Gerar o CSR para certificados de terceiros e baixar certificados em cadeia para o WLC

Contents

Introdução

Este documento descreve como gerar e importar certificados em AireOS WLCs.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o WLC, o Lightweight Access Point (LAP) e a placa de cliente sem fio para a operação básica.
- Como usar a aplicação de 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 com o firmware versão 8.3.102
- Aplicação de OpenSSL para Microsoft Windows
- Ferramenta de inscrição específica para a autoridade de certificado (CA) de terceiros

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Certificados em cadeia

Uma cadeia de certificados é uma sequência de certificados em que cada certificado da cadeia é assinado pelo certificado subsequente.

A finalidade de uma cadeia de certificados é estabelecer uma cadeia de confiança de um certificado de mesmo nível para um certificado de CA confiável. A CA confirma a identidade no certificado de mesmo nível quando ele é assinado.

Se a CA for confiável (indicada pela presença de uma cópia do certificado CA em seu diretório de certificado raiz), isso significa que você também pode confiar no certificado de mesmo nível assinado.

Geralmente, os clientes não aceitam os certificados porque não foram criados por uma CA conhecida. Normalmente, o cliente afirma que não é possível verificar a validade do certificado.

Esse é o caso quando o certificado é assinado por uma CA intermediária, que não é conhecida pelo navegador do cliente. Nesses casos, é necessário usar um certificado SSL em cadeia ou um grupo de certificados.

Suporte para certificado em cadeia

O controlador permite que o certificado do dispositivo seja baixado como certificado em cadeia para autenticação na Web.

Níveis de certificado

- Nível 0 â€“ Uso de apenas um certificado de servidor no WLC
- Nível 1 â€“ Uso de um certificado de servidor no WLC e um certificado de origem de CA
- Nível 2 â€“ Uso de um certificado de servidor no WLC, um único certificado intermediário de CA e um certificado de origem de CA
- Nível 3 â€“ Uso de um certificado de servidor no WLC, dois certificados intermediários de CA e um certificado de origem de CA

O WLC não permite certificados em cadeia com mais de 10 KB no WLC. No entanto, essa restrição foi removida no WLC versão 7.0.230.0 e posteriores.

Observação: os certificados em cadeia são suportados e realmente necessários para a autenticação da Web e a administração da Web

---

Observação: certificados curinga são totalmente suportados para EAP local, gerenciamento ou autenticação da Web

---

Os certificados de autenticação na Web podem ser:

- Em cadeia
- Sem cadeia
- Gerado automaticamente

> **Observação**: na versão 7.6 e posterior da WLC, somente certificados encadeados são suportados (e, portanto, necessários)

Para gerar um certificado não encadeado para fins de gerenciamento, use este documento e desconsidere as partes em que o certificado é combinado com o certificado CA.

Este documento discute como instalar corretamente um certificado SSL (Secure Socket Layer) em cadeia em um WLC.

Etapa 1. Gerar um CSR

Há duas maneiras de gerar um CSR. Seja manualmente com o OpenSSL (a única maneira possível no software WLC pré-8.3) ou vá na própria WLC para gerar o CSR (disponível após 8.3.102).

Opção A. CSR com OpenSSL

> **Observação**: o Chrome versão 58 e posterior não confia apenas no nome comum do certificado e exige que o nome alternativo do assunto também esteja presente. A próxima seção explica como adicionar campos SAN ao OpenSSL CSR, que é um novo requisito para este navegador.

Siga estas etapas para gerar um CSR com OpenSSL:

1. Instale e abra o OpenSSL.

   No Microsoft Windows, por padrão, o openssl.exe está localizado em **C:\ > openssl > bin.**

   > **Observação**: o OpenSSL Versão 0.9.8 é a versão recomendada para versões antigas do WLC; no entanto, a partir da Versão 7.5, o suporte para o OpenSSL Versão 1.0 também foi adicionado (consulte o bug da Cisco ID CSCti65315 - Need Support for certificates generate with OpenSSL v1.0) e é a versão recomendada para usar. O OpenSSL 1.1 também foi testado e funciona em versões 8.x e posteriores do WLC.

