Generieren von CSR für Drittanbieterzertifikate und Herunterladen von verketteten Zertifikaten für den WLC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Zertifikate auf AireOS-WLCs generiert und importiert werden.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, müssen Sie über folgende Themen verfügen:

- Konfigurieren des WLC, des Lightweight Access Point (LAP) und der Wireless Client Card für den Basisbetrieb
- Verwendung der OpenSSL-Anwendung
- Public-Key-Infrastructure und digitale Zertifikate

Verwendete Komponenten

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

- Cisco 5508 WLC mit Firmware-Version 8.3.102
- OpenSSL-Anwendung für Microsoft Windows
- Registrierungstool speziell für die Zertifizierungsstelle (Certification Authority, CA) eines Drittanbieters

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 verstehen.

Verkettete Zertifikate

Eine Zertifikatskette ist eine Folge von Zertifikaten, bei denen jedes Zertifikat in der Kette vom nachfolgenden Zertifikat signiert wird.

Der Zweck einer Zertifikatskette ist es, eine Vertrauenskette von einem Peer-Zertifikat zu einem vertrauenswürdigen CA-Zertifikat aufzubauen. Die Zertifizierungsstelle bestätigt die Identität im Peer-Zertifikat, wenn sie signiert wird.

Wenn die Zertifizierungsstelle eine vertrauenswürdige ist (durch eine Kopie des Zertifizierungsstellenzertifikats im Stammzertifikatverzeichnis angezeigt), impliziert dies, dass Sie auch dem signierten Peer-Zertifikat vertrauen können.

Häufig akzeptieren die Clients die Zertifikate nicht, da sie nicht von einer bekannten CA erstellt wurden. Der Client gibt in der Regel an, dass die Gültigkeit des Zertifikats nicht überprüft werden kann.

Dies ist der Fall, wenn das Zertifikat von einer zwischengeschalteten CA signiert wird, die dem Client-Browser nicht bekannt ist. In solchen Fällen muss ein verkettetes SSL-Zertifikat oder eine Zertifikatsgruppe verwendet werden.

Unterstützung für verkettete Zertifikate

Der Controller ermöglicht das Herunterladen des Gerätezertifikats als verkettetes Zertifikat für die Web-Authentifizierung.

Zertifikatsebenen

- Stufe 0 − Verwendung eines Serverzertifikats auf dem WLC
- Stufe 1 − Verwendung eines Serverzertifikats auf dem WLC und eines CA-Stammzertifikats
- Stufe 2 − Verwendung eines Serverzertifikats auf dem WLC, eines einzelnen CA-Zwischenzertifikats und eines CA-Stammzertifikats
- Stufe 3 − Verwendung eines Serverzertifikats auf dem WLC, zweier CA-Zwischenzertifikate und eines CA-Stammzertifikats

Der WLC unterstützt keine verketteten Zertifikate mit einer Größe von mehr als 10 KB auf dem WLC. Diese Einschränkung wurde jedoch in WLC Version 7.0.230.0 und höher entfernt.

Anmerkung: Verkettete Zertifikate werden unterstützt und sind für die Web-Authentifizierung und die Webverwaltung erforderlich

Anmerkung: Wildcard-Zertifikate werden vollständig für lokale EAP-, Management- oder Webauthentifizierung unterstützt.

Es gibt folgende Web-Authentifizierungszertifikate:

- Verkettet
- Nicht verkettet
- Automatisch generiert

Anmerkung: In WLC Version 7.6 und höher werden nur verkettete Zertifikate unterstützt (und sind daher erforderlich).

Um ein nicht verkettetes Zertifikat für Verwaltungszwecke zu erstellen, ignorieren Sie in diesem Dokument die Teile, in denen das Zertifikat mit dem Zertifizierungsstellenzertifikat kombiniert wird.

In diesem Dokument wird beschrieben, wie ein verkettetes SSL-Zertifikat (Secure Socket Layer) ordnungsgemäß auf einem WLC installiert wird.

Schritt 1: CSR erstellen

Es gibt zwei Möglichkeiten, eine CSR zu generieren. Entweder manuell mit OpenSSL (der einzige Weg, der in der WLC-Software vor 8.3 möglich ist), oder gehen Sie auf dem WLC selbst, um die CSR zu generieren (verfügbar nach 8.3.102).

