# Índice



# Introdução

Este documento 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 4400 WLC que executa a versão de firmware 5.1.151.0
- 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. CA responde pela identidade no certificado de peer quando a assina. Se 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 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 CA intermediário, que não está sabido ao navegador cliente. Nesses casos, é necessário usar um certificado SSL ou um grupo acorrentado do certificado.

## Apoio para o certificado acorrentado

Em versões do controlador mais cedo do que a versão 5.1.151.0, os Certificados da autenticação da Web podem ser somente Certificados do dispositivo e não devem conter as raizes de CA acorrentadas ao certificado do dispositivo (nenhuns Certificados acorrentados). Com versão 5.1.151.0 do controlador e mais tarde, 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 de CA
- Nível 2 - Uso de um certificado de servidor no WLC, em um único certificado intermediário de CA, e em um certificado de raiz de CA
- Nível 3 - Uso de um certificado de servidor no WLC, em dois Certificados intermediários de CA, e em um certificado de raiz de 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.

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

Os Certificados da autenticação da Web podem ser qualquens um:

- Acorrentado
- Soltado
- Gerado automaticamente

Para WLC com versões de software mais cedo do que a versão 5.1.151.0, a ação alternativa é usar uma destas opções:

- Adquira um certificado soltado de CA, assim que significa que a raiz de assinatura está

confiada.
- Tenha todos os certificados de raiz intermediários válidos de CA (confiados ou não-confiável) instalados no cliente.

Para obter informações sobre de como usar Certificados soltados no WLC, para consultar para gerar o CSR para Certificados da terceira e para transferir soltou Certificados ao WLC.

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

## Gerencia um CSR

Termine estas etapas a fim gerar um CSR:

1. Instale e abra o OpenSSL.

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

   Nota: A versão 0.9.8 do OpenSSL é a versão recomendada; contudo, até à data da versão 7.5, o apoio para a versão 1.0 do OpenSSL foi adicionado igualmente (refira a identificação de bug Cisco CSCti65315 - apoio da necessidade para os Certificados gerados usando o v1.0 do OpenSSL).

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

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

   Nota: Os WLC apoiam um tamanho chave máximo de 2,048 bit.

3. Às vezes quando você tenta gerar um CSR novo, você pôde receber o erro **incapaz de carregar a informação de configuração do erro de /usr/local/ssl/openssl.cnf no req**. Isto pode acontecer se o lugar do arquivo openssl.cfg (ou openssl.cnf) não está no dobrador do OpenSSL do padrão. A fim fixar esta edição, você tem que especificar o pathname inteiro ao arquivo openssl.cfg no comando gerar o CSR. Aqui está um exemplo:

   ```
   OpenSSL> req -config "C:\Open SSL1\OpenSSL\bin\openssl.cfg" -new -newkey rsa:
   1024 -nodes -keyout mykey.pem -out myreq.pem
   ```

   Este trajeto, < C:\Open SSL1\OpenSSL\bin\openssl.cfg >, do arquivo de configuração do OpenSSL pôde diferir baseado no local de arquivo.

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

   Nota: 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 de host do Domain Name System (DNS) para o endereço IP de Um ou Mais Servidores Cisco ICM NT 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
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>
```

5. 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**

## Obtenha o arquivo Final.pem

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

   Depois que você submete o CSR a CA da terceira, 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 de CA. Se você tem somente um certificado intermediário como dentro dentro este exemplo, você recebe estes três Certificados de CA:

   Raiz certificate.pemCertificate.pem intermediárioDispositivo certificate.pem

   Nota: 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 do .pem em um outro arquivo nesta ordem:

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

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), e salvar o arquivo como final.pem**.**

   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
   ```

   Nota: 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. A próxima etapa é transferir este arquivo ao WLC.

## 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 do .pem de modo que o sistema operacional possa decifrar a chave e o certificado SSL.

   ```
   >transfer download certpassword password
   ```

Nota: Seja a certo que o valor para o **certpassword** é o mesmo que **-** senha do parâmetro do **passout** que foi ajustada em etapa 4 da geração uma seção CSR. Neste exemplo, o **certpassword** deve ser **check123**.

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 may 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.

## Transfira o certificado da terceira ao WLC com o GUI

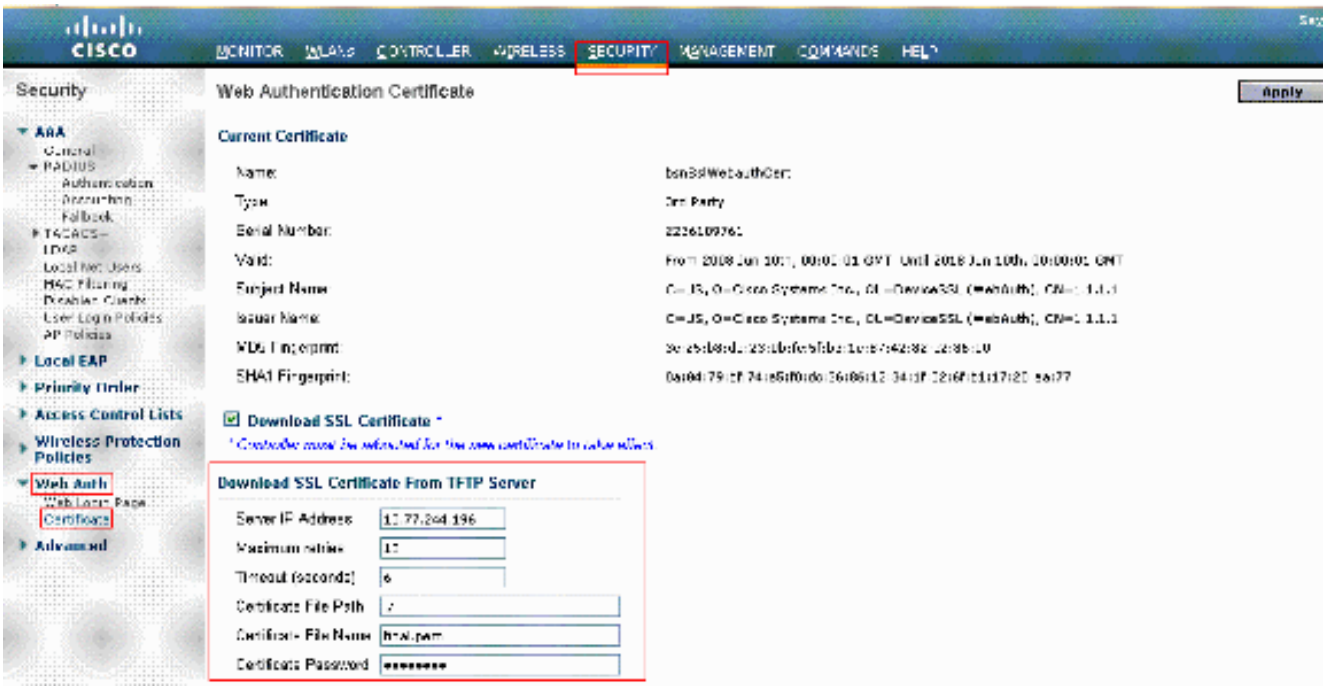
Termine estas etapas a fim transferir o certificado acorrentado ao WLC com o GUI:

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 endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT 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.

## 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 wireless (WCS)
- Solicitação de assinatura de certificado wireless do sistema de controle (WCS) (CSR) instalada em um exemplo de configuração do servidor Linux
- Suporte Técnico e Documentação - Cisco Systems