Generazione delle richieste CSR per certificati di terze parti e download di catene di certificati sul WLC

Sommario

Introduzione

In questo documento viene descritto come generare e importare certificati sui WLC di AireOS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare il WLC, il Lightweight Access Point (LAP) e la scheda client wireless per un funzionamento di base?
- Come utilizzare l'applicazione OpenSSL.
- Infrastruttura a chiave pubblica e certificati digitali

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 5508 WLC con firmware versione 8.3.102
- Applicazione OpenSSL per Microsoft Windows
- Strumento di registrazione specifico per l'Autorità di certificazione (CA) di terze parti

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Certificati concatenati

Una catena di certificati è una sequenza di certificati in cui ogni certificato della catena è firmato dal certificato successivo.

Lo scopo di una catena di certificati è stabilire una catena di attendibilità da un certificato peer a un certificato CA attendibile. La CA garantisce l'identità nel certificato peer quando è firmato.

Se la CA è considerata attendibile (indicata dalla presenza di una copia del certificato CA nella directory principale del certificato), è possibile considerare attendibile anche il certificato peer firmato.

Spesso i client non accettano i certificati perché non sono stati creati da una CA nota. Il client in genere indica che non è possibile verificare la validità del certificato.

Ciò si verifica quando il certificato è firmato da una CA intermedia, che non è nota al browser client. In questi casi, è necessario utilizzare un certificato SSL concatenato o un gruppo di certificati.

Supporto per certificati concatenati

Il controller consente di scaricare il certificato del dispositivo come certificato concatenato per l'autenticazione Web.

Livelli certificato

- Livello 0 - Utilizzo di un solo certificato server sul WLC
- Livello 1 - Utilizzo di un certificato server sul WLC e di un certificato radice CA
- Livello 2 - Utilizzo di un certificato server sul WLC, un singolo certificato intermedio CA e un certificato radice CA
- Livello 3 - Utilizzo di un certificato server sul WLC, due certificati intermedi CA e un certificato radice CA

Il WLC non supporta certificati concatenati di dimensioni superiori a 10 KB sul WLC. Tuttavia, questa restrizione è stata rimossa in WLC versione 7.0.230.0 e successive.

Nota: i certificati concatenati sono supportati ed effettivamente necessari per l'autenticazione e l'amministrazione Web

---

Nota: i certificati con caratteri jolly sono completamente supportati per l'autenticazione EAP, di gestione o Web locale

---

I certificati di autenticazione Web possono essere i seguenti:

- Concatenato
- Non concatenato
- Generato automaticamente

Nota: in WLC versione 7.6 e successive, sono supportati solo i certificati concatenati (e pertanto obbligatori)

Per generare un certificato non concatenato a scopo di gestione, questo documento ignora le parti in cui il certificato è combinato con il certificato CA.

In questo documento viene descritto come installare correttamente un certificato SSL (Secure Sockets Layer) concatenato in un WLC.

Passaggio 1. Genera un CSR

Esistono due modi per generare un CSR. Manualmente con OpenSSL (l'unico modo possibile nel software WLC precedente alla versione 8.3) oppure sul WLC stesso per generare il CSR (disponibile dopo la versione 8.3.102).

Opzione A. CSR con OpenSSL

Nota: Chrome versione 58 e successive non considera attendibile solo il nome comune del certificato e richiede che sia presente anche il nome soggetto alternativo. La sezione successiva spiega come aggiungere campi SAN al CSR OpenSSL, che è un nuovo requisito per questo browser.

Completare questa procedura per generare un CSR con OpenSSL:

1. Installare e aprire OpenSSL .

   In Microsoft Windows, per impostazione predefinita, il file openssl.exe si trova in **C:\ > openssl > bin.**

   Nota: OpenSSL versione 0.9.8 è la versione consigliata per le versioni precedenti di WLC; tuttavia, a partire dalla versione 7.5, è stato aggiunto anche il supporto per OpenSSL versione 1.0 (fare riferimento all'ID bug Cisco CSCti65315 - È necessario il supporto per i certificati generati con OpenSSL v1.0) ed è la versione consigliata da utilizzare. OpenSSL 1.1 funziona anche su versioni 8.x e successive di WLC.

