Gerar e fazer download de certificados CSR em WLCs Catalyst 9800

Contents

Introduction

Este documento descreve como gerar uma solicitação de assinatura de certificado (CSR) para obter um certificado de terceiros. Em seguida, como fazer o download de um certificado encadeado para um Catalyst 9800 Wireless LAN Controller (9800 WLC) e usar para webauth e portal webadmin.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar a WLC 9800, o ponto de acesso (AP) para operação básica
- Como usar a aplicação de OpenSSL
- Infraestrutura de Chave Pública (PKI) e certificados digitais

Componentes Utilizados

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

- 9800-L, Cisco IOS® XE versão 17.3.3
- aplicativo OpenSSL

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Em 16.10.X, os 9800s não oferecem suporte a um certificado diferente para autenticação e administração da Web. O portal de login na Web sempre usa o certificado padrão.

Em 16.11.X, você pode configurar um certificado dedicado para autenticação da Web, definir o ponto de confiança dentro do mapa de parâmetros global.

Há duas opções para obter um certificado para uma WLC 9800.

1. Gere CSR (Certificate Signing Request, Solicitação de assinatura de certificado) com OpenSSL ou qualquer outro aplicativo SSL. Obtenha um certificado PKCS12 assinado por sua Autoridade de Certificação (CA) e carregue-o diretamente na WLC 9800. Isso significa que a chave privada é agrupada com esse certificado.
2. Use a CLI da WLC 9800 para gerar uma CSR, assine-o por uma CA e carregue cada certificado na cadeia manualmente na WLC 9800.

Use o que melhor se adapta às suas necessidades.

Opção 1 - Carregar um certificado PKCS12 pré-existente assinado

Definir uma solicitação de assinatura

Se ainda não tiver o certificado, você precisará gerar uma solicitação de assinatura para fornecer à sua CA.

Edite o arquivo **openssl.cnf** do diretório atual (em um laptop com OpenSSL instalado), copie e cole essas linhas para incluir o campo Nomes alternativos do assunto (SAN) nos CSRs recém-criados.

```
[ req ]
default_bits       = 4096
distinguished_name = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
stateOrProvinceName         = State or Province Name (full name)
localityName                = Locality Name (eg, city)
organizationName            = Organization Name (eg, company)
commonName                  = Common Name (e.g. server FQDN or YOUR name)
[ req_ext ]
```

```
subjectAltName = @alt_names
[alt_names]
DNS.1   = testdomain.com
DNS.2   = example.com
DNS.3   = webadmin.com
```

Substitua os nomes DNS.X por sua SAN. Substitua os campos principais pelos detalhes de certificado necessários. Certifique-se de repetir o nome comum dentro dos campos SAN (DNS.x). O Google Chrome requer que o nome presente no URL esteja nos campos SAN para confiar no certificado.

No caso do administrador da Web, você também precisa preencher os campos de SAN com variações da URL (apenas nome do host ou Nome de domínio totalmente qualificado (FQDN) completo, por exemplo) para que o certificado corresponda independentemente dos tipos de administrador na URL na barra de endereços do navegador.

Gere o CSR do OpenSSL com este comando:

```
openssl req -out myCSR.csr -newkey rsa:4096 -nodes -keyout private.key -config openssl.cnf
```

O CSR gera como **myCSR.csr** e sua chave como **private.key** no diretório de onde o OpenSSL é executado, a menos que o caminho completo seja fornecido para o comando.

Certifique-se de manter o arquivo **private.key** seguro, pois ele é usado para criptografar comunicações.