Option A. CSR mit OpenSSL

Anmerkung: Chrome Version 58 und höher vertraut dem Common Name (CN) des Zertifikats nicht allein. Der Subject Alternate Name (SAN) muss ebenfalls vorhanden ist. Im nächsten Abschnitt wird erläutert, wie dem OpenSSL CSR, einer neuen Anforderung für diesen Browser, SAN-Felder hinzugefügt werden.

Führen Sie diese Schritte aus, um eine CSR mit OpenSSL zu generieren:

1. Installieren und öffnen Sie OpenSSL.

   In Microsoft Windows befindet sich openssl.exe standardmäßig unter **C:\ > openssl > bin.**

   Anmerkung: OpenSSL Version 0.9.8 wird für alte WLC-Versionen empfohlen. Ab Version 7.5 wurde jedoch auch die Unterstützung für OpenSSL Version 1.0 hinzugefügt (siehe Cisco Bug ID CSCti65315 - Need Support für Zertifikate, die mit OpenSSL v1.0 generiert wurden) und ist die empfohlene Version. OpenSSL 1.1 wurde ebenfalls getestet und funktioniert mit 8.x und späteren WLC-Versionen.
2. Suchen Sie die OpenSSL-Konfigurationsdatei und erstellen Sie eine Kopie, um sie für diese CSR zu bearbeiten. Bearbeiten Sie die Kopie, um die nächsten Abschnitte hinzuzufügen:

3.

```
[req]
req_extensions = v3_req

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

Die Zeilen, die mit "DNS.1", "DNS.2" (usw.) beginnen, müssen alle alternativen Namen Ihrer Zertifikate enthalten. Schreiben Sie dann alle möglichen URLs, die für den WLC verwendet werden. Die fett formatierten Zeilen im vorherigen Beispiel waren nicht vorhanden oder wurden in unserer offenenSSL-Testversion kommentiert. Sie kann je nach Betriebssystem und OpenSSL-Version stark variieren. In diesem Beispiel wird diese geänderte Version der Konfiguration als **openssl-san.cnf gespeichert.**

4. Geben Sie diesen Befehl ein, um eine neue CSR-Anfrage zu erstellen:

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
```

Anmerkung: WLCs unterstützen ab der Softwareversion 8.5 eine maximale Schlüsselgröße von 4.096 Bit

5. Einige Informationen werden angezeigt: Landesname, Staat bzw. Bundesland, Stadt usw. Geben Sie alle erforderlichen Informationen ein.

Anmerkung: Es ist wichtig, den richtigen Common Name anzugeben. Stellen Sie sicher, dass der Hostname, der zum Erstellen des Zertifikats (Common Name) verwendet wird, mit dem Domain Name System (DNS)-Hostnameneintrag für die IP-Adresse der virtuellen Schnittstelle auf dem WLC übereinstimmt und dass der Name auch im DNS vorhanden ist. Außerdem müssen Sie das System neu starten, nachdem die Änderung an der Virtual IP (VIP)-Schnittstelle vorgenommen wurde, damit diese Änderung wirksam wird.
Hier ein Beispiel:

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
Loading 'screen' into random state - done
Generate a 1024 bit RSA private key
.....................................................................++++++
.................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:(email address)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:OpenSSL>
```

6. Sie können die CSR (insbesondere bei presenceE-SAN-Attributen) mit openssl req -text -noout -in csrfilename überprüfen
7. Nachdem Sie alle erforderlichen Details eingegeben haben, werden zwei Dateien generiert:

   ein neuer privater Schlüssel, der den Namen **mykey.pem enthält**eine CSR, die den Namen **myreq.pem enthält**

Option B. CSR wird vom WLC erstellt

Wenn auf dem WLC die Softwareversion 8.3.102 oder höher ausgeführt wird, besteht die sicherere Option darin, den WLC zum Generieren des CSR zu verwenden. Der Vorteil ist, dass der Schlüssel auf dem WLC generiert wird auf dem WLC verbleibt und daher nie nach außen offengelegt wird.

Bisher ist es mit dieser Methode nicht möglich, SAN im CSR zu konfigurieren, was bekanntermaßen zu Problemen mit bestimmten Browsern führt, die das Vorhandensein eines SAN-Attributs erfordern. Einige CA ermöglichen das Einfügen von SAN-Feldern zum Zeitpunkt der Signierung. Es empfiehlt sich daher, sich mit Ihrer CA in Verbindung zu setzen.

Bei der CSR-Generierung durch den WLC selbst wird eine Schlüsselgröße von 2048 Bit und eine Schlüsselgröße von 256 Bit für den ecdsa-Schlüssel verwendet.

> **Anmerkung:** Wenn Sie den Befehl csr generation ausführen und das nachfolgende Zertifikat noch nicht installieren, wird der WLC beim nächsten Neustart auf HTTPS völlig unerreichbar gemacht, da der WLC den neu generierten CSR-Schlüssel nach dem Neustart verwendet, aber nicht über das entsprechende Zertifikat verfügt.

Um eine CSR für die Web-Authentifizierung zu generieren, geben Sie diesen Befehl ein:

```
(WLC) >config certificate generate csr-webauth BE BR Brussels Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQIIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
```

FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----

Um eine CSR für den Webadmin zu generieren, wechselt der Befehl zu:

(WLC) >config certificate generate csr-webadmin BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com

> **Anmerkung:** Die CSR wird auf dem Terminal angezeigt, nachdem Sie den Befehl eingegeben haben. Es gibt keine anderen Möglichkeiten, sie abzurufen. Es ist nicht möglich, sie vom WLC hochzuladen oder zu speichern. Sie müssen sie kopieren und in eine Datei auf Ihrem Computer einfügen, nachdem Sie den Befehl eingegeben haben. Der generierte Schlüssel verbleibt auf dem WLC, bis die nächste CSR generiert wird (der Schlüssel wird somit überschrieben). Wenn Sie die WLC-Hardware zu einem späteren Zeitpunkt (RMA) ändern müssen, können Sie das gleiche Zertifikat wie ein neuer Schlüssel nicht neu installieren, und auf dem neuen WLC wird eine CSR-Nummer generiert.

zu

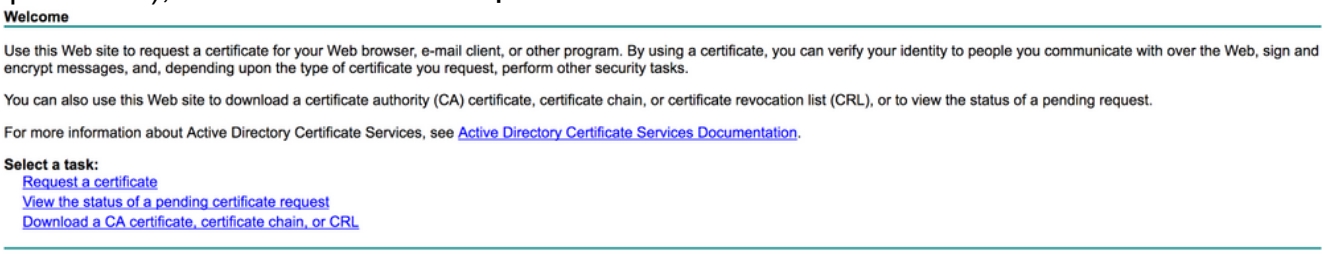
Sie müssen diese CSR dann an die Signaturstelle eines Drittanbieters oder die Public-Key-Infrastructure (PKI) des Unternehmens übergeben.

Schritt 2: Zertifikat signieren lassen

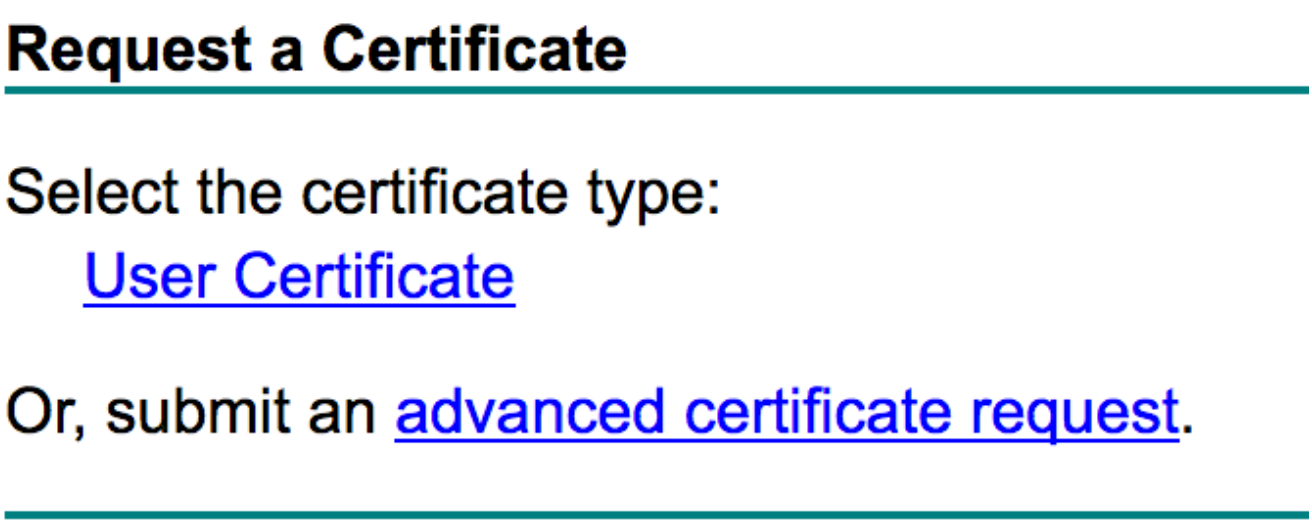
Option A: Abrufen der Datei Final.pem von Ihrer Unternehmenszertifizierungsstelle

In diesem Beispiel wird nur eine aktuelle CA für Unternehmen (in diesem Beispiel Windows Server 2012) gezeigt. Die Schritte zum Einrichten einer CA für Windows-Server werden nicht von Grund auf beschrieben.