2. Individuare il file di configurazione OpenSSL e crearne una copia per modificarlo per questo CSR. Modifica la copia per aggiungere le sezioni successive:
3. <#root>

```
[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
```

Le righe che iniziano con "DNS.1", "DNS.2" e così via devono contenere tutti i nomi alternativi dei certificati. Scrivere quindi eventuali URL utilizzati per il WLC. Le righe in grassetto nell'esempio precedente non erano presenti o sono state commentate nella nostra versione lab openSSL. Può variare molto a seconda del sistema operativo e della versione openssl. La versione modificata della configurazione verrà salvata con nome **openssl-san.cnf** per questo esempio.

4. Immettere questo comando per generare un nuovo CSR:

```
<#root>

OpenSSL>

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

> **Nota**: i WLC supportano una dimensione massima della chiave di 4096 bit a partire dalla versione software 8.5

---

5. Viene richiesto di fornire alcune informazioni: nome del paese, stato, città e così via. Fornire le informazioni richieste.

> **Nota**: è importante fornire il nome comune corretto. Verificare che il nome host utilizzato per creare il certificato (nome comune) corrisponda alla voce del nome host DNS (Domain Name System) per l'indirizzo IP dell'interfaccia virtuale sul WLC e che il nome esista anche nel DNS. Inoltre, dopo aver apportato la modifica all'interfaccia IP virtuale (VIP), è necessario riavviare il sistema per rendere effettiva la modifica.

Di seguito è riportato un esempio:

```
<#root>

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. È possibile verificare la CSR (in particolare per gli attributi SAN presentiE) con **openssl req -text -noout -in csrfilename**
7. Dopo aver fornito tutti i dettagli richiesti, vengono generati due file:

   - una nuova chiave privata che include il nome **mykey.pem**
   - un CSR che include il nome **myreq.pem**

Opzione B. CSR generato dal WLC

Se il WLC esegue il software versione 8.3.102 o successive, l'opzione più sicura è quella di utilizzare il WLC per generare il CSR. Il vantaggio è che la chiave viene generata sul WLC e non lascia mai il WLC; quindi non viene mai esposta nel mondo esterno.

Attualmente, questo metodo non consente di configurare la SAN nel CSR, che è noto possa causare problemi con alcuni browser che richiedono la presenza di un attributo SAN. Alcune CA consentono di inserire campi SAN al momento della firma, pertanto è consigliabile verificare con la CA.

La generazione della CSR da parte del WLC utilizza una chiave di 2048 bit e una chiave ecdsa di 256 bit.

> **Nota**: se si esegue il comando csr generation e non si installa ancora il certificato successivo, il WLC viene reso completamente irraggiungibile su HTTPS al successivo riavvio, in quanto il WLC utilizza la chiave CSR appena generata dopo il riavvio ma non dispone del certificato associato.

Per generare un CSR per l'autenticazione Web, immettere questo comando:

(WLC)**config certificate generate csr-webauth BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com**
â€”INIZIA RICHIESTA CERTIFICATOâ€”
MIICqjCAZICAQAwZTELMAkGA1UECAwCQlIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OjFGOGu
NkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K

ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
DtWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc= Wkc/wH4DyYdH7x5jzHc
â€”TERMINA RICHIESTA CERTIFICATOâ€”

Per generare un CSR per l'amministratore Web, il comando viene modificato in:

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

---

> **Nota**: dopo aver immesso il comando, il CSR viene stampato sul terminale. Non ci sono altri modi per recuperarlo; non è possibile caricarlo dal WLC né salvarlo. È necessario copiarlo/incollarlo in un file sul computer dopo aver immesso il comando. La chiave generata rimane sul WLC finché non viene generato il CSR successivo (la chiave viene quindi sovrascritta). In caso sia necessario modificare l'hardware WLC in un secondo momento (RMA), non sarà possibile reinstallare lo stesso certificato di una nuova chiave e sul nuovo WLC verrà generato CSR.

