CSR genereren voor certificaten van derden en certificaten in ketens downloaden naar de WLC

Inhoud

Inleiding

Dit document beschrijft hoe u certificaten op AireOS WLC's kunt genereren en importeren.

Voorwaarden

Vereisten

Alvorens u deze configuratie probeert, moet u kennis hebben van deze onderwerpen:

- Hoe u de WLC, het Lichtgewicht Access Point (LAP) en de draadloze clientkaart voor basisbediening kunt configureren
- Hoe de OpenSSL-toepassing wordt gebruikt
- Openbare basisinfrastructuur en digitale certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5508 WLC-software met firmware versie 8.3.10

- OpenSSL-toepassing voor Microsoft Windows
- Inschrijvingsgereedschap dat specifiek is voor de certificeringsinstantie van derden (CA)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Gekette certificaten

Een certificeringsketen is een reeks certificaten waarbij elk certificaat in de keten door het volgende certificaat wordt ondertekend.

Het doel van een certificeringsketen is het opzetten van een vertrouwensketen van een peer certificaat tot een vertrouwde CA-certificaat. De CA vouches voor de identiteit in het peer certificaat wanneer het wordt ondertekend.

Als CA een is die u vertrouwt (aangegeven door de aanwezigheid van een exemplaar van het CA certificaat in uw folder van het wortelcertificaat), betekent dit dat u ook het ondertekende peer certificaat kunt vertrouwen.

Vaak aanvaarden de klanten de certificaten niet omdat ze niet door een bekende CA zijn gecreëerd. De cliënt geeft doorgaans aan dat de geldigheid van het certificaat niet kan worden geverifieerd.

Dit is het geval wanneer het certificaat wordt ondertekend door een intermediaire CA, die niet bekend is aan de browser van de cliënt. In dergelijke gevallen moet u een gekoppelde SSL-certificaat of certificeringsgroep gebruiken.

Ondersteuning van gekerfd certificaat

De controller laat toe dat het apparaatcertificaat wordt gedownload als een kettingcertificaat voor webverificatie.

certificaatniveau

- Niveau 0 - gebruik van alleen een servercertificaat op de WLC
- Niveau 1 - gebruik van een servercertificaat op de WLC en een CA wortel certificaat
- Niveau 2 - gebruik van een servercertificaat op de WLC, één CA-intermediair certificaat en een CA-basiscertificaat
- Niveau 3 - gebruik van een servercertificaat op de WLC, twee CA intermediaire certificaten en een CA wortel certificaat

De WLC ondersteunt gekoppelde certificaten niet meer dan 10 KB in grootte op de WLC. Deze beperking is echter zowel in WLC versie 7.0.230.0 als later verwijderd.

> **Opmerking:** Gefabriceerde certificaten worden ondersteund en daadwerkelijk vereist voor web authenticatie en web admin

> **Opmerking:** Wildkaartcertificaten worden volledig ondersteund voor lokaal MAP, beheer of

web-authenticatie

Web authenticatiecertificaten kunnen elk van de volgende soorten zijn:

- gebogen
- ongeketend
- Automatisch gegenereerd

Opmerking: In WLC versie 7.6 en hoger worden alleen gekoppelde certificaten ondersteund (en zijn daarom vereist)

Om een onbepaald certificaat te genereren voor beheerdoeleinden, wordt met dit document geen rekening gehouden met de onderdelen waarin het certificaat is gecombineerd met het CA-certificaat.

Dit document beschrijft hoe u een gekoppeld Secure Socket Layer (SSL)-certificaat naar een WLC kunt installeren.

Stap 1: genereert een CSR

Er zijn twee manieren om een MVO op te bouwen. Ofwel handmatig met OpenSSL (de enige manier die in de pre-8.3 WLC-software mogelijk is) of gebruik de WLC zelf om de CSR te genereren (Beschikbaar na 8.3.102).