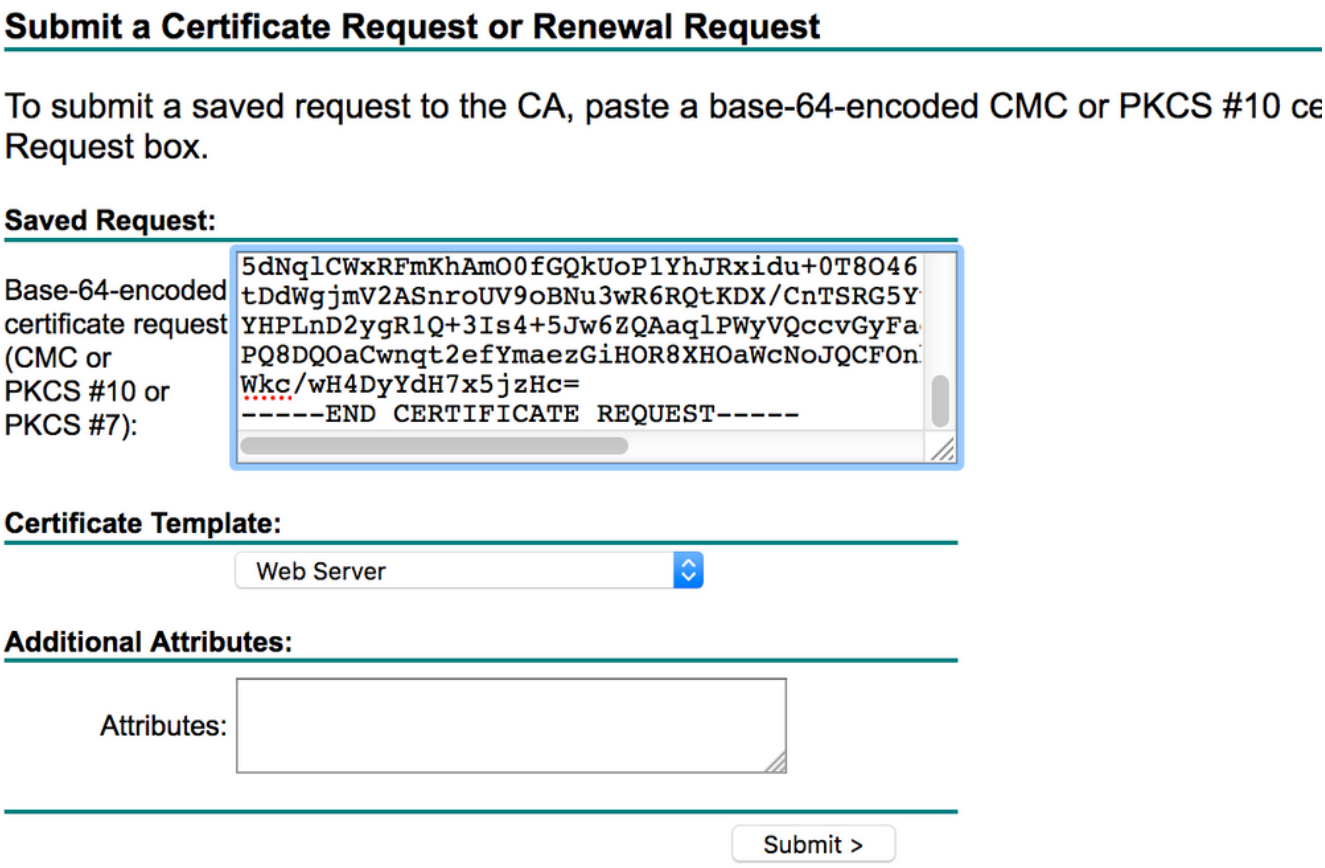
1. Öffnen Sie im Browser die Seite Ihres Unternehmens CA (in der Regel https://<CA-ip>/certsrv), und klicken Sie auf **Request a certificate**.



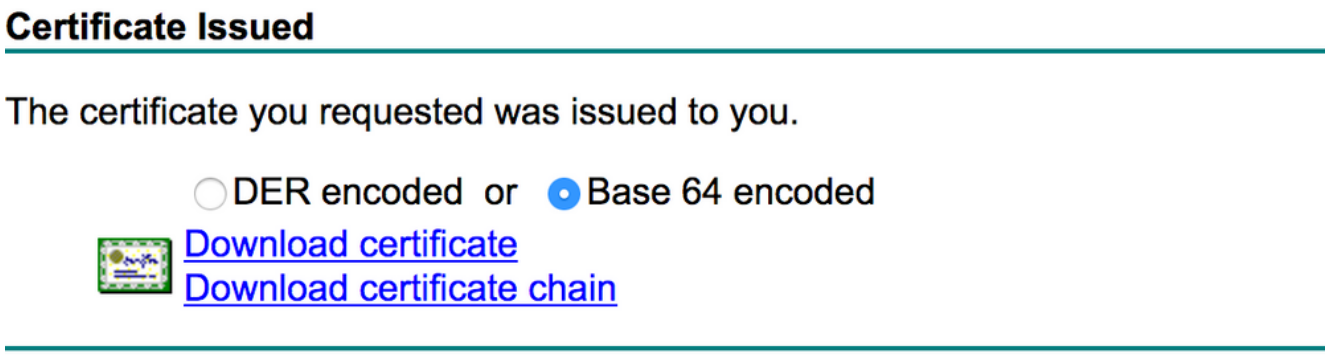
2. Klicken Sie auf **advanced certificate request**.



3. Geben Sie die CSR ein, die Sie vom WLC oder OpenSSL erhalten haben. Wählen Sie in der Dropdownliste Zertifikatvorlage die Option **Web Server**.



4. Klicken Sie auf **Base 64 encoded**ein.



5. Wenn das heruntergeladene Zertifikat vom Typ PKCS7 (.p7b) ist, konvertieren Sie es in PEM (im nächsten Beispiel wurde die Zertifikatskette als Dateiname "All certs.p7b" heruntergeladen):