> a

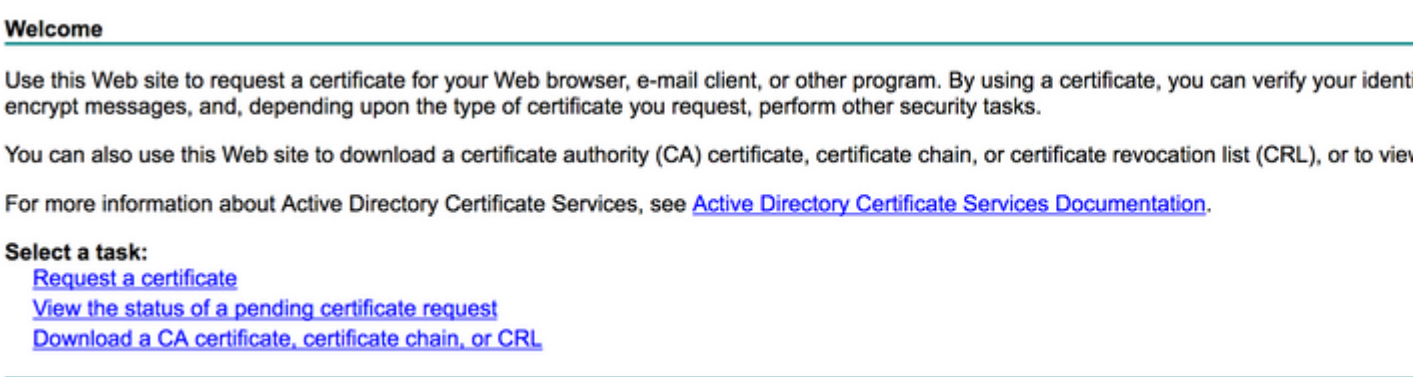
Sarà quindi necessario consegnare questo CSR all'autorità di firma di terze parti o all'infrastruttura a chiave pubblica (PKI) dell'organizzazione.

Passaggio 2. Ottieni certificato firmato

Opzione A: recupero del file Final.pem dalla CA dell'organizzazione (Enterprise)