Optie A. CSR met OpenSSL

Opmerking: Chrome versie 58 en later vertrouwt de gemeenschappelijke naam van het certificaat niet alleen en vereist dat ook de Onderwerp Alternate Name aanwezig is. In de volgende sectie wordt uitgelegd hoe u SAN-velden aan de OpenSSL CSR kunt toevoegen, wat een nieuwe eis voor deze browser is.

Voltooi deze stappen om een CSR met OpenSSL te genereren:

1. Installeer en open het OpenSSL.

   In Microsoft Windows is openssl.exe standaard gevestigd op **C:\ > openssl > bin**.

   Opmerking: OpenSSL versie 9.8 is de aanbevolen versie voor oude WLC-releases. vanaf versie 7.5 is er echter ook ondersteuning voor OpenSSL versie 1.0 toegevoegd (raadpleeg Cisco bug ID CSCti65315 - Noodondersteuning voor certificaten die gegenereerd zijn met OpenSSL v1.0) en is de aanbevolen versie voor gebruik. OpenSSL 1.1-werken zijn ook getest en werkt op 8.x en latere WLC-releases.
2. Pak uw OpenSSL configuratiebestand vast en maak een kopie ervan om het voor deze CSR te bewerken. Bewerk de kopie om de volgende secties toe te voegen:
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
```

De lijnen die met "DNS.1", "DNS.2" (enzovoort) beginnen, moeten alle alternatieve namen van uw certificaten bevatten. Schrijf vervolgens een mogelijke URL die voor de WLC gebruikt wordt. De regels in vet in het vorige voorbeeld waren niet aanwezig of werden becommentarieerd in onze lab openSSL-versie. Het kan enorm verschillen met het besturingssysteem en de opensl-versie. We slaan deze aangepaste versie van de configuratie op als **openssl-san.cnf** voor dit voorbeeld.

4. Typ deze opdracht om een nieuwe CSR te genereren:

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

Opmerking: WLC's ondersteunen een maximale grootte van 4096 bits per 8,5 softwareversie

5. Er is informatie te vinden onder: naam, staat, stad, enzovoort. Verstrek de vereiste informatie.

Opmerking: Het is belangrijk de juiste gemeenschappelijke naam te geven. Zorg ervoor dat de hostnaam die wordt gebruikt om het certificaat (Common Name) te maken overeenkomt met de bestandsnaam van het Domain Name System (DNS) voor het virtuele interface-IP-adres in de WLC en dat de naam ook in de DNS-indeling voorkomt. Ook, nadat u de wijziging in de Virtual IP (VIP)-interface hebt gemaakt, moet u het systeem opnieuw opstarten om deze verandering van kracht te laten worden.
Hierna volgt een voorbeeld:

```
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. U kunt de CSR (met name voor SAN-eigenschappen presencE) controleren met **openssl req -text -no-in csrfilename**
7. Nadat u alle vereiste gegevens hebt verstrekt, worden twee bestanden gegenereerd:

   een nieuwe privé - sleutel met de naam **mykey.pem**Een CSR met de naam **myreq.pem**

Optie B. CSR gegenereerd door de WLC

Als uw WLC-software versie 8.3.102 of hoger uitvoert, is de meer beveiligde optie om de WLC te gebruiken om de CSR te genereren. Het voordeel is dat de sleutel op de WLC wordt gegenereerd en nooit de WLC verlaat; in de buitenwereld wordt het dus nooit blootgelegd .

Met deze methode is het momenteel niet mogelijk SAN in de CSR te configureren, waarvan bekend is dat deze tot problemen met bepaalde browsers heeft geleid, hetgeen de aanwezigheid van een SAN-eigenschap vereist. Sommige CA staan toe om SAN velden op te nemen bij het ondertekenen van tijd, dus is het een goed idee om met uw CA te controleren.

CSR-generatie door het WLC zelf gebruikt een grootte van 2048 bits en de ecdsa-toets is 256 bits.