2. Localize o arquivo de configuração do OpenSSL e faça uma cópia para ser editada neste CSR. Edite a cópia para adicionar as próximas seções:
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
```

As linhas que começam com "DNS.1", "DNS.2" (e assim por diante) devem conter todos os nomes alternativos de seus certificados. Em seguida, escreva qualquer URL possível utilizado para a WLC. As linhas em negrito no exemplo anterior não estavam presentes ou foram comentadas em nossa versão openSSL do laboratório. Pode variar muito com o sistema operacional e a versão do openssl. Salvamos esta versão modificada da configuração como **openssl-san.cnf** neste exemplo.

4. Insira este comando para gerar um novo CSR:

<#root>

OpenSSL>

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

---

Observação: as WLCs suportam um tamanho de chave máximo de 4096 bits a partir da versão de software 8.5

---

5. Há um prompt para algumas informações: nome do país, estado, cidade, etc. Forneça as informações necessárias.

Observação: é importante fornecer o nome comum correto. Verifique se o nome do host usado para criar o certificado (nome comum) corresponde à entrada de nome do host do DNS (Domain Name System) para o endereço IP da interface virtual no WLC e se o nome também existe no DNS. Além disso, depois de fazer a alteração na interface IP virtual (VIP), você deve reiniciar o sistema para que essa alteração entre em vigor.

Aqui está um exemplo:

<#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. Você pode verificar o CSR (especialmente para a presença de atributos de SAN) com **openssl req -text -noout -in csrfilename**
7. Depois de fornecer todos os detalhes necessários, dois arquivos são gerados:

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