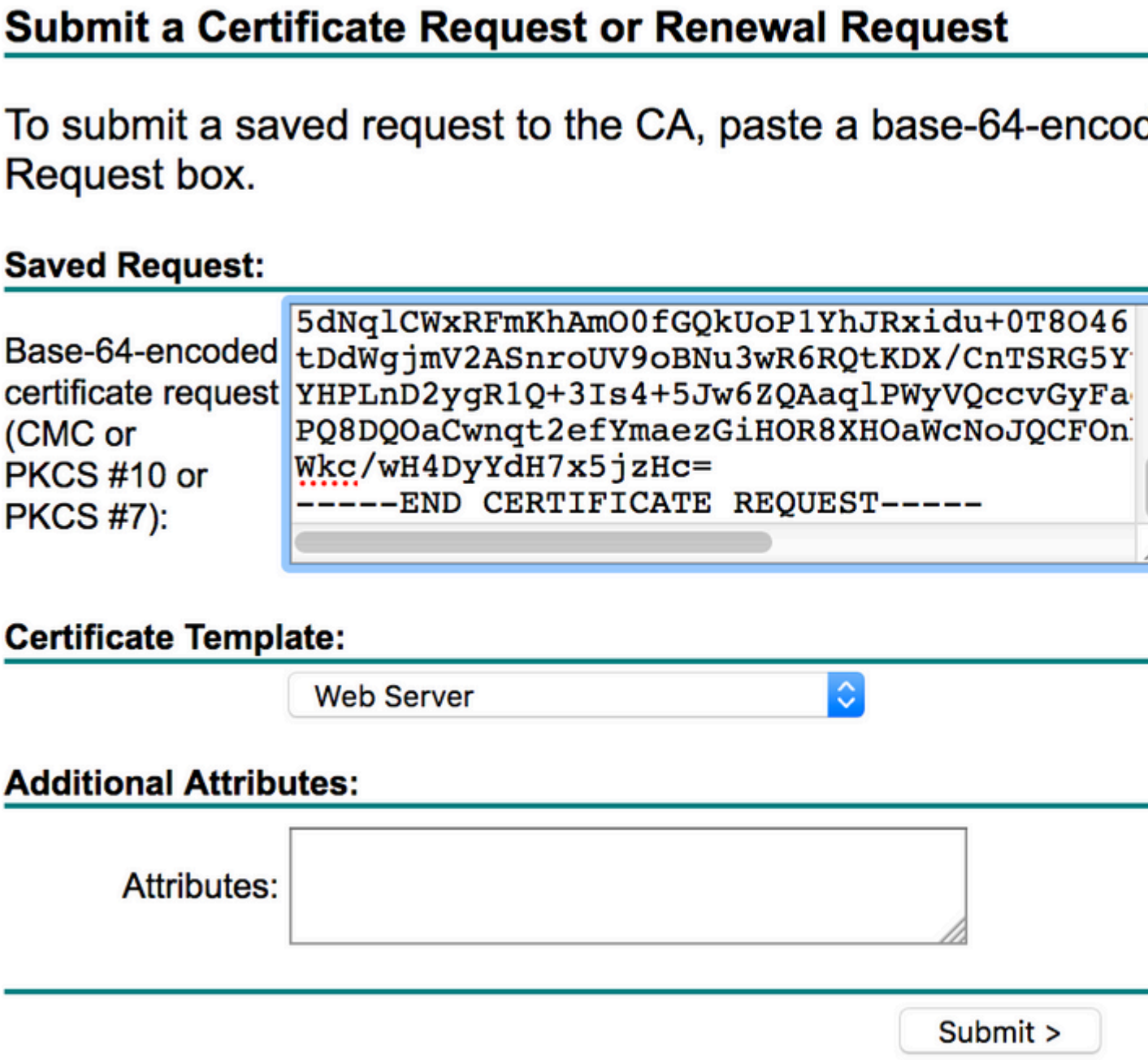
In questo esempio viene illustrata solo una CA dell'organizzazione (Windows Server 2012 nell'esempio) corrente e non vengono illustrati i passaggi necessari per configurare una CA di Windows Server da zero.

1. Andare alla pagina CA dell'azienda nel browser (generalmente https://<CA-ip>/certsrv) e fare clic su **Request a certificate.**