> **Opmerking:** Als u de opdracht voor csr-generatie uitvoert en het daaropvolgende certificaat nog niet installeert, wordt uw WLC bij de volgende herstart volledig onbereikbaar gemaakt voor HTTPS, omdat de WLC de nieuw gegenereerde CSR-toets gebruikt nadat u het opnieuw hebt opgestart, maar niet het certificaat heeft dat bij deze optie hoort.

Om een CSR voor web authenticatie te genereren dient u deze opdracht in te voeren:

(WLC) > **Config-certificaat genereert csr-website BE BR Brussel Cisco TAC mywebauthportal.wireless.com tac@cisco.com**

—BEGIN CERTIFICAATVERZOEK—
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMPEGydXNzZWxzMQ4w
DAYDVQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUWWiYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+UV5SCOuzfBsTz5bfQ1NLZqg1hNeminhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OFGOGu
NkgYefrrBN+WkDc6c55bxErwIDAQABoWQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafovphlcXIEIL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNQLCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
DdWgjmV2ASnroUV9BNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LKU6pzA69XD
YHPLnD2ygR1Q+3is4+5JW6ZQAaqlPWyVQcvGyFacscA7L+NZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+JSzt4

WKC/wH4DyYdH7x5jzHc=
—EINDCERTIFICAATVERZOEK—

Om een CSR voor de webadmin te genereren, verandert de opdracht in:

(WLC) > **Config-certificaat genereert csr-webadmin BE BR Brussel Cisco TAC mywebauthportal.wireless.com tac@cisco.com**

> **Opmerking:** De CSR wordt op de terminal afgedrukt nadat u de opdracht hebt ingevoerd. Er zijn geen andere manieren om het terug te krijgen; het is niet mogelijk om het uit de WLC te uploaden en het is ook niet mogelijk om het op te slaan. U moet deze naar een bestand op uw computer kopiëren/plakken nadat u de opdracht hebt ingevoerd. De gegenereerde toets blijft op de WLC totdat de volgende CSR gegenereerd wordt (de toets is dus overschreven). Als u de WLC-hardware later dient te wijzigen (RMA), kunt u niet hetzelfde certificaat opnieuw installeren als een nieuwe toets en wordt CSR gegenereerd op de nieuwe WLC.

in

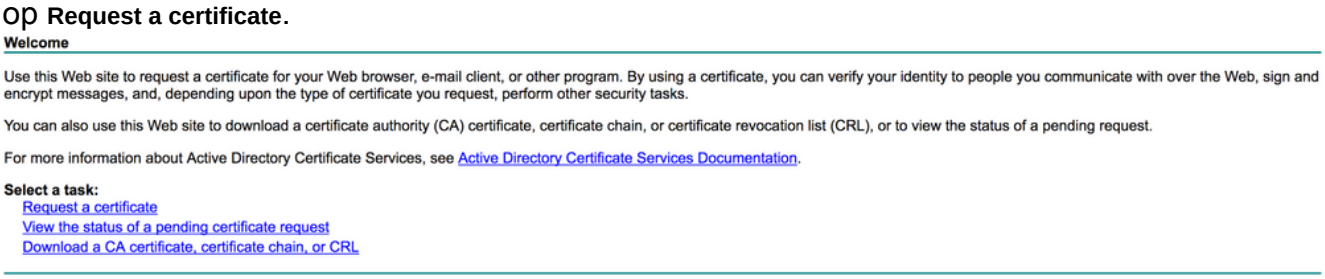
U moet deze CSR vervolgens overdragen aan uw ondertekenende autoriteit van derden of uw PKI-infrastructuur (Public Key Infrastructure).