Você pode verificar seu conteúdo com:

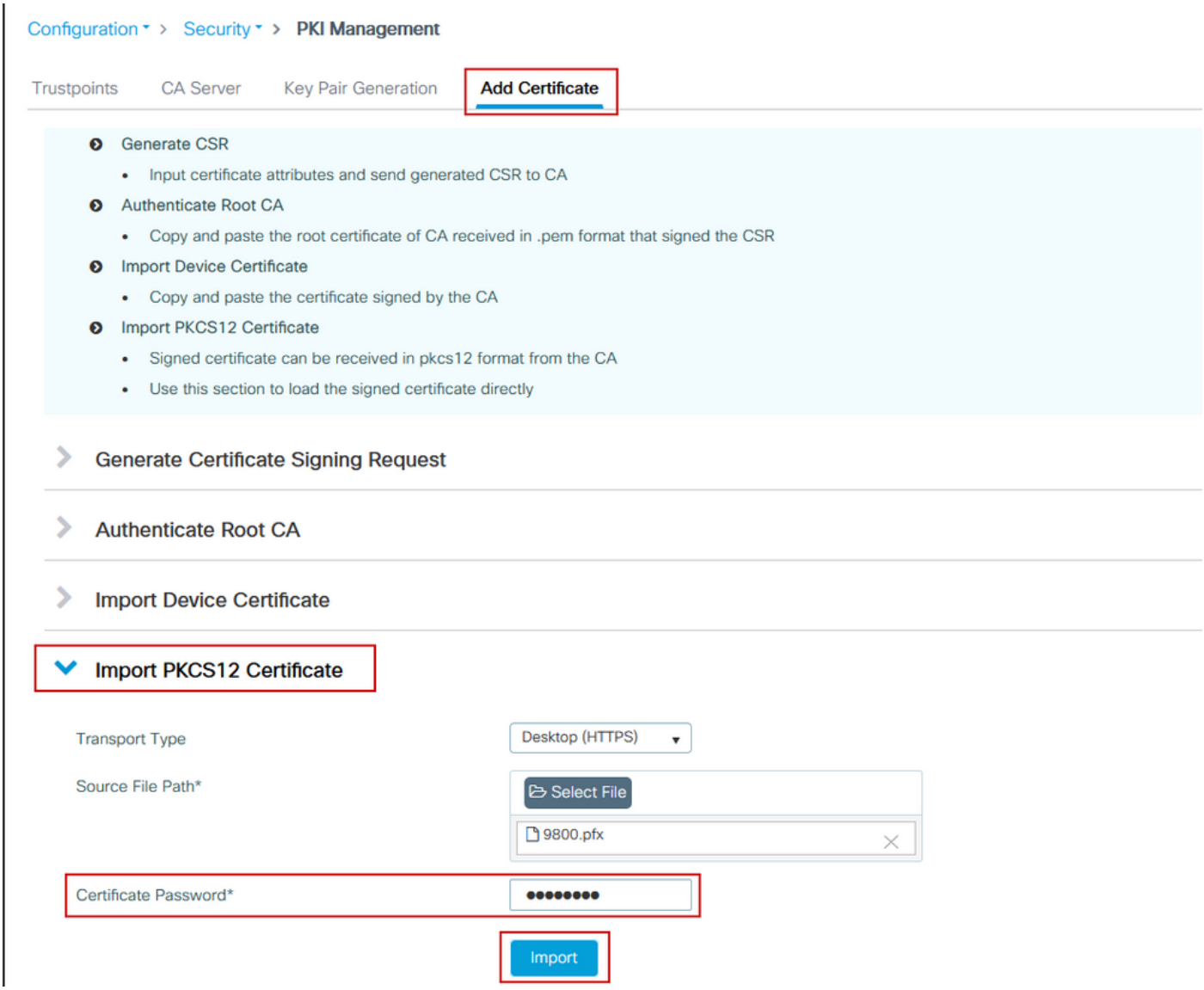
```
openssl req -noout -text -in myCSR.csr
```

Você pode fornecer esse CSR à sua CA para que ela seja assinada e receba um certificado de volta. Verifique se a cadeia completa foi baixada da CA e se o certificado está no formato Base64, caso precise de manipulação adicional.