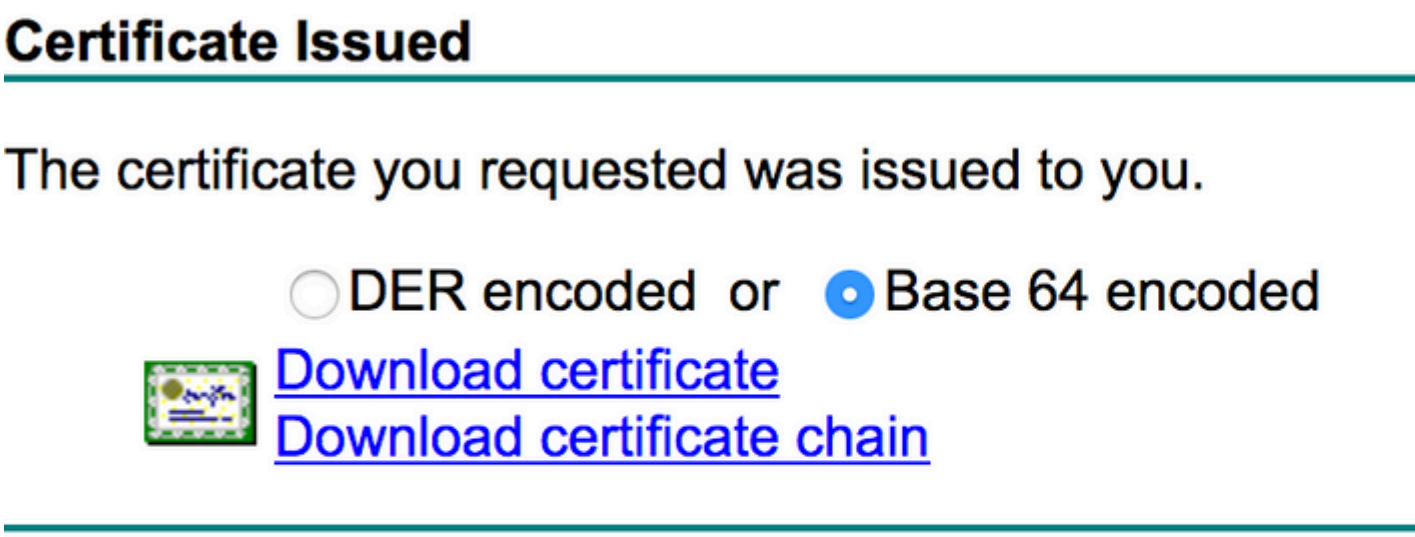


2. Fare clic su **advanced certificate request.**

3. Immettere il CSR ottenuto dal WLC o da OpenSSL. Nell'elenco a discesa Modello di certificato scegliere **Web Server**.



4. Fare clic sul pulsante **Base 64 encoded**pulsante di opzione.



5. Se il certificato scaricato è di tipo PKCS7 (.p7b), convertirlo in PEM (nell'esempio successivo la catena di certificati è stata scaricata come nome file "All-certs.p7b"):

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

6. Combinare la catena di certificati (nell'esempio riportato il nome è "All-certs.pem") con la chiave privata generata insieme al CSR (la chiave privata del certificato del dispositivo, che in questo esempio è mykey.pem) se si è utilizzata l'opzione A (OpenSSL per generare il CSR) e salvare il file come **final.pem**. Se la CSR è stata generata direttamente dal WLC (opzione B), ignorare questo passaggio.

Immettere questi comandi nell'applicazione OpenSSL per creare i file All-certs.pem e final.pem:

<#root>

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

Nota: in questo comando è necessario immettere una password per i parametri **-passin** e **-passout**. La password configurata per il parametro **-passout** deve corrispondere al parametro **certpassword** configurato sul WLC. Nell'esempio, la password configurata per i parametri **-passin** e **-passout** è **check123**.

Final.pem è il file da scaricare sul WLC se è stata seguita l'opzione A. CSR con OpenSSL.

Se è stata seguita l'opzione B. CSR generato dal WLC stesso, All-certs.pem è il file da scaricare sul WLC. Il passaggio successivo è quello di scaricare questo file sul WLC.

Nota: se il caricamento del certificato nel WLC non riesce, verificare che ci sia l'intera catena nel file pem. Fare riferimento al passaggio 2 dell'opzione B (ottenere il file final.pem da un'autorità di certificazione di terze parti) per vedere come deve apparire. Se nel file è presente un solo certificato, è necessario scaricare manualmente tutti i file dei certificati CA intermedi e radice e aggiungerli (mediante semplice copia e incolla) al file per creare la catena.

Opzione B: recupero del file Final.pem da un'autorità di certificazione di terze parti

1. Copiare e incollare le informazioni CSR in qualsiasi strumento di registrazione CA.

   Dopo l'invio del CSR all'autorità di certificazione di terze parti, quest'ultima firma digitalmente il certificato e restituisce la catena di certificati firmata tramite posta elettronica. Nel caso di certificati concatenati, si riceve l'intera catena di certificati dalla CA. Se si dispone di un solo certificato intermedio, come nell'esempio riportato, dalla CA verranno inviati i tre certificati seguenti:

   - Certificato radice.pem
   - Certificato intermedio.pem
   - Certificato dispositivo.pem

   Nota: verificare che il certificato sia compatibile Apache con la crittografia SHA1 (Secure Hash Algorithm 1).