Stap 2. Ontvang het certificaat

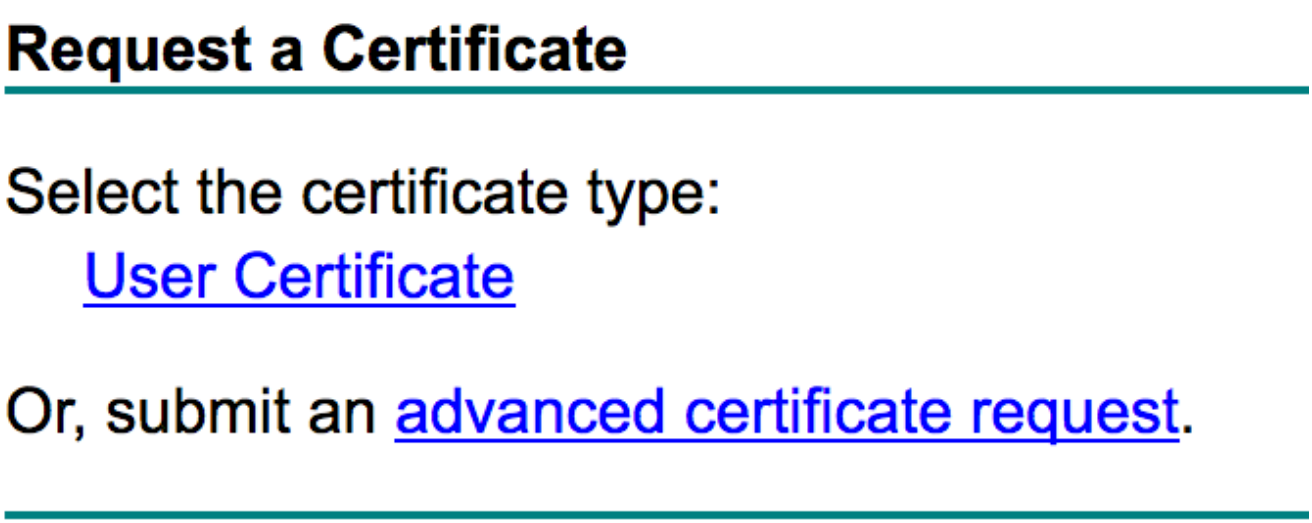
Optie A: Ontvang het bestand Final.pem van uw Enterprise CA

Dit voorbeeld laat alleen een huidige onderneming CA (Windows Server 2012 in dit voorbeeld) zien en heeft geen betrekking op de stappen om een Windows Server CA vanaf nul op te zetten.