Importar o certificado

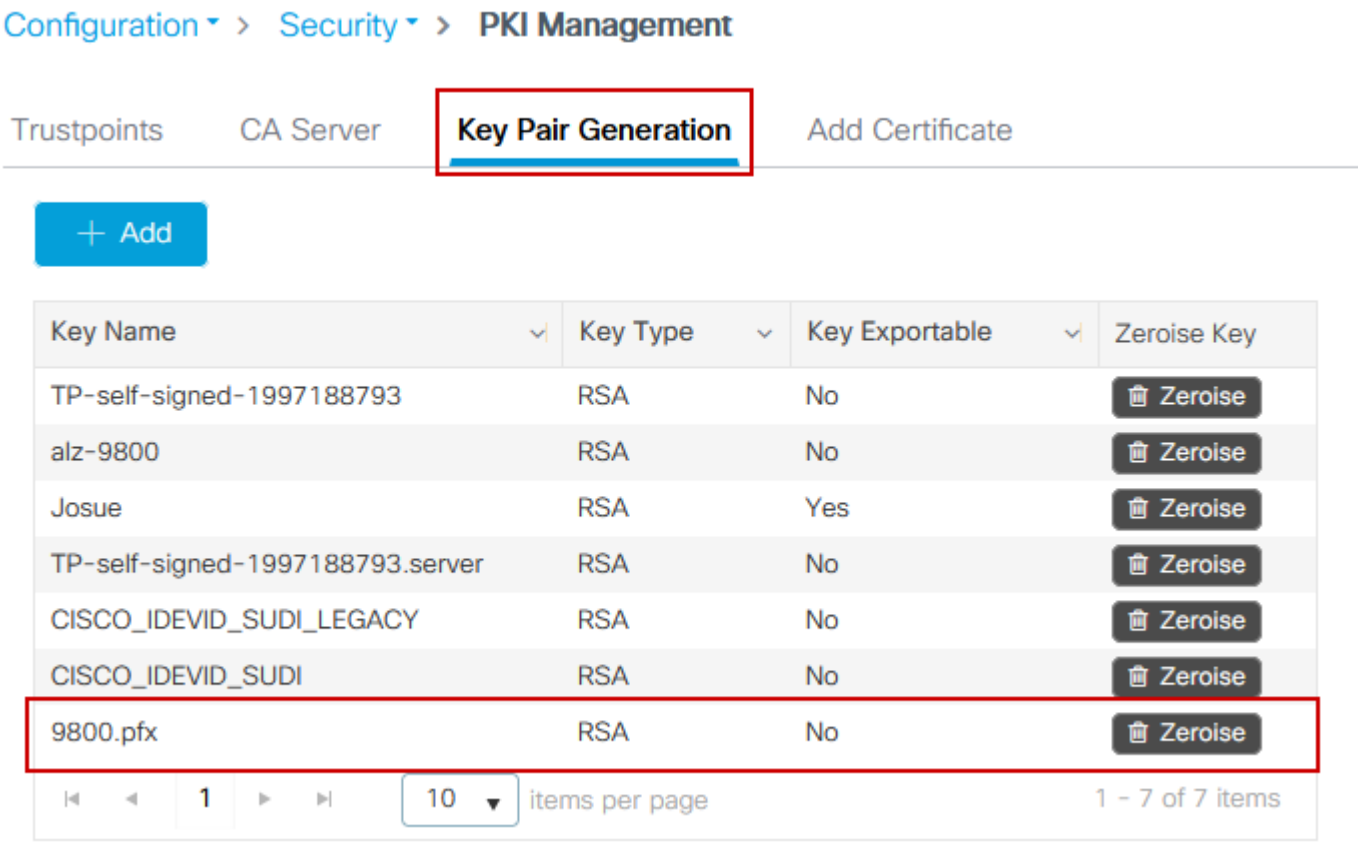
Etapa 1. Salve seu certificado PKCS12 em um servidor de Protocolo de Transferência de Arquivo Trivial (TFTP - Trivial File Transfer Protocol) que possa ser acessado a partir do WLC 9800. O certificado PKCS12 deve conter a chave privada e a cadeia de certificados até a CA raiz.

