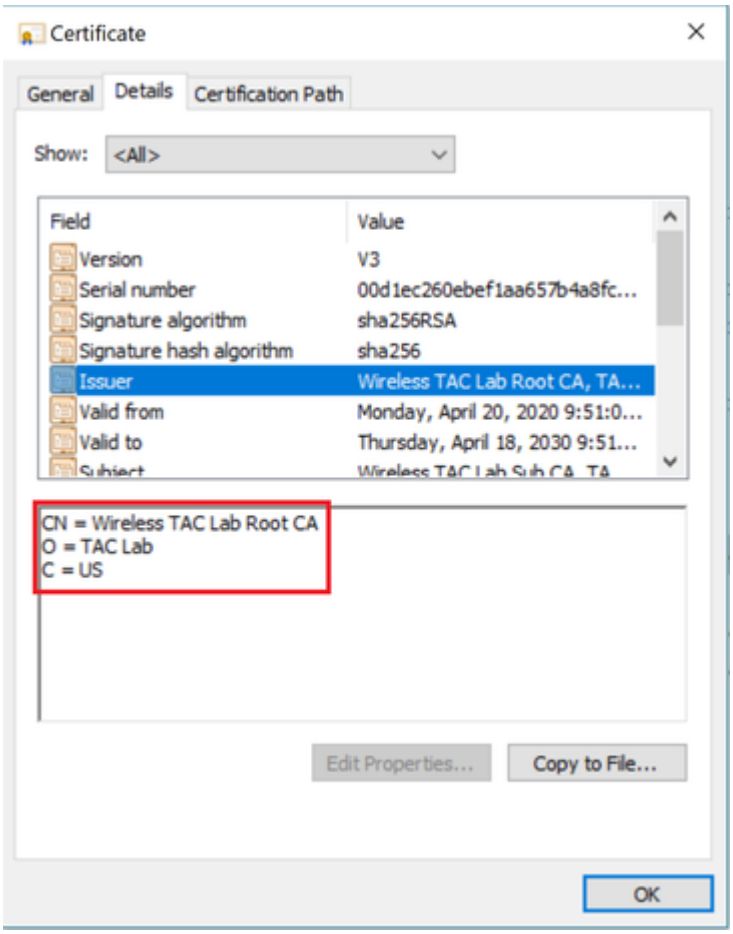
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

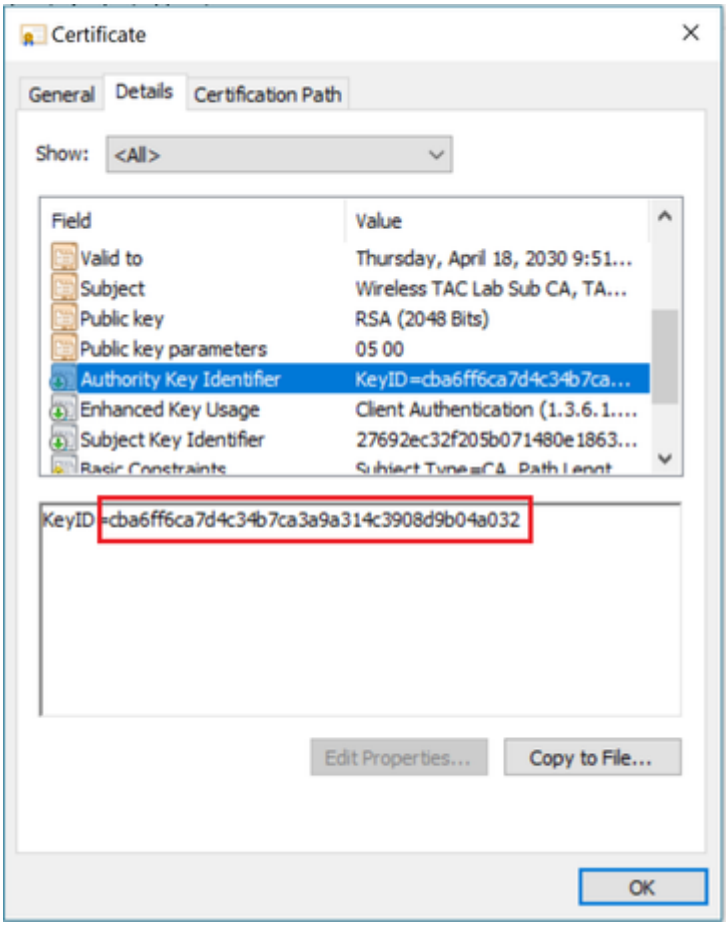
...