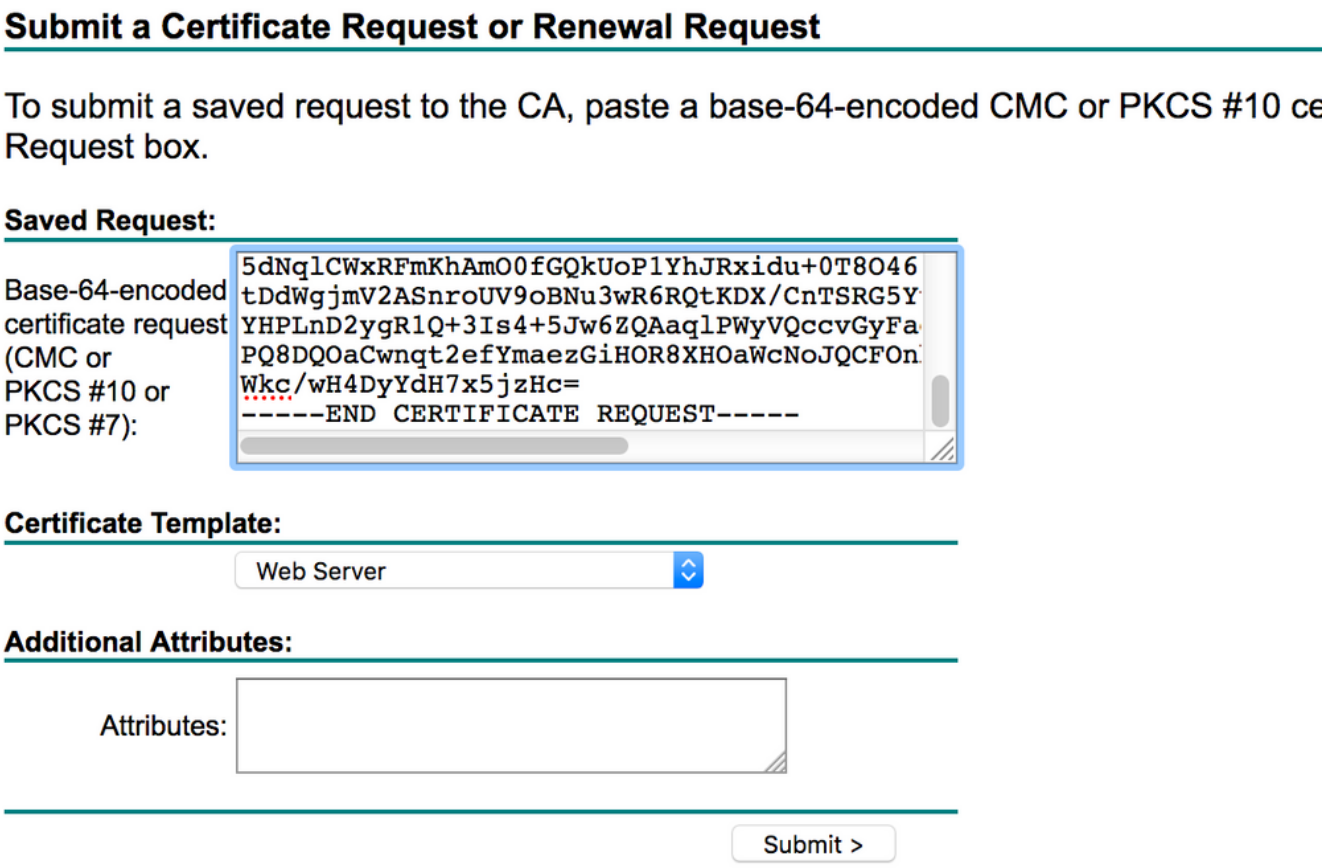
1. Ga naar de CA-pagina van uw bedrijf in de browser (meestal https://<CA-ip>/certsrv) en klik op **Request a certificate.**



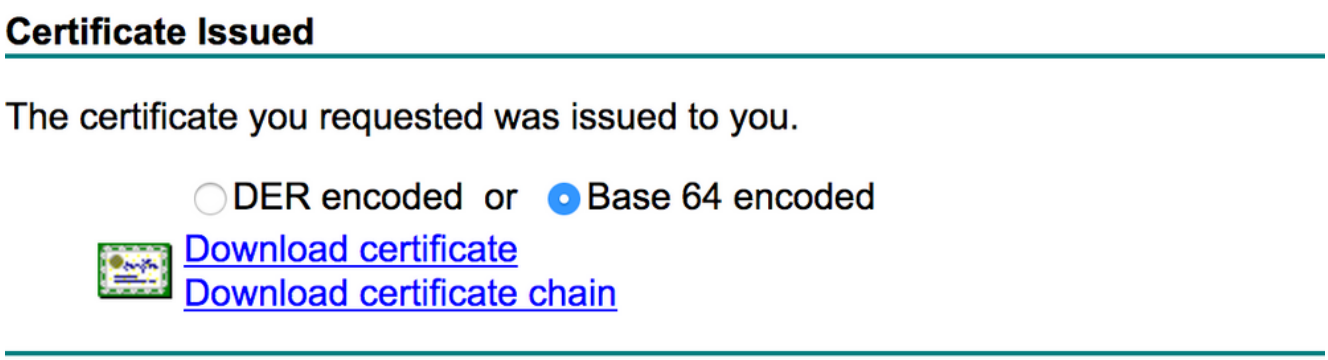
2. Klik **advanced certificate request.**



3. Voer de CSR in die u via WLC of OpenSSL hebt verkregen. Selecteer in de vervolgkeuzelijst certificaatsjabloon de optie **Web Server**.