Etapa 2. Abra a GUI da WLC 9800 e navegue para **Configuration > Security > PKI Management**, clique na guia **Add Certificate . Expanda o menu Import PKCS12 Certificate** e preencha os detalhes do TFTP. Como alternativa, a opção **Desktop (HTTPS)** na lista suspensa **Transport Type** permite o carregamento HTTP através do navegador. **A senha do certificado** refere-se à senha que foi usada quando o certificado PKCS12 foi gerado.



Etapa 3. Verifique se as informações estão corretas e clique em **Import. Depois disso, você verá o novo par de chaves de certificado para esse novo ponto confiável instalado na guia Geração de par de chaves**. Após a importação bem-sucedida, a WLC 9800 também cria um ponto de confiança adicional para CAs de vários níveis.

> **Note**: Atualmente, a WLC 9800 não apresenta a cadeia completa de certificados sempre que um ponto de confiança específico é usado para webauth ou webadmin, em vez disso, apresenta o certificado do dispositivo e seu emissor imediato. Isso é rastreado com a ID de bug da Cisco CSCwa23606 , corrigido no Cisco IOS® XE 17.8.



CLI:

```
9800# configure terminal
9800(config)#crypto pki import
```

> **Note**: É importante que o nome do arquivo do certificado e o nome do ponto confiável correspondam exatamente para a WLC 9800 para criar quaisquer pontos confiáveis adicionais para CAs de vários níveis.

Conversão de Formato PKCS12 e Cadeia de Certificados em Cenários CA de Vários Níveis.

Épossível acabar em uma situação em que você tem um arquivo de chave privada e um certificado no formato PEM ou CRT e deseja combiná-los em um formato PKCS12 (.pfx) para carregar no WLC 9800. Para fazer isso, insira este comando:

```
openssl pkcs12 -export -in
```

Caso você tenha uma cadeia de certificados (uma ou várias CAs intermediárias e raiz), tudo no formato PEM, será necessário combinar tudo em um único arquivo .pfx.

Primeiro, combine manualmente os certificados CA em um único arquivo como tal. Copie e cole o conteúdo (salve o arquivo no formato .pem):

```
----- BEGIN Certificate --------
<intermediate CA cert>
------END Certificate --------
-----BEGIN Certificate -----
<root CA cert>
-----END Certificate--------
```

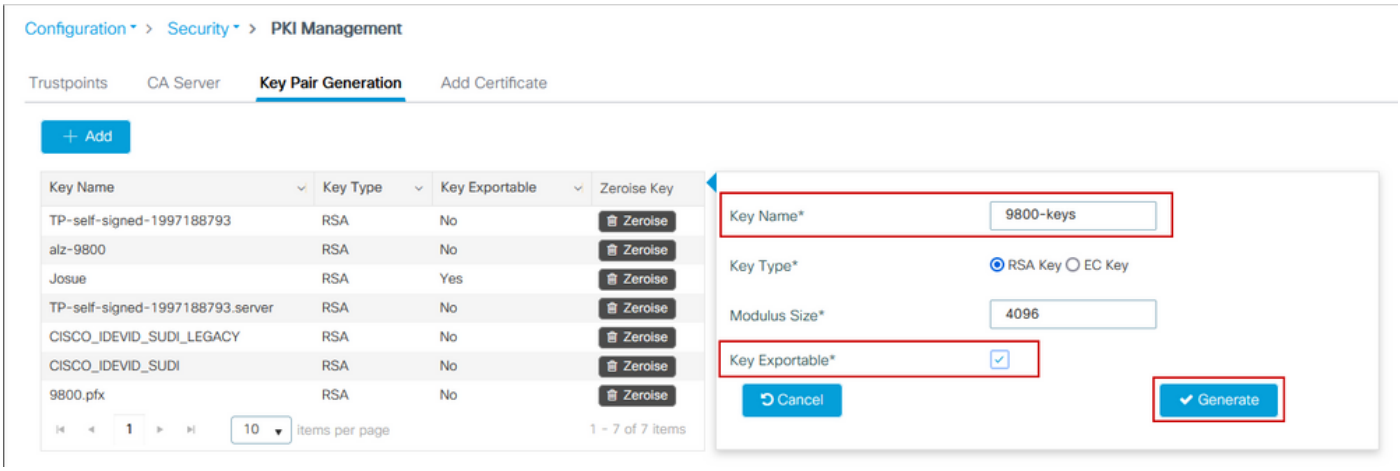
Posteriormente, você poderá combinar tudo em um arquivo de certificado PKCS12 com :

```
openssl pkcs12 -export -out chaincert.pfx -inkey
```