2. Dopo avere ottenuto tutti e tre i certificati, copiare e incollare il contenuto di ogni file con estensione pem in un altro file nell'ordine seguente:

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

3. Salvare il file come **All-certs.pem**.

4. Combinare il certificato All-certs.pem con la chiave privata generata insieme al CSR (la chiave privata del certificato del dispositivo, che in questo esempio è mykey.pem) se si è utilizzata l'opzione

A (OpenSSL per generare il CSR) e salvare il file come **final.pem**. Se la CSR è stata generata direttamente dal WLC (opzione B), ignorare questo passaggio.

Immettere questi comandi nell'applicazione OpenSSL per creare i file All-certs.pem e final.pem:

```
<#root>

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
```

Nota: in questo comando è necessario immettere una password per i parametri **-passin** e **-passout**. La password configurata per il parametro **-passout** deve corrispondere al parametro **certpassword** configurato sul WLC. Nell'esempio, la password configurata per i parametri **-passin** e **-passout** è **check123**.

Final.pem è il file da scaricare sul WLC se è stata seguita l'opzione A. CSR con OpenSSL. Se è stata seguita l'opzione B. CSR generato dal WLC stesso, All-certs.pem è il file da scaricare sul WLC. Il passaggio successivo è quello di scaricare questo file sul WLC.

Nota: è supportato anche SHA2. L'ID bug Cisco CSCuf20725 è una richiesta di supporto per SHA512.

Passaggio 3 CLI. Scaricare il certificato di terze parti nel WLC con la CLI

Completare questi passaggi per scaricare il certificato concatenato sul WLC con la CLI:

1. Spostare il file **final.pem** nella directory predefinita sul server TFTP.
2. Nella CLI, immettere questi comandi per modificare le impostazioni di download:

```
<#root>

    >

transfer download mode tftp


    >

transfer download datatype webauthcert
```

```
    >
transfer download serverip
```

```
    >
transfer download path
```

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

3. Immettere la password per il file con estensione pem in modo che il sistema operativo possa decrittografare la chiave e il certificato SSL.

```
<#root>

>

transfer download certpassword password
```

Nota: assicurarsi che il valore per **certpassword** sia lo stesso della password del parametro **-passout** impostata nel passaggio 4 (o 5) della sezione Generate a CSR. Nell'esempio, il valore di **certpassword** deve essere **check123**. Se è stata scelta l'opzione B (ossia, utilizzare il WLC stesso per generare il CSR), lasciare vuoto il campo certpassword.

---

4. Immettere il **transfer download start** per visualizzare le impostazioni aggiornate. Quindi immettere **y** al prompt per confermare le impostazioni di download correnti e avviare il download del certificato e della chiave. Di seguito è riportato un esempio:

```
<#root>

(Cisco Controller) >

transfer download start
```

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
```

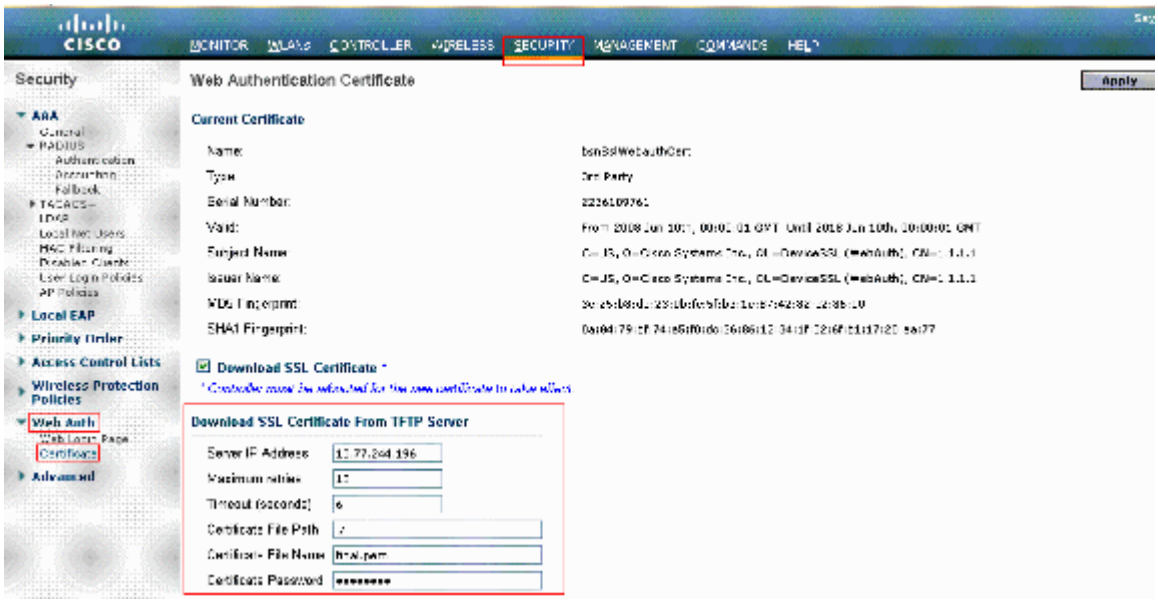
```
TFTP Max Retries..............................  10
TFTP Path.....................................  /
TFTP Filename.................................  final.pem

