# Gerencia o CSR para Certificados da terceira e transfira Certificados acorrentados ao WLC

## Índice



## Introdução

Este original descreve como gerar uma solicitação de assinatura de certificado (CSR) a fim obter um certificado da terceira e como transferir um certificado acorrentado a um controlador do Wireless LAN (WLAN) (WLC).

## Pré-requisitos

### Requisitos

Antes que você tente esta configuração, você deve ter o conhecimento destes assuntos:

- Como configurar o WLC, o Access point de pouco peso (REGAÇO), e o cartão do cliente Wireless para a operação básica
- Como usar o aplicativo do OpenSSL
- Infraestrutura de chave pública e Certificados digitais

### Componentes Utilizados

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

- Cisco 5508 WLC que executa a versão de firmware 8.3.102
- Pedido do OpenSSL para Microsoft Windows
- Ferramenta do registro que é específica ao Certification Authority (CA) da terceira

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# Certificados acorrentados

Um certificate chain é uma sequência dos Certificados, onde cada certificado na corrente é assinado pelo certificado subsequente. A finalidade de um certificate chain é estabelecer uma corrente da confiança de um certificado de peer a um certificado de CA confiado. O CA responde pela identidade no certificado de peer quando a assina. Se o CA é um que você confia, que está indicado pela presença de uma cópia do certificado de CA em seu diretório do certificado de raiz, este implica-o pode confiar o certificado de peer assinado também.

Frequentemente, os clientes não aceitam os Certificados porque não foram criados por um CA conhecido. O cliente indica tipicamente que a validez do certificado não pode ser verificada. Este é o caso quando o certificado é assinado por um CA intermediário, que não esteja sabido ao navegador cliente. Nesses casos, é necessário usar um certificado SSL ou um grupo acorrentado do certificado.

## Apoio para o certificado acorrentado

O controlador permite o certificado do dispositivo ser transferido como um certificado acorrentado para a autenticação da Web.

## Níveis do certificado

- Nível 0 - Uso somente de um certificado de servidor no WLC
- Nível 1 - Uso de um certificado de servidor no WLC e em um certificado de raiz CA
- Nível 2 - Uso de um certificado de servidor no WLC, em um único certificado intermediário CA, e em um certificado de raiz CA
- Nível 3 - Uso de um certificado de servidor no WLC, em dois Certificados intermediários CA, e em um certificado de raiz CA

O WLC não apoia Certificados acorrentados mais do que 10KB em tamanho no WLC. Contudo, esta limitação foi removida na versão 7.0.230.0 WLC e mais tarde.

> **Note**: Os Certificados acorrentados são apoiados para a autenticação da Web somente; não são apoiados para o certificado do Gerenciamento.

> **Note**: Os Certificados do convite são apoiados inteiramente para o EAP local, o Gerenciamento ou o webauthentication

Os Certificados da autenticação da Web podem ser qualquens um:

- Acorrentado

- Soltado
- Auto-gerado

**Note**: Na versão 7.6 e mais recente WLC, somente os Certificados acorrentados são apoiados no WLC para a autenticação da Web.

Se você está olhando para gerar um certificado soltado para o propósito do gerenciamento, você pode seguir este original e ignorar as peças onde o certificado é combinado com o certificado de CA.

Este original discute como instalar corretamente um certificado acorrentado do Secure Socket Layer (SSL) a um WLC.

# Etapa 1. Gerencia um CSR

Há duas maneiras de gerar um CSR. Manualmente com OpenSSL (a única maneira possível no software WLC pre-8.3) ou utilização do WLC próprio para gerar o CSR (disponível após 8.3.102).

## Opção A. CSR com OpenSSL

**Note**: A versão 58 e mais recente de Chrome não confia o Common Name do certificado apenas e exige o nome alternativo sujeito a também esta presente. A seguinte seção explicará como adicionar campos SAN ao OpenSSL CSR que é uma exigência nova para este navegador.