Opção B. CSR gerado pelo WLC

Se sua WLC executar a versão 8.3.102 ou posterior do software, a opção mais segura é usar a WLC para gerar o CSR. A vantagem é que a chave é gerada na WLC e nunca deixa a WLC; portanto, nunca é exposta no mundo exterior.

A partir de agora, esse método não permite configurar a SAN no CSR, que já foi conhecido por causar problemas com determinados navegadores, o que requer a presença de um atributo SAN. Algumas autoridades de certificação permitem inserir campos de SAN no momento da assinatura, portanto, é recomendável verificar com sua autoridade de certificação.

A geração de CSR pelo próprio WLC usa um tamanho de chave de 2048 bits e o tamanho de chave ecdsa é de 256 bits.

> **Observação**: se você executar o comando csr generation e ainda não instalar o certificado subsequente, sua WLC será considerada completamente inacessível no HTTPS na próxima reinicialização, pois a WLC usará a chave CSR recém-gerada após a reinicialização, mas não terá o certificado que a acompanha.

Para gerar um CSR para autenticação na Web, insira este comando:

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQlIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
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-----

Para gerar um CSR para o webadmin, o comando é alterado para:

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

---

Observação: o CSR é impresso no terminal depois que você digita o comando. Não há outras maneiras de recuperá-lo; não é possível carregá-lo da WLC nem salvá-lo. Você deve copiar/colar em um arquivo no computador após inserir o comando. A chave gerada permanece no WLC até que o próximo CSR seja gerado (a chave será substituída). Se você tiver que alterar o hardware da WLC posteriormente (RMA), não será possível reinstalar o mesmo certificado como uma nova chave e o CSR será gerado na nova WLC.