4. Klik op het **Base 64 encoded**radioknop.



5. Als het gedownload certificaat van type PKCS7 (.p7b) is, moet het naar PEM worden geconverteerd (in het volgende voorbeeld werd de certificeringsketen gedownload als bestandsnaam "All-certs.p7b"):

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

6. Combineer de certificaatketen (in dit voorbeeld, wordt het "All-certs.pem" genoemd) certificaten met de privé sleutel die samen met de CSR (de privé sleutel van het apparaatcertificaat, dat in dit voorbeeld mykey.pem is) gegenereerd werd, als u met optie A (OpenSSL om de CSR te genereren) was gegaan en bewaar het bestand als **definitief.pem**. Als u de CSR rechtstreeks vanuit WLC (optie B) gegenereerd hebt, slaat u deze stap over.

Voer deze opdrachten in de OpenSSL-toepassing om de bestanden All-certs.pem en final.pem te maken:

```
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
```

Opmerking: In deze opdracht moet u een wachtwoord invoeren voor de parameters **- passin** en **-passout**. Het wachtwoord dat wordt ingesteld voor de **-passout**-parameter moet overeenkomen met de parameter **wachtwoord** die in de WLC is ingesteld. In dit voorbeeld is het wachtwoord dat is ingesteld voor zowel de parameters **-passin** als **-passout check123**.

Final.pem is het bestand dat u naar de WLC kunt downloaden als u "Optie A. CSR met OpenSSL" hebt gevolgd.

Als u "Optie B. CSR die door de WLC zelf gegenereerd is", dan is All-certs.pem het bestand dat u naar de WLC wilt downloaden. De volgende stap is het downloaden van dit bestand naar de WLC.

Opmerking: Als het uploaden van het certificaat naar de WLC mislukt, controleert u of er de

hele keten in het pem-bestand is. Raadpleeg stap 2 van optie B (verkrijg de finale.pem van een CA van de derde partij) om te zien hoe dit er moet uitzien. Als u slechts één certificaat in het bestand ziet, moet u alle middelste en basisbestanden van het CA-certificaat handmatig downloaden en naar het bestand toevoegen (door eenvoudige kopie te plakken) om de keten te maken.

Optie B: Verkrijg het bestand Final.pem van een derde partij CA

1. Kopieer en plak de CSR informatie in een CA-inschrijvingsgereedschap.

   Nadat u de CSR aan de CA van de derde partij hebt verzonden, tekent de CA van de derde digitaal het certificaat en stuurt zij de ondertekende certificatenketen via e-mail terug. In het geval van kettingcertificaten ontvangt u de gehele keten van certificaten van de CA. Als u slechts één tussencertificaat hebt zoals in dit voorbeeld, ontvangt u deze drie certificaten van CA:

   Opstartcertificaat.pemIntermediair certificaat.pemApparaatcertificaat.pem**Opmerking:** Zorg ervoor dat het certificaat compatibel is met Secure Hash Algorithm 1 (SHA1).
2. Zodra u alle drie de certificaten hebt, kopieert en voegt u de inhoud van elk .pem-bestand naar een ander bestand in deze volgorde:

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

3. Sla het bestand op als **All-certs.pem**.

4. Comprimeer het All-certs.pem certificaat met de privé sleutel die samen met de CSR gegenereerd is (de privé sleutel van het apparaatcertificaat, dat in dit voorbeeld mykey.pem is) als u optie A (OpenSSL) hebt gebruikt om de CSR te genereren, en bewaar het bestand als **finaal.pem**. Als u de CSR rechtstreeks vanuit WLC (optie B) gegenereerd hebt, slaat u deze stap over.

   Voer deze opdrachten in de OpenSSL-toepassing om de bestanden All-certs.pem en final.pem te maken:

```
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
```

   Opmerking: In deze opdracht moet u een wachtwoord invoeren voor de parameters **- passin**

en **-passout**. Het wachtwoord dat wordt ingesteld voor de **-passout**-parameter moet overeenkomen met de parameter **wachtwoord** die in de WLC is ingesteld. In dit voorbeeld is het wachtwoord dat is ingesteld voor zowel de parameters **-passin** als **-passout** **check123**.Final.pem is het bestand dat naar de WLC gedownload moet worden als u "Optie A. CSR met OpenSSL" volgde. Als u "Optie B. CSR die door de WLC zelf gegenereerd is", dan is All-certs.pem het bestand dat u naar de WLC moet downloaden. De volgende stap is het downloaden van dit bestand naar de WLC.