Termine estas etapas a fim gerar um CSR com OpenSSL:

1. Instale e abra o OpenSSL.

   Em Microsoft Windows, à revelia, openssl.exe é ficado situado em C:\ **> no OpenSSL > no escaninho.**

   **Note**: A versão 0.9.8 do OpenSSL é a versão recomendada para liberações velhas WLC; contudo, até à data da versão 7.5, o apoio para a versão 1.0 do OpenSSL igualmente foi adicionado (refira a identificação de bug Cisco CSCti65315 - apoio da necessidade para os Certificados gerados usando o v1.0 do OpenSSL) e é a versão recomendada a usar-se. O OpenSSL 1.1 trabalhos igualmente foi testado e trabalha grande em 8.x e em umas liberações mais atrasadas WLC.
2. Encontre seu arquivo da configuração do OpenSSL e faça uma cópia dela a fim editá-la para este CSR. Edite a cópia para adicionar as seguintes seções:
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
```

As linhas que começam com "DNS.1", "DNS.2" e assim por diante devem conter todos os nomes que alternativos seus Certificados terão. Você pode então escrever toda a URL que possível você se esteja usando para o WLC. As linhas em acima corajoso não estavam atuais nem foram comentadas em nossa versão do OpenSSL do laboratório, pode variar extremamente segundo o sistema operacional e a versão do OpenSSL. Nós salvar esta versão modificada da configuração como **openssl-san.cnf para** este exemplo.

4. Emita este comando a fim gerar um CSR novo:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
```

**Note**: Apoio de WLCs um tamanho chave máximo de 2,048 bit.

5. Depois que você emite o comando, há um alerta para alguma informação: nome do país, estado, cidade, e assim por diante. Forneça a informação requerida.

**Note**: É importante que você fornece o Common Name correto. Assegure-se de que o nome de host que é usado para criar o certificado (Common Name) combine a entrada de nome do host do Domain Name System (DNS) para o IP address da interface virtual no WLC e que o nome existe no DNS também. Também, depois que você faz a mudança à relação do IP virtual (VIP), você deve recarregar o sistema para que esta mudança tome o efeito. Aqui está um exemplo:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be 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 will be a default value,
If you enter '.', the field will be 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 []:Test@abc.com
```

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

6. Você pode verificar o CSR (especialmente para o SAN atribui a presença) com **req do OpenSSL - texto - noout - no csrfilename**
7. Depois que você fornece todos os detalhes exigidos, dois arquivos estão gerados:

   uma chave privada nova que inclua o nome **mykey.pem**um CSR que inclua o nome **myreq.pem**

## Opção B. CSR Generated pelo WLC

Se seu WLC executa a versão de software 8.3.102 ou mais atrasado, mais opção segura (e o mais fáceis demasiado) são usar o WLC para gerar o CSR. A vantagem é que a chave está gerada no WLC e nunca sae do WLC; assim é exposto nunca no mundo exterior.

A partir de agora, este método não reserva configurar o SAN no CSR que pôde conduzir às edições com determinados navegadores que exige a presença de um atributo SAN. Algum CA reserva introduzir campos SAN no tempo de assinatura, assim que é uma boa ideia verificar com seu CA.

Gerar o CSR pelo WLC próprio usará um tamanho chave de 2048 bit e o tamanho chave do ecdsa será os bit 256.

> **Note**: Se você executa o comando da geração csr e não instala o certificado resultante ainda, seu WLC será completamente inacessível em HTTPS na repartição seguinte, porque o WLC usará a chave recentemente gerada CSR depois que a repartição mas não tem o certificado que vai com ela.

A fim gerar um CSR para a autenticação da Web, incorpore este comando:

**O certificate generate CSR-webauth do** >config (WLC) **SEJA tac Cisco mywebauthportal.wireless.com tac@cisco.com de Bruxelas do BR**