Consulte a seção Verify (Verificar) no final do artigo para ver a aparência do certificado final.

Opção 2 - Definir uma solicitação de chave e assinatura (CSR) na WLC 9800

Etapa 1. Gere um par de chaves RSA de uso geral. Navegue para **Configuration > Security > PKI Management**, escolha a guia **Key Pair Generation** e clique em **+ Add**. Insira os detalhes, verifique se a caixa de seleção **Key Exportable** está marcada e clique em **Generate**.



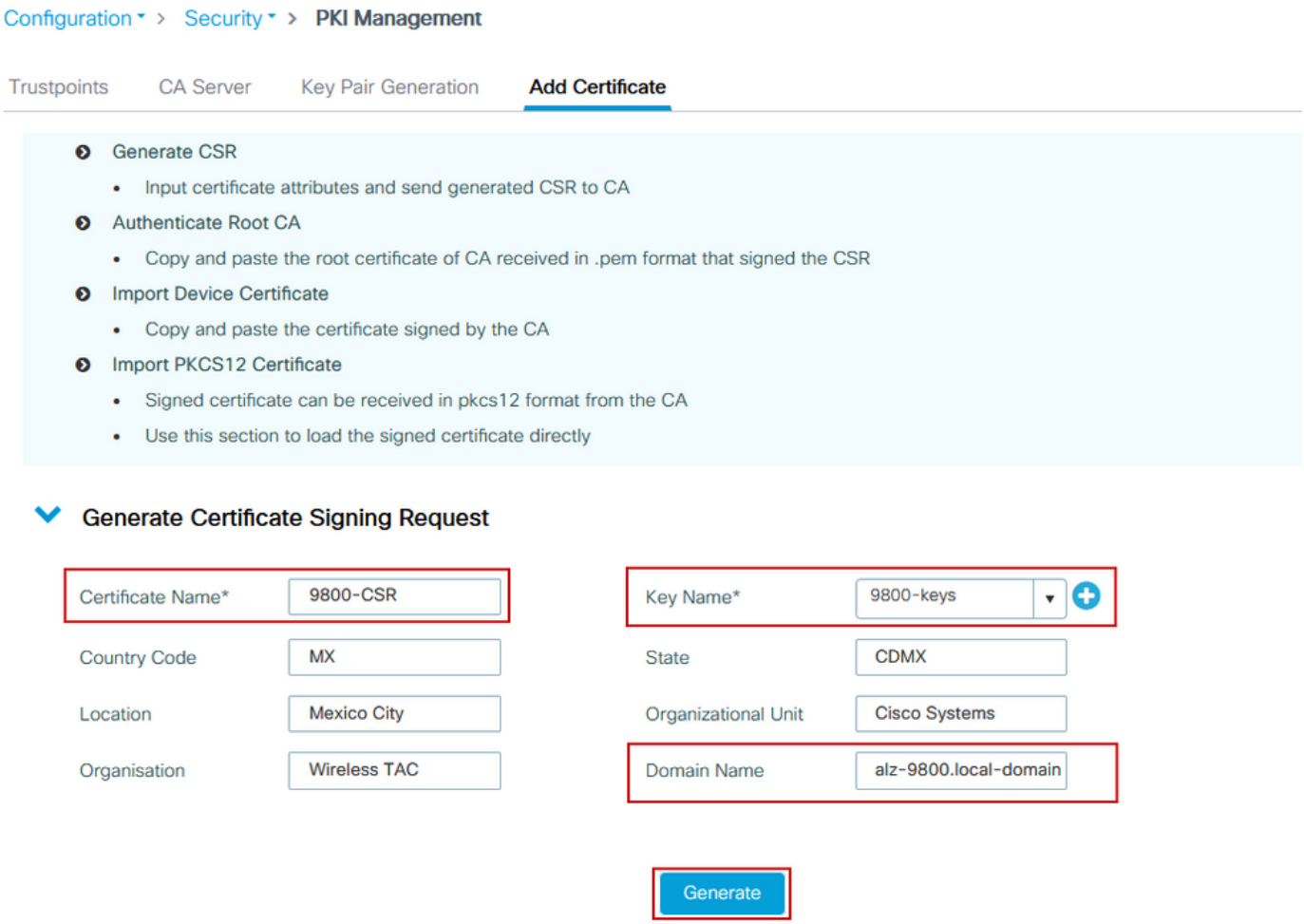
Configuração de CLI:

```
9800(config)#crypto key generate rsa general-keys label 9800-keys exportable
The name for the keys will be: 9800-keys
Choose the size of the key modulus in the range of 512 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [1024]: 4096
% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 9 seconds)
```