```
openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem
```

6. Kombinieren Sie die Zertifikatskette (in diesem Beispiel wird sie als "All-certs.pem" bezeichnet) mit dem privaten Schlüssel, der zusammen mit dem CSR (dem privaten Schlüssel des Gerätezertifikats, in diesem Beispiel mykey.pem) generiert wurde, wenn Sie Option A (OpenSSL zum Generieren des CSR) ausgewählt haben, und speichern Sie die Datei als **final.pem**. Wenn Sie die CSR direkt vom WLC generiert haben (Option B), überspringen Sie diesen Schritt.

Geben Sie die folgenden Befehle in der OpenSSL-Anwendung ein, um die Dateien All-certs.pem und final.pem zu erstellen:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

Anmerkung: In diesem Befehl müssen Sie ein Kennwort für die Parameter -passin und -passout eingeben. Das für den Parameter -passout konfigurierte Kennwort muss mit dem auf dem WLC konfigurierten Parameter certpassword übereinstimmen. In diesem Beispiel lautet das Kennwort, das für die Parameter -passin und -passout konfiguriert ist, **check123**.

Final.pem ist die Datei, die auf den WLC heruntergeladen werden, wenn Sie "Option A. CSR mit OpenSSL".

Wenn Sie "Option B" gefolgt sind. "CSR generated by the WLC Self" (Vom WLC selbst generierte CSR) ist dann All-certs.pem die Datei, die auf den WLC heruntergeladen werden soll. Im nächsten Schritt müssen Sie diese Datei auf den WLC herunterladen.

Anmerkung: Wenn der Upload des Zertifikats in den WLC fehlschlägt, stellen Sie sicher, dass die gesamte Kette in der Paketdatei vorhanden ist. In Schritt 2 von Option B (erhalten Sie die final.pem-Datei von einer Zertifizierungsstelle eines Drittanbieters) wird gezeigt, wie sie aussehen muss. Wenn Sie nur ein Zertifikat in der Datei sehen, müssen Sie alle CA-Zwischenzertifikate und CA-Stammzertifikate manuell herunterladen und an die Datei anhängen (durch Kopieren und Einfügen), um die Kette zu erstellen.

Option B: Abrufen der Datei Final.pem von der Zertifizierungsstelle eines Drittanbieters

1. Kopieren Sie die CSR-Informationen und fügen Sie sie in ein CA-Registrierungstool ein.

   Nachdem Sie die CSR bei der Drittanbieter-CA eingereicht haben, signiert die Drittanbieter-CA das Zertifikat digital und sendet die signierte Zertifikatskette per E-Mail zurück. Bei verketteten Zertifikaten erhalten Sie die gesamte Zertifikatskette von der CA. Wenn Sie nur ein Zwischenzertifikat wie in diesem Beispiel haben, erhalten Sie diese drei Zertifikate von der CA:

   Stammzertifikat.pemZwischenzertifikat.pemGerätezertifikat.pem**Anmerkung:** Stellen Sie sicher, dass das Zertifikat Apache-kompatibel mit Secure Hash Algorithm 1 (SHA1)-Verschlüsselung ist.
2. Sobald alle drei Zertifikate vorliegen, kopieren Sie den Inhalt der einzelnen .pem-Dateien und fügen Sie ihn in eine anderer Datei in der folgenden Reihenfolge ein:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

3. Speichern Sie die Datei als **All-certs.pem.**

4. Kombinieren Sie das All-certs.pem-Zertifikat mit dem privaten Schlüssel, der zusammen mit dem CSR (dem privaten Schlüssel des Gerätezertifikats, der in diesem Beispiel mykey.pem lautet) generiert wurde, wenn Sie Option A (OpenSSL zum Generieren des CSR) verwenden, und speichern Sie die Datei als **final.pem**. Wenn Sie die CSR direkt vom WLC generiert haben (Option B), überspringen Sie diesen Schritt.

   Geben Sie die folgenden Befehle in der OpenSSL-Anwendung ein, um die Dateien All-certs.pem und final.pem zu erstellen:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
```

```
-passin pass:check123 -passout pass:check123
```