```
-----COMECE O PEDIDO DO CERTIFICADO-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4w
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=
-----TERMINE O PEDIDO DO CERTIFICADO-----
```

A fim gerar um CSR para o webadmin, o comando muda mal:

**O certificate generate CSR-webadmin do** >config (WLC) **SEJA tac Cisco mywebauthportal.wireless.com tac@cisco.com de Bruxelas do BR**

> **Note**: O CSR está imprimido no terminal depois que você incorpora o comando. Não há nenhuma outra maneira de recuperá-lo; não é possível transferi-lo arquivos pela rede do WLC nem é possível salvar o. Você deve copiar/pasta ele a um arquivo em seu computador depois que você incorpora o comando. A chave gerada fica no WLC até que o CSR seguinte esteja gerado (a chave overwritten assim). Se você nunca tem que mudar o hardware WLC mais tarde (RMA), você não poderá reinstalar o mesmo certificado que uma chave e um CSR novos terão que ser gerados no WLC novo.

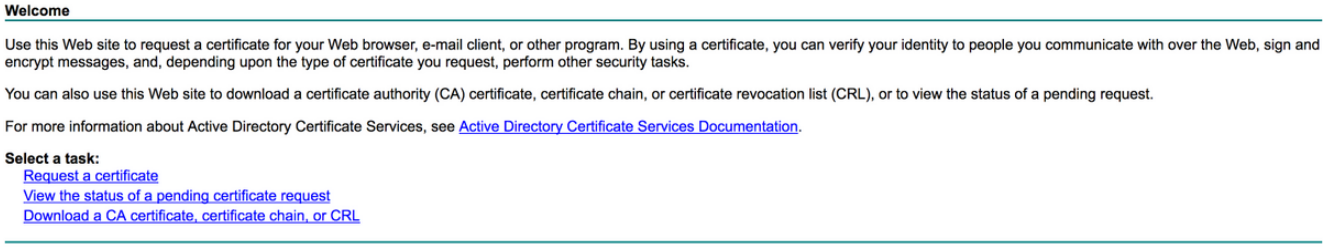
Você então tem que ceder este CSR a sua autoridade de assinatura da terceira ou a seu Public Key Infrastructure (PKI) da empresa.

# Etapa 2. Obtenha o certificado assinado

## Opção A: Obtenha o arquivo Final.pem de sua empresa CA

Este exemplo apresenta somente uma empresa existente CA (Windows Server 2012 neste exemplo) e não cobre as etapas para estabelecer a partir do zero Windows Server CA.

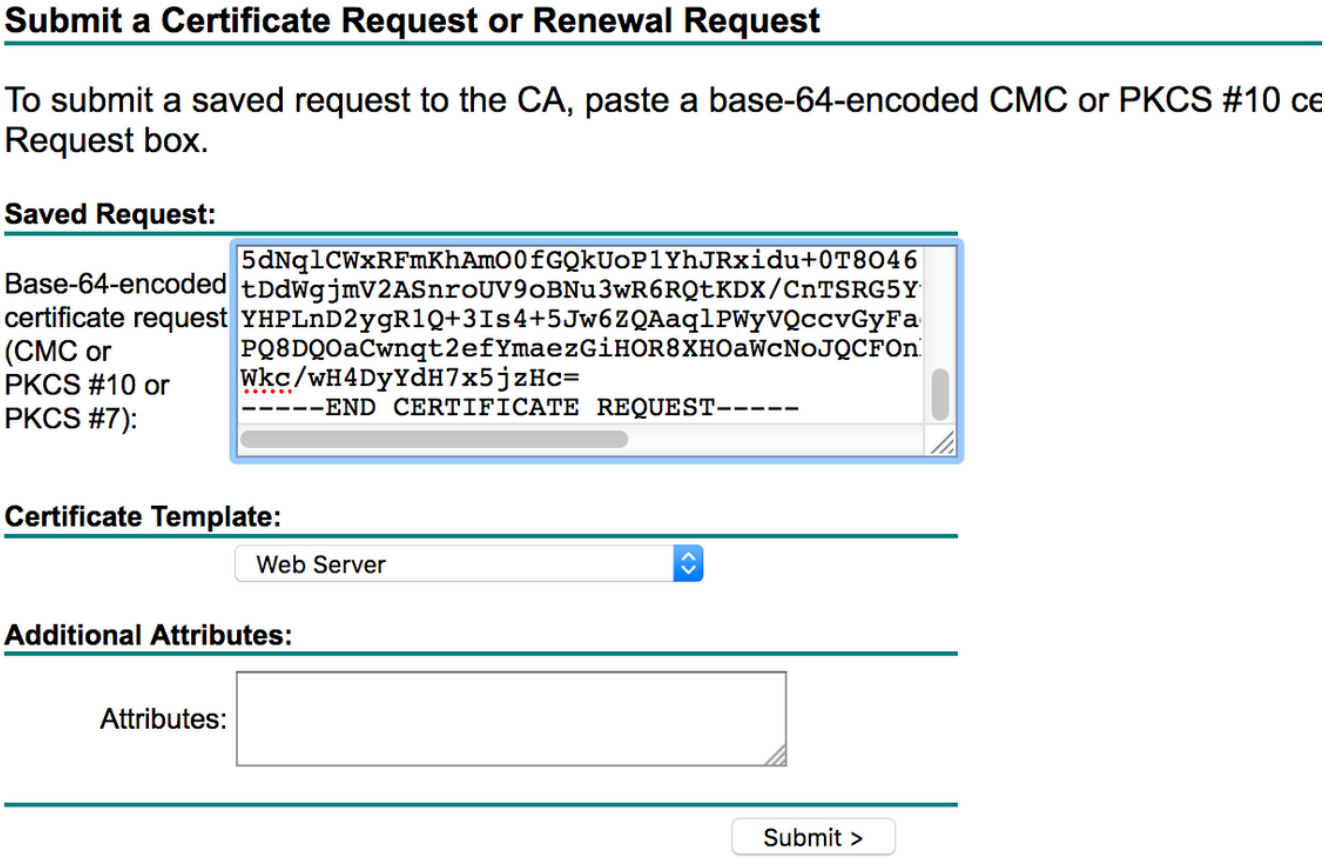
1. Vai a sua página do enteprrise CA no navegador (geralmente https:// <CA-ip>/certsrv) e clica o **pedido um certificado**.



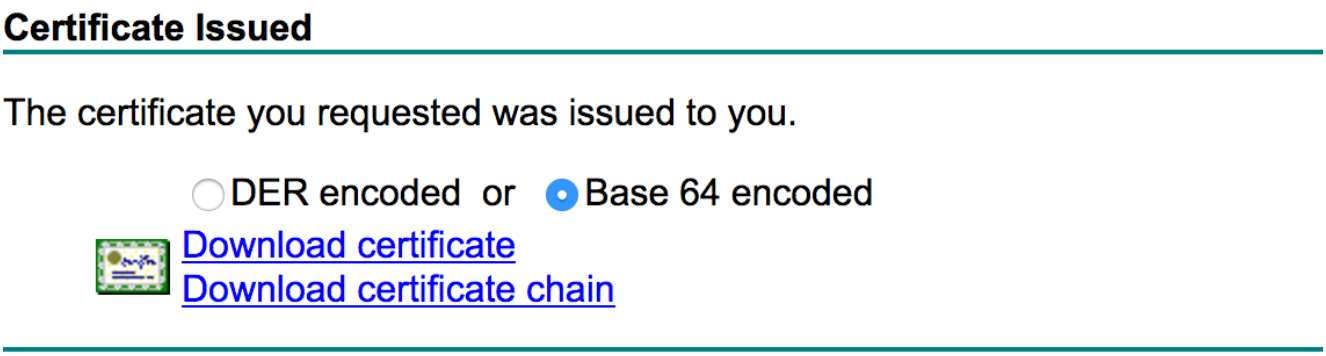

2. **Pedido do certificado avançado do** clique.


3. Incorpore o CSR que você obteve do WLC ou do OpenSSL. Na lista de drop-down do molde

de certificado, escolha o **servidor de Web**.




4. Clique o botão de rádio **codificado da base 64**.




5. Se o certificado transferido é do tipo PKCS7 (.p7b), a seguir você precisa de convertê-lo ao PEM (no exemplo abaixo nós transferimos o certificate chain como o nome de arquivo "All-certs.p7b"):

OpenSSL pkcs7 - print_certs - em All-certs.p7b - para fora All-certs.pem

6. Combine neste exemplo, é nomeado “All-certs.pem”) os Certificados do certificate chain (com a chave privada que você gerou junto com o CSR (a chave privada do certificado do dispositivo, que é mykey.pem neste exemplo) se você foi com opção A (isto é, você usou o OpenSSL para gerar o CSR), e salvar o arquivo como final.pem**. Se você** gerou o CSR diretamente do WLC (opção B) você pode saltar esta etapa.

Emita estes comandos no aplicativo do OpenSSL a fim criar os arquivos All-certs.pem e final.pem:

```
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
```

> **Note**: Neste comando, você deve incorporar uma senha para os parâmetros **- passin** e **- passout**. A senha que é configurada para **-** parâmetro do **passout** deve combinar o parâmetro do **certpassword** que é configurado no WLC. Neste exemplo, a senha que é configurada para **- passin** e **- os** parâmetros do **passout** são **check123**.

Final.pem é o arquivo que você deve transferir ao WLC se você seguiu a “opção A. CSR com OpenSSL”. Se você seguiu a “opção B. CSR gerada pelo WLC próprio”, a seguir All-certs.pem é o arquivo que você deve transferir ao WLC. A próxima etapa é transferir este arquivo ao WLC.

> **Note**: Se a transferência de arquivo pela rede do certificado ao WLC falha, pode-se ser que você não tenha a corrente inteira no arquivo PEM. Refira etapa 2 da opção B (obtenha o final.pem de uma 3ª parte CA) abaixo para ver como deve olhar como. Se você vê somente um certificado no arquivo, a seguir você necessidade de transferir manualmente todos os arquivos do intermediário e de certificado CA raiz e de adicioná-los (pela pasta da cópia simples) ao arquivo para criar a corrente.

## Opção B: Obtenha o arquivo Final.pem de um CA da terceira

1. A cópia e cola a informação CSR em toda a ferramenta do registro CA.

   Depois que você submete o CSR ao CA da terceira, o CA da terceira digitalmente assina o certificado e envia para trás a corrente de certificado assinado através do email. No caso dos Certificados acorrentados, você recebe a corrente inteira dos Certificados do CA. Se você tem somente um certificado intermediário como neste exemplo, você recebe estes três Certificados do CA:

   Raiz certificate.pemCertificate.pem intermediárioDispositivo certificate.pem**Note**: Certifique-se de que o certificado é Apache-compatível com criptografia do algoritmo de mistura segura 1 (SHA1).
2. Uma vez que você tem todos os três Certificados, copie e cole os índices de cada arquivo .pem em um outro arquivo nesta ordem:

   ```
   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
```

3. Salvar o arquivo como **All-certs.pem.**

4. Combine o certificado All-certs.pem com a chave privada que você gerou junto com o CSR (a chave privada do certificado do dispositivo, que é mykey.pem neste exemplo) se você foi com opção A (isto é, você usou o OpenSSL para gerar o CSR), e salvar o arquivo como final.pem**. Se você** gerou o CSR diretamente do WLC (opção B) você pode saltar esta etapa.

   Emita estes comandos no aplicativo do OpenSSL a fim criar os arquivos All-certs.pem e final.pem:

```
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
```

   **Note**: Neste comando, você deve incorporar uma senha para os parâmetros **- passin** e **- passout**. A senha que é configurada para **-** parâmetro do **passout** deve combinar o parâmetro do **certpassword** que é configurado no WLC. Neste exemplo, a senha que é configurada para **- passin** e **- os** parâmetros do **passout** são **check123**.Final.pem é o arquivo que você deve transferir ao WLC se você seguiu a “opção A. CSR com OpenSSL”. Se você seguiu a “opção B. CSR gerada pelo WLC próprio”, a seguir All-certs.pem é o arquivo que você deve transferir ao WLC. A próxima etapa é transferir este arquivo ao WLC.

   **Note**: SHA2 é apoiado igualmente. A identificação de bug Cisco CSCuf20725 é um pedido para o apoio SHA512.

# Etapa 3 CLI. Transfira o certificado da terceira ao WLC com o CLI

Termine estas etapas a fim transferir o certificado acorrentado ao WLC com o CLI:

1. Mova o **arquivo final.pem** para o diretório padrão em seu servidor TFTP.

2. No CLI, emita estes comandos a fim mudar os ajustes da transferência:

```
    >transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip <TFTP server IP address>
>transfer download path <absolute TFTP server path to the update file>
>transfer download filename final.pem
```

3. Incorpore a senha para o arquivo .pem de modo que o sistema operacional possa decifrar a chave e o certificado SSL.

```
>transfer download certpassword password
```

**Note**: Seja a certo que o valor para o **certpassword** é o mesmo que **-** senha do parâmetro do **passout** que foi ajustada na etapa 4 (ou 5) da geração uma seção CSR. Neste exemplo, o **certpassword** deve ser **check123**. Se você tinha escolhido a opção B (isto é, use o WLC próprio para gerar o CSR) que você pode deixar a placa do campo do certpassword.

4. Emita o **comando transfer download start** a fim ver os ajustes actualizados. Incorpore então **y no** alerta a fim confirmar os ajustes atuais da transferência e começar a transferência do certificado e da chave. Aqui está um exemplo:

```
(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 starting.