X509v3 Subject Key Identifier:

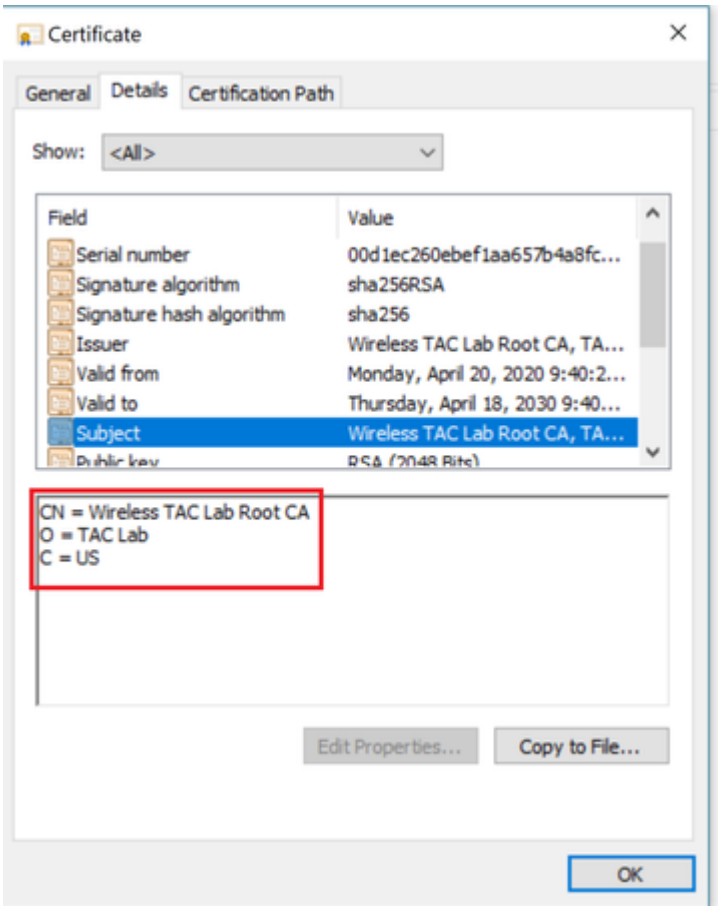
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