Anmerkung: In diesem Befehl müssen Sie ein Kennwort für die Parameter -passin und -passout eingeben. Das für den Parameter -passout konfigurierte Kennwort muss mit dem auf dem WLC konfigurierten Parameter certpassword übereinstimmen. In diesem Beispiel lautet das Kennwort, das für die Parameter -passin und -passout konfiguriert ist, **check123**.Final.pem ist die Datei, die auf den WLC heruntergeladen werden, wenn Sie "Option A. CSR mit OpenSSL". Wenn Sie "Option B" gefolgt sind. "CSR generated by the WLC Self" (Vom WLC selbst generierte CSR) ist dann All-certs.pem die Datei, die Sie auf den WLC herunterladen müssen. Im nächsten Schritt müssen Sie diese Datei auf den WLC herunterladen.

Anmerkung: SHA2 wird ebenfalls unterstützt. Die Cisco Bug-ID CSCuf20725 ist eine Anfrage für die SHA512-Unterstützung.

Schritt 3: CLI Herunterladen des Drittanbieterzertifikats auf den WLC mit der CLI

Gehen Sie wie folgt vor, um das verkettete Zertifikat über die CLI auf den WLC herunterzuladen:

1. Verschieben Sie die Datei **final.pem in das Standardverzeichnis auf Ihrem TFTP-Server.**
2. Geben Sie in der CLI diese Befehle ein, um die Downloadeinstellungen zu ändern:

```
    >transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip
```

```
>transfer download path
```

```
>transfer download filename final.pem
```

3. Geben Sie das Kennwort für die PEM-Datei ein, damit das Betriebssystem den SSL-Schlüssel und das Zertifikat entschlüsseln kann.

```
>transfer download certpassword password
```

Anmerkung: Stellen Sie sicher, dass der Wert für certpassword mit dem Parameterkennwort -passout übereinstimmt, das in Schritt 4 (oder 5) des Abschnitts Generieren einer CSR festgelegt wurde. In diesem Beispiel muss certpassword **check123** lauten. Wenn Sie Option B ausgewählt haben (d. h., verwenden Sie den WLC selbst, um die CSR zu generieren),

lassen Sie das Feld certpassword leer.

4. Geben Sie den Befehl **transfer download start** ein, um die aktualisierten Einstellungen anzuzeigen. Geben Sie dann bei der Eingabeaufforderung **y ein, um die aktuellen Download-Einstellungen zu bestätigen und den Download von Zertifikat und Schlüssel zu starten.** Hier ein Beispiel:

```
(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path......................................./
TFTP Filename............................ final.pem

This might take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer start.

Certificate installed.
Reboot the switch to use new certificate.
```

5. Starten Sie den WLC neu, damit die Änderungen übernommen werden.

Schritt 3: GUI Herunterladen des Drittanbieterzertifikats auf den WLC mit der GUI

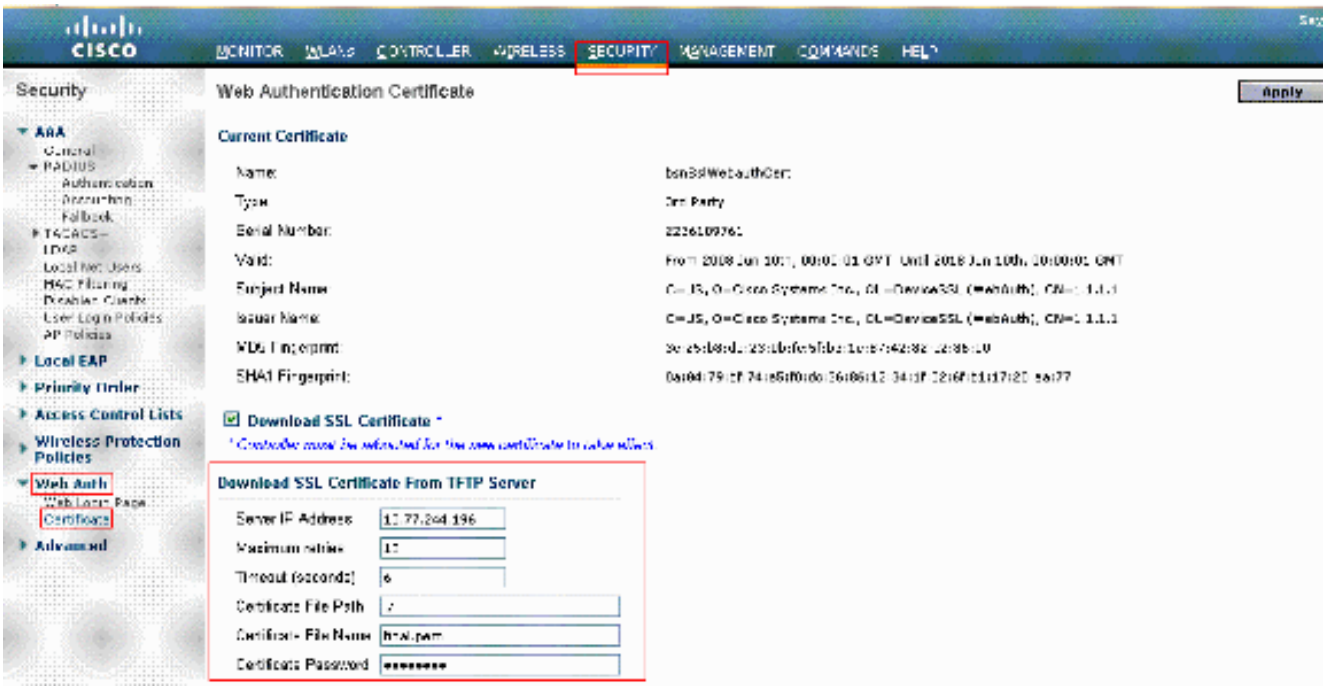
Gehen Sie wie folgt vor, um das verkettete Zertifikat über die Benutzeroberfläche in den WLC herunterzuladen:

1. Kopieren Sie das Gerätezertifikat final.pem in das Standardverzeichnis auf Ihrem TFTP-Server.

2. Auswählen **Security > Web Auth > Cert** , um die Seite Web Authentication Certificate (Webauthentifizierungszertifikat) zu öffnen.