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

5. Recarregue o WLC para que as mudanças tomem o efeito.

# Etapa 3 GUI. Transfira o certificado da terceira ao WLC com o GUI

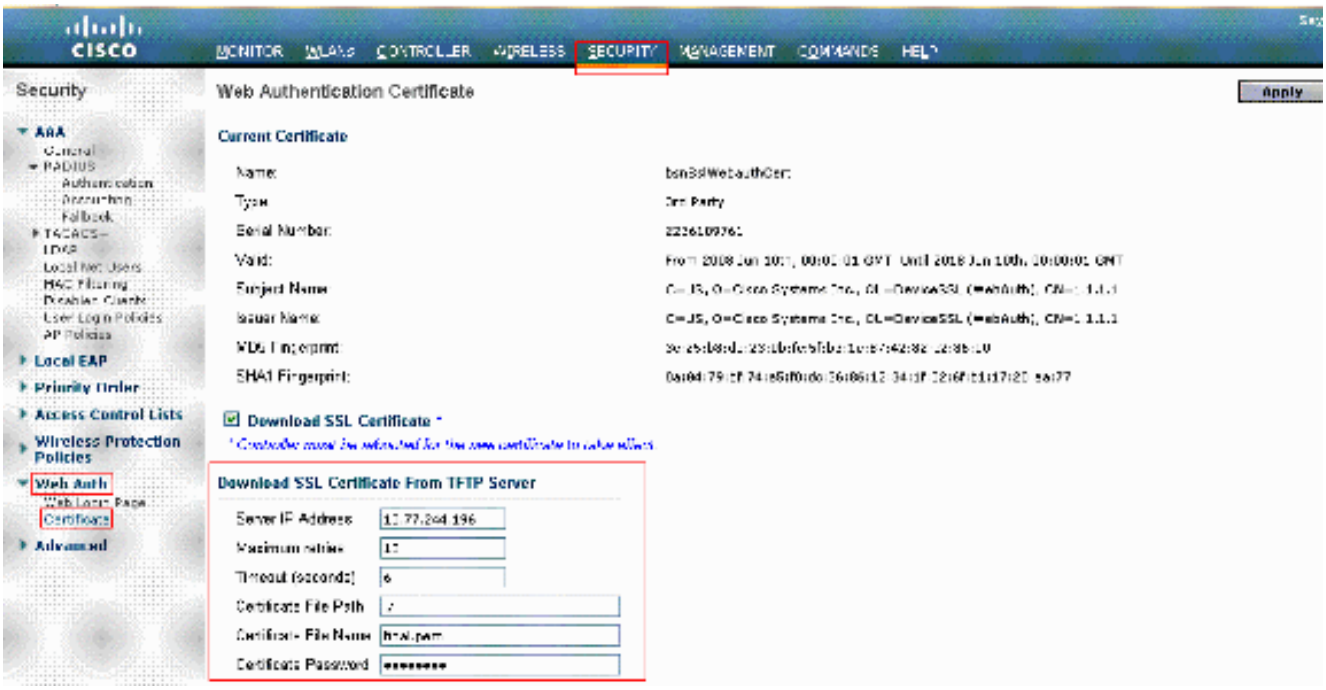
Termine estas etapas a fim transferir o certificado acorrentado ao WLC com o GUI:

1. Copie o certificado final.pem do dispositivo ao diretório padrão em seu servidor TFTP.

2. Escolha o **AUTH da Segurança > da Web > o CERT** a fim abrir a página do certificado da autenticação da Web.

3. Verifique a caixa de verificação do **certificado da transferência SSL** a fim ver o certificado da transferência SSL dos parâmetros do servidor TFTP.

4. No campo do IP address, incorpore o IP address do servidor TFTP.




5. No campo do caminho de arquivo, entre no caminho de diretório do certificado.

6. No campo de nome de arquivo, dê entrada com o nome do certificado.

7. No campo de senha do certificado, incorpore a senha que foi usada para proteger o certificado.

8. Clique em Apply.

9. Depois que a transferência está completa, escolha **comandos > repartição > repartição**.

10. Se alertado para salvar suas mudanças, clique a **salvaguarda e recarregue-a**.

11. Clique a **APROVAÇÃO** a fim confirmar sua decisão para recarregar o controlador.

# Troubleshooting

O que levantará muito provavelmente um problema é a instalação do certificado no WLC. A fim pesquisar defeitos, para abrir uma linha de comando no WLC e para entrá-la **debugar transferência que todos permitem** e **debugar o pki pm permitem** então completo o procedimento do certificado da transferência.

```
(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 starting.

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

Você precisa de verificar o formato do certificado e o encadeamento então. Recorde que WLCs mais tarde do que a versão 7.6 exige a corrente inteira a esta presente, assim que você não pode somente transferir arquivos pela rede seu certificado WLC apenas. A corrente até a obrigação da CA raiz esta presente no arquivo.

Está aqui um exemplo de debuga quando o CA intermediário está incorreto:

```
(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 starting.

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

# Informações Relacionadas

- Gerar CSR para certificados de terceiros e fazer o download de certificados desencadeados para o WLC
- Geração da solicitação de assinatura de certificado (CSR) para um certificado da terceira em um sistema de controle sem fio (WCS)
- Solicitação de assinatura de certificado sem fio do sistema de controle (WCS) (CSR) instalada em um exemplo de configuração do servidor Linux
- Suporte Técnico e Documentação - Cisco Systems