Etapa 2. Gere um CSR para a WLC 9800. Navegue até a guia **Add Certificate** e expanda **Generate Certificate Signing Request**, preencha os detalhes e escolha o par de chaves criado anteriormente na lista suspensa. É importante que **Domain Name** corresponda à URL definida para acesso do cliente na WLC 9800 (página de administração da Web, página de autenticação

da Web, etc.), **Certificate Name** é o nome do ponto de confiança para que você possa nomear com base em seu uso.

> **Note**: As WLCs 9800 suportam certificados com parâmetros curinga dentro de seus nomes comuns.



Verifique se as informações estão corretas e clique em **Gerar**. Isso exibe o CSR em uma caixa de texto ao lado do formulário original.

Copiar salva uma cópia na área de transferência para que você possa colá-la em um editor de texto e salvar o CSR. Se **Save to device** for selecionado, a WLC 9800 criará uma cópia do CSR e a armazenará no **bootflash:**/csr. Por exemplo, siga estes comandos:

```
9800#dir bootflash:/csr
Directory of bootflash:/csr/
```

```
1046531 -rw- 1844 Sep 28 2021 18:33:49 +00:00 9800-CSR1632856570.csr

26458804224 bytes total (21492699136 bytes free)
9800#more bootflash:/csr/9800-CSR1632856570.csr
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Configuração de CLI:

```
9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#enrollment terminal pem
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#subject-name C=MX, ST=CDMX, L=Mexico City, O=Cisco Systems, OU=Wireless TaC,
CN=alz-9800.local-domain.com
9800(ca-trustpoint)#rsakeypair 9800-keys
9800(ca-trustpoint)#subject-alt-name domain1.mydomain.com,domain2.mydomain.com
9800(ca-trustpoint)#exit

(config)#crypto pki enroll 9800-CSR
% Start certificate enrollment ..

% The subject name in the certificate will include: C=MX, ST=CDMX, L=Mexico City, O=Cisco
Systems, OU=Wireless TaC, CN=alz-9800.local-domain.com
% The subject name in the certificate will include: alz-9800
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

Parâmetros disponíveis para a configuração do nome do assunto:

C : País, deve ter apenas duas letras maiúsculas.

ST: Algum Estado, refere-se ao Nome do Estado ou Província.

L: Nome do local, refere-se à cidade.

O: Nome da organização, refere-se à empresa.

OU: Nome da Unidade Organizacional, pode consultar a seção.