---

para

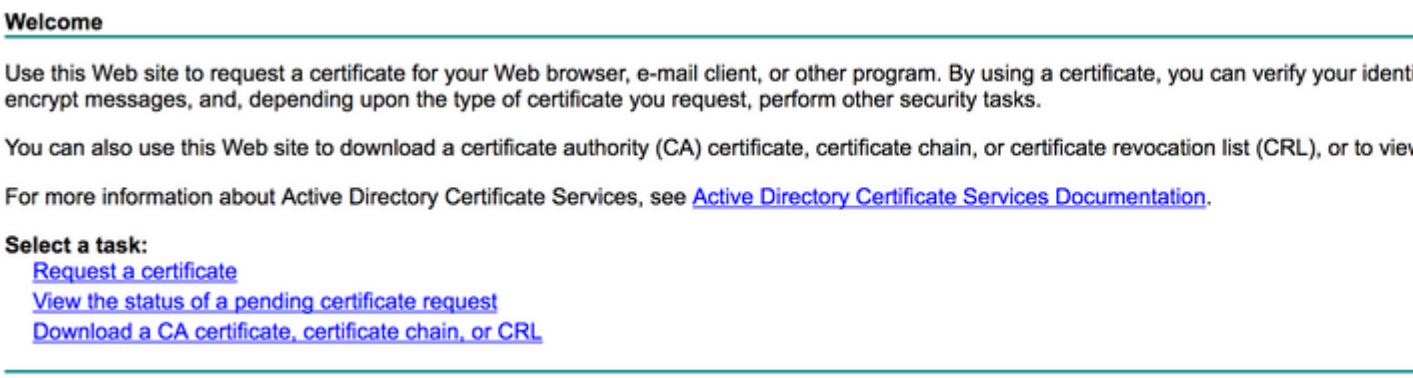
Você precisará entregar esse CSR à autoridade de assinatura de terceiros ou à infraestrutura de chave pública (PKI) corporativa.

Etapa 2. Obtenha o certificado assinado

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

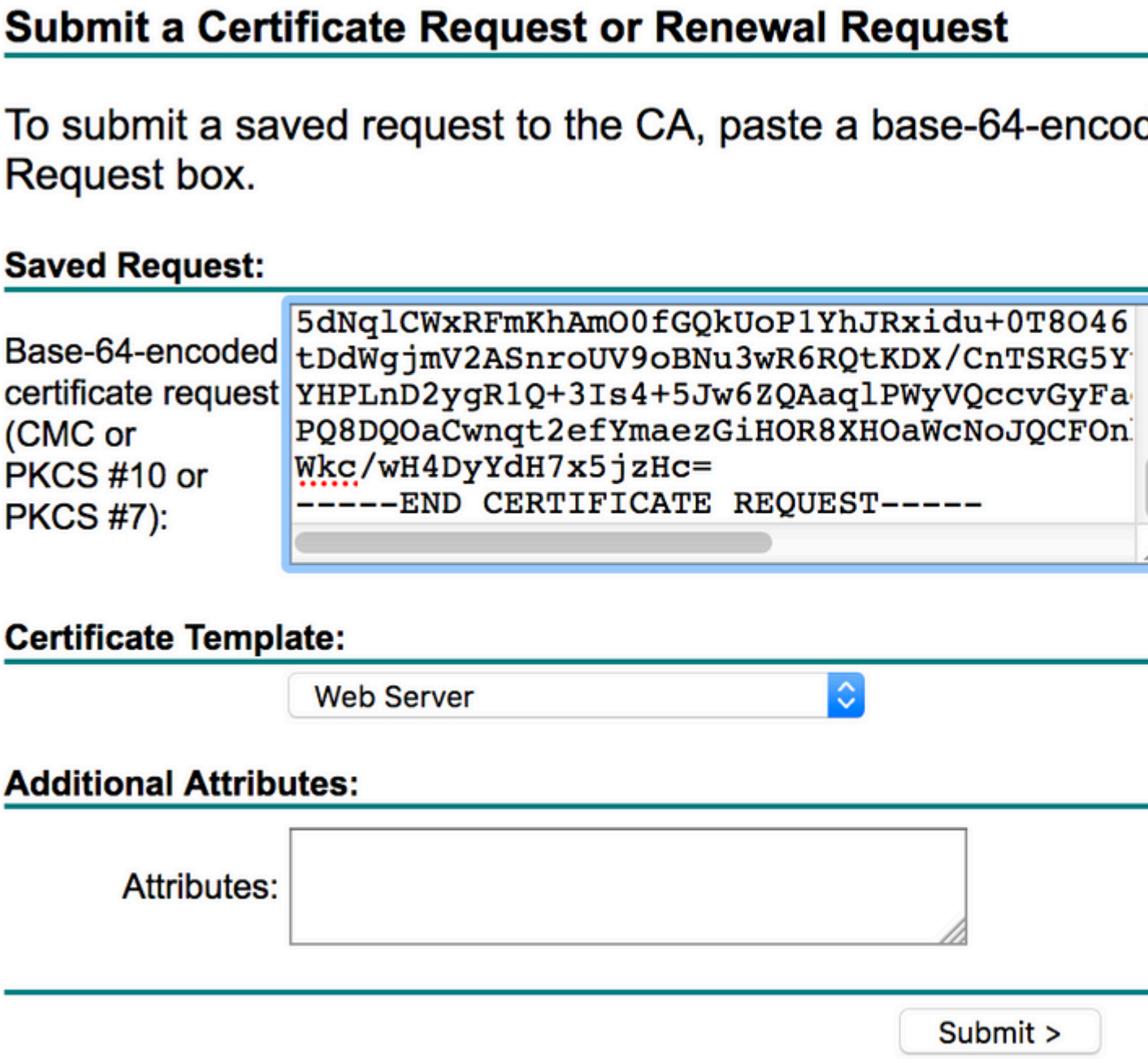
Este exemplo mostra apenas uma CA corporativa atual (Windows Server 2012 neste exemplo) e não abrange as etapas para configurar uma CA do Windows Server desde o início.

1. Acesse a página da autoridade de certificação corporativa no navegador (geralmente https://<CA-ip>/certsrv) e clique em **Request a certificate.**

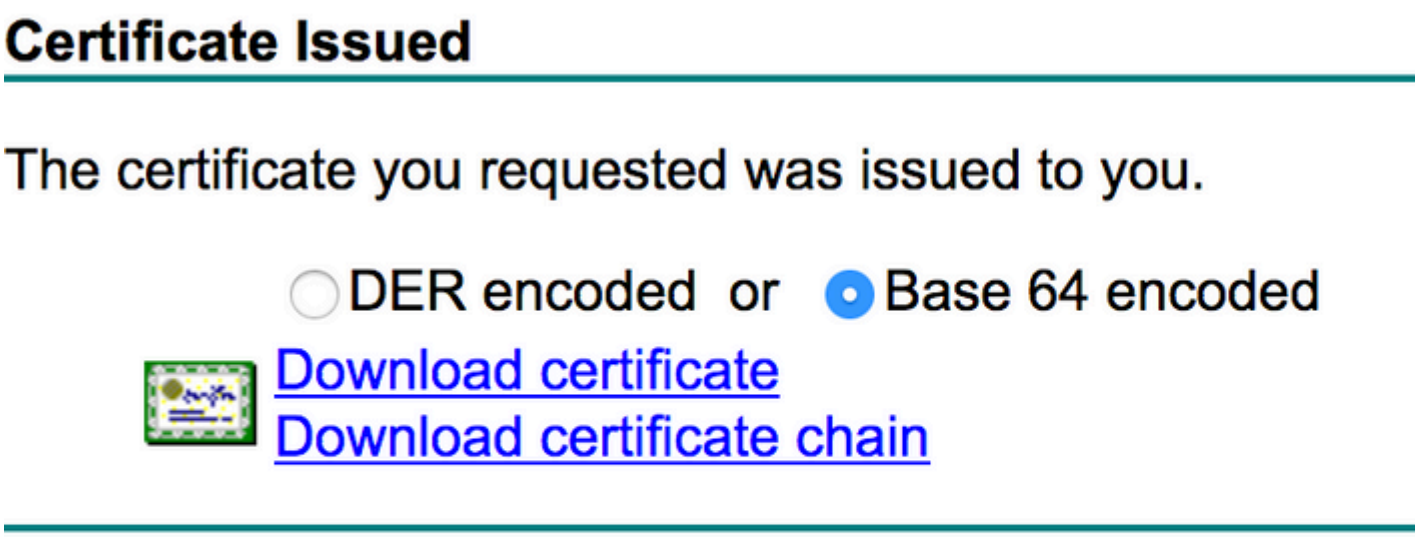


2. Clique em **advanced certificate request.**

3. Insira o CSR obtido no WLC ou no OpenSSL. Na lista suspensa Modelo de certificado, escolha **Web Server**.



4. Clique no botão **Base 64 encoded**botão de opção.



5. Se o certificado baixado for do tipo PKCS7 (.p7b), converta-o para PEM (no próximo exemplo, a cadeia de certificados foi baixada como o nome de arquivo "All-certs.p7b") :

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

6. Combine a cadeia de certificados (neste exemplo, ela é denominada "All-certs.pem") com a chave privada que foi gerada junto com o CSR (a chave privada do certificado do dispositivo, que é mykey.pem neste exemplo) se você tiver optado pela opção A (OpenSSL para gerar o CSR) e salve o arquivo como **final.pem**. Se você gerou o CSR diretamente do WLC (opção B), ignore esta etapa.

Insira estes comandos no aplicativo OpenSSL para criar os arquivos 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
```