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. Riavviare il WLC per rendere effettive le modifiche.

Interfaccia grafica 3. Scaricare il certificato di terze parti sul WLC con la GUI

Completare questi passaggi per scaricare il certificato concatenato sul WLC con la GUI:

1. Copiare il certificato del dispositivo final.pem nella directory predefinita del server TFTP.
2. Scegli **Security** > **Web Auth** > **Cert** per aprire la pagina Certificato di autenticazione Web.
3. Controllare la **Download SSL Certificate**per visualizzare i parametri Scarica certificato SSL dal server TFTP.
4. Nel campo Indirizzo IP, immettere l'indirizzo IP del server TFTP.



5. Nel campo Percorso file immettere il percorso della directory del certificato.
6. Nel campo Nome file immettere il nome del certificato.
7. Nel campo Password certificato immettere la password utilizzata per proteggere il certificato.
8. Fare clic su **Apply**.
9. Al termine del download, scegliere **Commands > Reboot > Reboot.**
10. Se viene richiesto di salvare le modifiche, fare clic su **Save and Reboot.**
11. Fare clic su **OK** per confermare la decisione di riavviare il controller.

Risoluzione dei problemi

Per risolvere i problemi di installazione del certificato sul WLC, aprire una riga di comando sul WLC e immettere **debug transfer all enable** e **debug pm pki enable** quindi completare la procedura di download del certificato.

```
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.
```

Verificare il formato e la catena del certificato. Tenere presente che le WLC successive alla versione 7.6 richiedono la presenza dell'intera catena, quindi non è possibile caricare il certificato WLC da solo. La catena fino alla CA radice deve essere presente nel file.

Di seguito è riportato un esempio di debug quando la CA intermedia non è corretta:

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using password ch
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password check12
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) t
*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 le
*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
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth
*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 (verifyCh
```

```
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

Considerazioni su High Availability (HA SSO)

Come spiegato nella guida alla distribuzione di WLC HA SSO, i certificati non vengono replicati dal controller primario a quello secondario in uno scenario HA SSO.

Ciò significa che è necessario importare tutti i certificati nel database secondario prima di formare la coppia HA.

Un'altra avvertenza è che questa operazione non funziona se il file CSR (e quindi la chiave è stata creata localmente) è stato generato sul WLC primario perché la chiave non può essere esportata.

L'unico modo è generare il CSR per il WLC primario con OpenSSL (e quindi avere la chiave collegata al certificato) e importare la combinazione di certificato/chiave su entrambi i WLC.

Informazioni correlate

- **Genera CSR per certificati di terze parti e scarica i certificati non concatenati nel WLC**
- **Generazione di una richiesta di firma del certificato (CSR) per un certificato di terze parti su un sistema di controllo wireless (WCS)**
- **Esempio di richiesta di firma del certificato (CSR) Wireless Control System (WCS) installata su un server Linux**
- **Documentazione e supporto tecnico â€“ Cisco Systems**
- **Guida WLC HA SSO**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).