Opmerking: SHA2 wordt ook ondersteund. Cisco bug-ID CSCuf20725 is een verzoek voor SHA512-ondersteuning.

Stap 3 CLI. Download het certificaat van derden aan de WLC met de CLI

Voltooi deze stappen om het gekoppelde certificaat aan de WLC met de CLI te downloaden:

1. Verplaats het bestand**.pem** naar de standaardmap op uw TFTP-server.

2. Typ in het CLI deze opdrachten om de downloadinstellingen te wijzigen:

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

```
>transfer download path
```

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

3. Voer het wachtwoord voor het .pem-bestand in zodat het besturingssysteem de SSL-toets en het certificaat kan decrypteren.

```
>transfer download certpassword password
```

Opmerking: Verzeker u ervan dat de waarde voor **bepaalde wachtwoorden** hetzelfde is als het wachtwoord **-passout** dat is ingesteld in Stap 4 (of 5) van de sectie Generate een CSR. In dit voorbeeld moet het **defaultwachtwoord check123** zijn. Als u optie B (dat wil zeggen, gebruik de WLC zelf om de CSR te genereren), laat het veld Wachtwoord van het wachtwoord leeg.

4. Geef de opdracht **download start** van de **overdracht op** om de bijgewerkte instellingen te bekijken. Voer het formulier in om de huidige downloadinstellingen te bevestigen en start het certificaat en de toetsencombinatie. Hierna volgt een voorbeeld:

```
(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. Reinig de WLC zodat de wijzigingen van kracht kunnen worden.

Stap 3 GUI. Download het certificaat van derden aan de WLC met de GUI

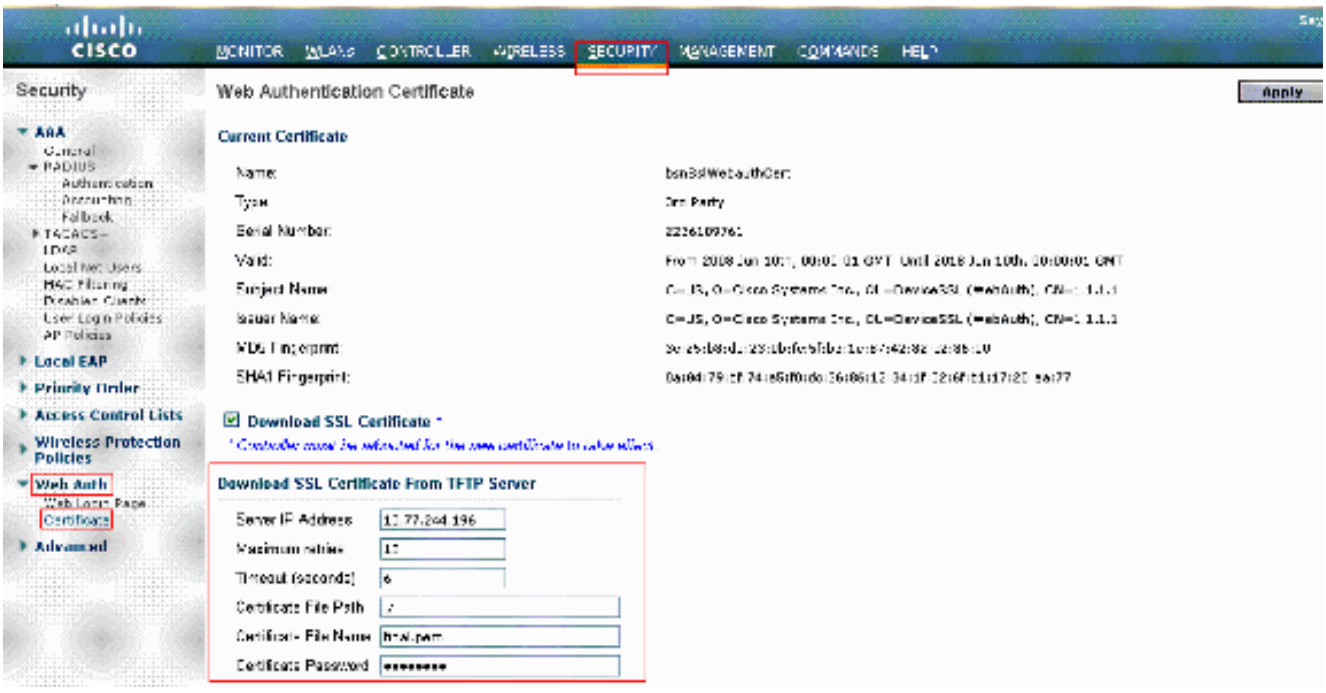
Voltooi de volgende stappen om het gechaineerde certificaat aan de GUI te downloaden:

1. Kopieer het apparaatcertificaat final.pem naar de standaardmap op uw TFTP-server.

2. Kies **Security > Web Auth > Cert** Zo opent u de pagina Web Verificatie-certificaat.

3. Controleer het **Download SSL Certificate**Schakel dit vakje in om het SSL-certificaat van de TFTP-serverparameters te bekijken.

4. Voer in het veld IP-adres het IP-adres van de TFTP-server in.



5. Typ in het veld Bestand pad de directory van het certificaat.

6. Typ in het veld Bestandsnaam de naam van het certificaat.

7. Typ in het veld Wachtwoord voor certificaat het wachtwoord dat is gebruikt om het certificaat te beveiligen.

8. Klik **Apply**.

9. Kies nadat de download is voltooid **Commands > Reboot > Reboot**.

10. Klik indien u wordt gevraagd de wijzigingen op te slaan **Save and Reboot**.

11. Klik op **OK** om te bevestigen dat u de controller wilt herstarten.

Problemen oplossen

Om de installatie van het certificaat op de WLC te kunnen oplossen, opent u een opdrachtregel in de WLC en **voert u debug transfer in, zodat u deze vervolgens kunt** en **debug pm kunt** uitvoeren.