3. Überprüfen Sie die **Download SSL Certificate**aktivieren, um die Parameter SSL-Zertifikat vom TFTP-Server herunterladen anzuzeigen.

4. Geben Sie im Feld „IP Address“ die IP-Adresse für den TFTP-Server ein.



5. Geben Sie im Feld „File Path“ (Dateipfad) den Verzeichnispfad des Zertifikats ein.

6. Geben Sie im Feld „File Name“ (Dateiname) den Namen des Zertifikats ein.

7. Geben Sie im Feld „Certificate Password“ (Zertifikatskennwort) das Kennwort ein, das zum Schutz des Zertifikats verwendet wurde.

8. Klicken Sie auf **Apply**.

9. Wenn der Download abgeschlossen ist, wählen Sie **Commands > Reboot > Reboot.**

10. Wenn Sie aufgefordert werden, die Änderungen zu speichern, klicken Sie auf **Save and Reboot.**

11. Klicken Sie auf **OK, um den Neustart des Controllers zu bestätigen.**

Fehlerbehebung

Um die Fehlerbehebung bei der Installation des Zertifikats auf dem WLC zu beheben, öffnen Sie eine Befehlszeile im WLC, und geben Sie **debug transfer all enable** and **debug pm pki enable ein,** schließen Sie dann das Download-Zertifikatsverfahren ab.

```
In some cases, the logs only say that the certificate installation failed:
*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing
Certificate.
*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13

TFTP receive complete... Installing Certificate.
*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.
*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.
```

Überprüfen Sie das Zertifikatsformat und die Zertifikatskette. Denken Sie daran, dass WLCs, die

älter als Version 7.6 sind, die gesamte Kette benötigen, sodass Sie Ihr WLC-Zertifikat nicht allein hochladen können. Die Kette bis zur Stammzertifizierungsstelle muss in der Datei vorhanden sein.

Im Folgenden finden Sie ein Beispiel für Debugs, wenn die Zwischenzertifizierungsstelle falsch ist:

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using
password check123
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password
check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate
(verify: YES)
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking
string length instead
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return
code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result
text: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at
0 depth: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM
certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table
(verifyChain: TRUE)
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

Überlegungen zur Hochverfügbarkeit (HA SSO)

Wie im Handbuch für die WLC-HA-SSO-Bereitstellung erläutert, werden Zertifikate in einem HA-SSO-Szenario nicht vom primären zum sekundären Controller repliziert.

Das bedeutet, dass Sie alle Zertifikate in die Sekundäreinheit importieren müssen, bevor Sie das HA-Paar bilden.

Ein weiterer Vorbehalt besteht darin, dass dies nicht funktioniert, wenn Sie die CSR (und den Schlüssel daher lokal erstellt) für den primären WLC generiert haben, da dieser Schlüssel nicht exportiert werden kann.

Die einzige Möglichkeit besteht darin, die CSR für den primären WLC mit OpenSSL zu generieren (und daher den Schlüssel an das Zertifikat anzuhängen) und diese Zertifikat-/Schlüsselkombination auf beiden WLCs zu importieren.

Zugehörige Informationen

- Generieren von CSR für Drittanbieterzertifikate und Herunterladen von nicht verketteten Zertifikaten für den WLC
- Generieren von Zertifikatsignierungsanfrage (Certificate Signing Request ;CSR) für ein Drittanbieterzertifikat auf einem Wireless Control System (WCS)
- Beispiel der Konfiguration einer Zertifikatsignierungsanfrage (Certificate Signing Request, CSR) auf einem Wireless Control System (WCS) auf einem Linux-Server
- Technischer Support und Dokumentation für Cisco Systeme
- WLC-HA-SSO-Handbuch