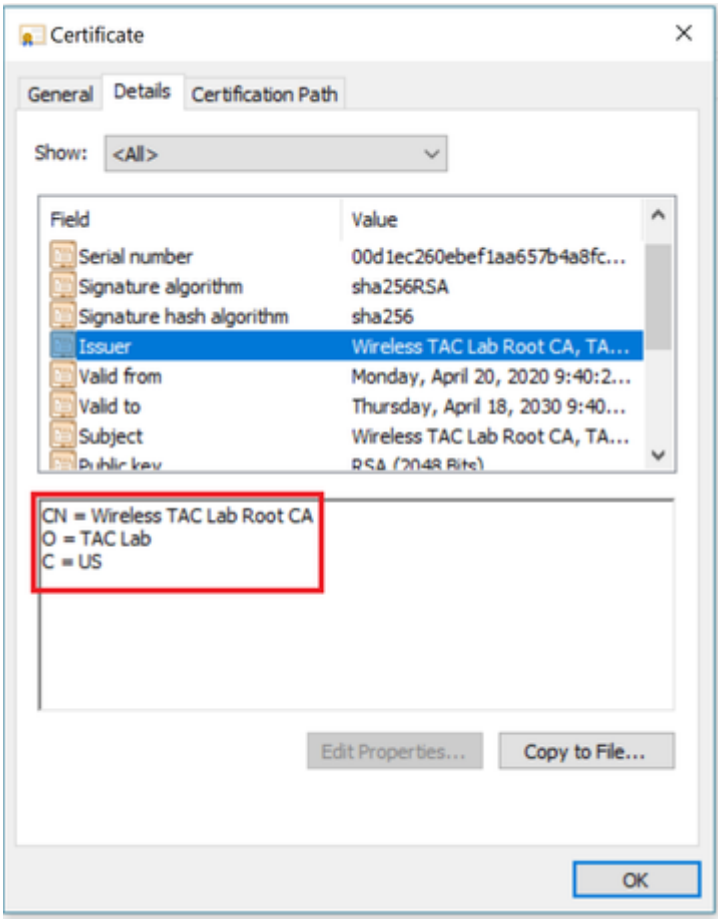
Certificado CA intermediário

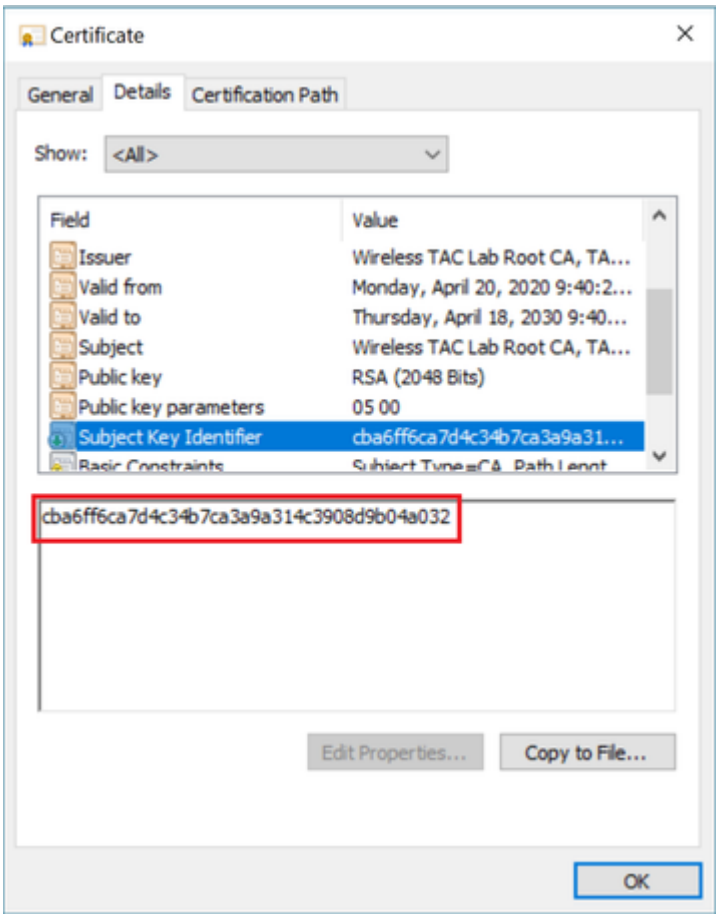




Certificado CA raiz:


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



Quando o certificado da CA raiz for identificado (o Emissor e o Assunto são os mesmos), continue com a cadeia de acordo e reinstale.

> **Observação**: este documento usa três cadeias de certificados (folha, CA intermediário, CA raiz), que é o cenário mais comum. Pode haver situações em que 2 certificados CA intermediários estão envolvidos. A mesma diretriz deste cenário pode ser usada até que o certificado de CA raiz seja encontrado.

Cenário 4. Não há certificados CA na cadeia

<#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.
```

Solução: Sem nenhum outro certificado no arquivo além do certificado WLC, a validação falha na **Verificação a 0 profundidade**. O arquivo pode ser aberto em um editor de texto para ser validado. As diretrizes dos cenários 2 e 3 podem ser seguidas para identificar a cadeia inteira até a CA raiz e reencadear de acordo e reinstalar.

Cenário 5. Nenhuma Chave 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.
```

Solução: a WLC espera que a chave privada seja incluída no arquivo se a CSR (Certificate Signing Request, solicitação de assinatura de certificado) tiver sido gerada externamente e precisar ser encadeada no arquivo. Caso o CSR tenha sido gerado na WLC, certifique-se de que a WLC não seja recarregada antes da instalação, caso contrário, a chave privada será perdida.

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.