```
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.
```

Controleer het certificaatformaat en de -keten. Vergeet niet dat WLC's die later zijn dan versie 7.6, vereisen dat de hele keten aanwezig is, zodat u uw WLC-certificaat niet alleen kunt uploaden. De ketting tot de wortel CA moet in het bestand aanwezig zijn.

Hier is een voorbeeld van debugs wanneer de intermediaire CA onjuist is:

```
*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
```

BF-overwegingen (High Availability)

Zoals uitgelegd in de WLC HA SSO-implementatiehandleiding, worden certificaten niet nagemaakt van primaire naar secundaire controller in een HA SSO-scenario.

Dit betekent dat je alle certificaten moet importeren naar de secundaire kliniek voordat je het HA-paar vormt.

Een ander voorbehoud is dat dit niet werkt als u de CSR (en daarom lokaal de sleutel creëerde) op de primaire WLC omdat die sleutel niet geëxporteerd kan worden.

De enige manier is het genereren van de CSR voor het primaire WLC met OpenSSL (en dus de sleutel aan het certificaat gekoppeld) en het importeren van de certificaat/sleutelcombinatie op beide WLC's.

Gerelateerde informatie

- CSR genereren voor certificaten van derden en ongebonden certificaten downloaden aan de WLC
- CSR-generatie (certificaataanvraag) voor een certificaat van derden op een draadloos controlesysteem (WCS)
- WCS (Wireless Control System) certificaataanvraag (CSR) geïnstalleerd op een configuratievoorbeeld van Linux-server
- Technische ondersteuning en documentatie – Cisco Systems
- WLC HA SSO-handleiding