Observação: nesse comando, você deve inserir uma senha para os parâmetros **-passin** e **-passout**. A senha configurada para o parâmetro **-passout** deve corresponder ao parâmetro **certpassword** configurado no WLC. Neste exemplo, a senha configurada para os parâmetros **-passin** e **-passout** é **check123**.

Final.pem é o arquivo a ser baixado para a WLC se você tiver seguido a "Opção A. CSR com OpenSSL".

Se você seguiu a "Opção B. CSR gerada pela própria WLC", então All-certs.pem é o arquivo para download para a WLC. A próxima etapa é baixar esse arquivo no WLC.

Observação: se o upload do certificado para a WLC falhar, verifique se há toda a cadeia no arquivo pem. Consulte a etapa 2 da opção B (obtenha o final.pem de uma CA de terceiros) para ver como ele deve ser. Se você vir apenas um certificado no arquivo, precisará baixar manualmente todos os arquivos de certificado intermediário e de origem da CA e anexá-los (basta copiar e colar) ao arquivo para criar a cadeia.

Opção B: Obtenha o arquivo Final.pem de uma CA de terceiros

1. Copie e cole as informações do CSR em qualquer ferramenta de inscrição da CA.

   Depois que você envia o CSR para a CA de terceiros, a CA de terceiros assina digitalmente o certificado e devolve a cadeia de certificados assinados por e-mail. No caso de certificados em cadeia, você recebe toda a cadeia de certificados da CA. Se você tiver apenas um certificado intermediário, como neste exemplo, receberá estes três certificados da CA:

   - certificate.pem de origem
   - certificate.pem intermediário
   - certificate.pem do dispositivo

   Observação: certifique-se de que o certificado seja compatível com o Apache com a criptografia Secure Hash Algorithm 1 (SHA1).

2. Quando tiver todos os três certificados, copie e cole o conteúdo de cada arquivo .pem em 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. Salve o arquivo como **All-certs.pem**.

4. Combine o certificado All-certs.pem com a chave privada que foi gerada junto com o CSR (a chave privada do certificado do dispositivo, que é mykey.pem neste exemplo) se você usou a opção A

(OpenSSL para gerar o CSR) e salve o arquivo como **final.pem**. Se você gerou o CSR diretamente do WLC (opção B), ignore esta etapa.

Insira estes comandos no aplicativo OpenSSL para criar os arquivos 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
```

Observação: nesse comando, você deve inserir uma senha para os parâmetros **-passin** e **-passout**. A senha configurada para o parâmetro **-passout** deve corresponder ao parâmetro **certpassword** configurado no WLC. Neste exemplo, a senha configurada para os parâmetros **-passin** e **-passout** é **check123**.

Final.pem é o arquivo a ser baixado para a WLC se você tiver seguido a "Opção A. CSR com OpenSSL". Se você seguiu a "Opção B. CSR gerada pela própria WLC", então All-certs.pem é o arquivo que você deve baixar para a WLC. A próxima etapa é baixar esse arquivo no WLC.

Observação: SHA2 também é suportado. A ID de bug da Cisco CSCuf20725 é uma solicitação de suporte ao SHA512.

Etapa 3 CLI. Baixe o certificado de terceiros no WLC com a CLI

Conclua estes passos para fazer o download do certificado encadeado para o WLC com o CLI:

1. Mova o arquivo **final.pem** para o diretório padrão no servidor TFTP.
2. Na CLI, insira estes comandos para alterar as configurações de download:

```
<#root>

    >

transfer download mode tftp


    >

transfer download datatype webauthcert
```

```
    >
transfer download serverip
```

```
    >
transfer download path
```

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

3. Insira a senha do arquivo.pem para que o sistema operacional possa descriptografar a chave SSL e o certificado.

```
<#root>

>

transfer download certpassword password
```

Observação: certifique-se de que o valor de **certpassword seja o mesmo que o parâmetro de senha de -passout** que foi definido na Etapa 4 (ou 5) da seção **Gerar um CSR**. Neste exemplo, o **certpassword** deve ser **check123**. Se você tiver escolhido a opção B (ou seja, use a própria WLC para gerar o CSR), deixe o campo certpassword em branco.

---

4. Digite o **transfer download start** para exibir as configurações atualizadas. Em seguida, insira **y** no prompt para confirmar as configurações de download atuais e iniciar o download do certificado e da chave. Aqui está um exemplo:

```
<#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
```

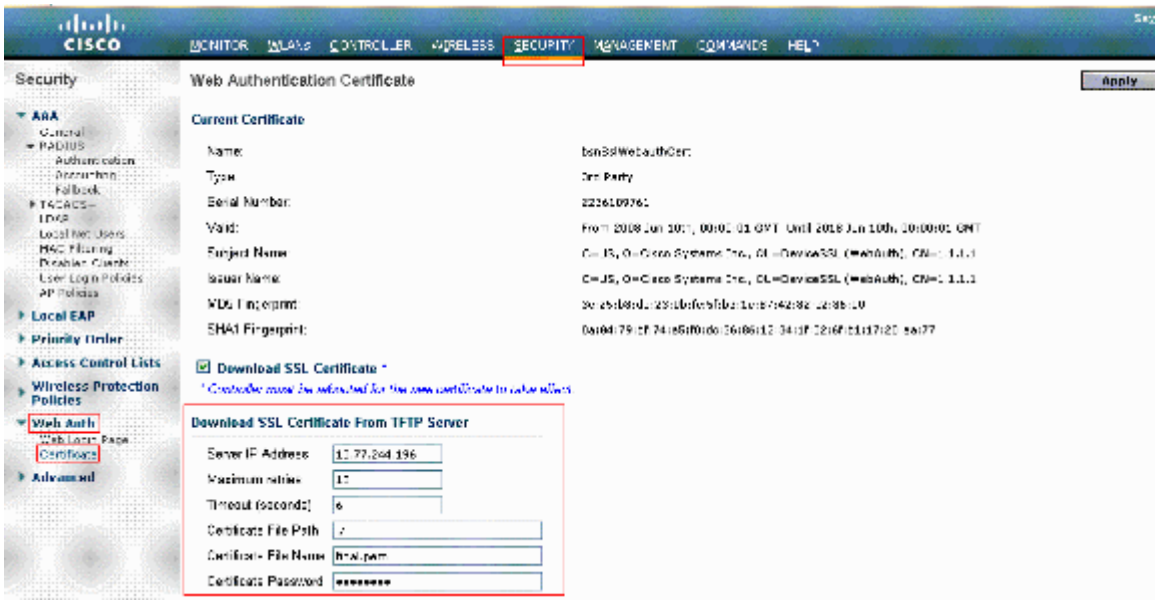
```
TFTP Path......................................./
TFTP Filename.................................. final.pem

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. Reinicie o WLC para que as alterações entrem em vigor.

Etapa 3 GUI. Baixe o certificado de terceiros no WLC com a GUI

Conclua estas etapas para fazer o download do certificado encadeado para o WLC com a GUI:

1. Copie o final.pem do certificado do dispositivo para o diretório padrão no servidor TFTP.
2. Escolher **Security** > **Web Auth** > **Cert** para abrir a página Certificado de autenticação da Web.
3. Marque a caixa **Download SSL Certificate**para exibir os parâmetros de Download SSL Certificate From TFTP Server.
4. No campo Endereço IP, insira o endereço IP do servidor TFTP.



5. No campo Caminho do arquivo, insira o caminho do diretório do certificado.

6. No campo Nome do arquivo, insira o nome do certificado.
7. No campo Senha do certificado, insira a senha usada para proteger o certificado.
8. Clique em **Apply**.
9. Após a conclusão do download, selecione **Commands > Reboot > Reboot.**
10. Se for solicitado salvar as alterações, clique em **Save and Reboot.**
11. Clique em **OK** para confirmar a decisão de reiniciar o controlador.

Troubleshooting

Para fazer o troubleshooting da instalação do certificado na WLC, abra uma linha de comando na WLC e insira **debug transfer all enable** e **debug pm pki enable** em seguida, conclua o procedimento de download de certificado.

```
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.
```

Verifique o formato e a cadeia do certificado. Lembre-se de que as WLCs posteriores à versão 7.6 exigem que toda a cadeia esteja presente, de modo que você não pode carregar seu certificado de WLC sozinho. A cadeia até a CA de origem deve estar presente no arquivo.

Este é um exemplo de depuração quando a CA intermediária está incorreta:

```
*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
```

Considerações sobre alta disponibilidade (HA SSO)

Como explicado no guia de implantação de SSO de alta disponibilidade do WLC, os certificados não são replicados do controlador primário para o secundário em um cenário de SSO de alta disponibilidade.

Isso significa que você precisa importar todos os certificados para o secundário antes de formar o par HA.

Outra advertência é que isso não funcionará se você tiver gerado o CSR (e, portanto, criado a chave localmente) na WLC primária porque essa chave não pode ser exportada.

A única maneira é gerar o CSR para o WLC primário com OpenSSL (e, portanto, ter a chave anexada ao certificado) e importar essa combinação de certificado/chave em ambos os WLCs.

Informações Relacionadas

- **Gerar CSR para certificados de terceiros e fazer o download de certificados desencadeados para o WLC**
- **Geração de solicitação de assinatura de certificado (CSR) para um certificado de terceiros em um Wireless Control System (WCS)**
- **Solicitação de assinatura de certificado (CSR) do Wireless Control System (WCS) instalada em um exemplo de configuração do servidor Linux**
- **Suporte Técnico e Documentação - Cisco Systems**
- **Guia de SSO de alta disponibilidade do WLC**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.