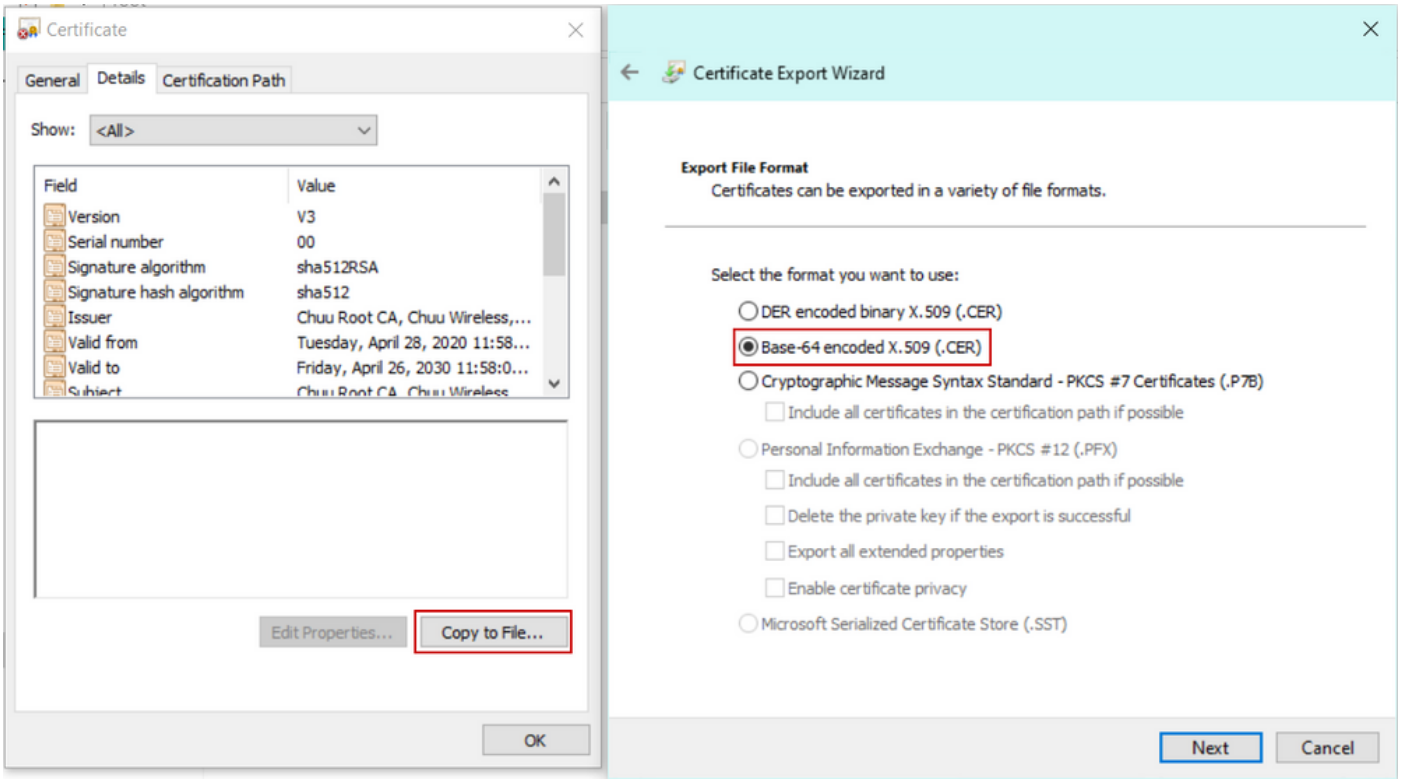
CN: (Nome comum)Refere-se ao assunto para o qual o certificado é emitido, você deve especificar o endereço IP específico a ser acessado (IP de gerenciamento sem fio, IP virtual e assim por diante) ou o nome de host configurado com FQDN.

> **Note**: Se você quiser adicionar um Nome alternativo do assunto, não será possível nas versões do Cisco IOS XE anteriores à 17.8.1 devido ao bug da Cisco ID CSCvt15177 . Esse cenário pode resultar em alguns alertas do navegador devido à ausência de SAN, para evitar isso, crie a chave e o CSR off-box, como mostrado na Opção 1.

Etapa 3. Faça com que seu CSR seja assinado por sua Autoridade de Certificação (CA). A cadeia de caracteres completa precisa ser enviada à autoridade de certificação para que seja assinada.

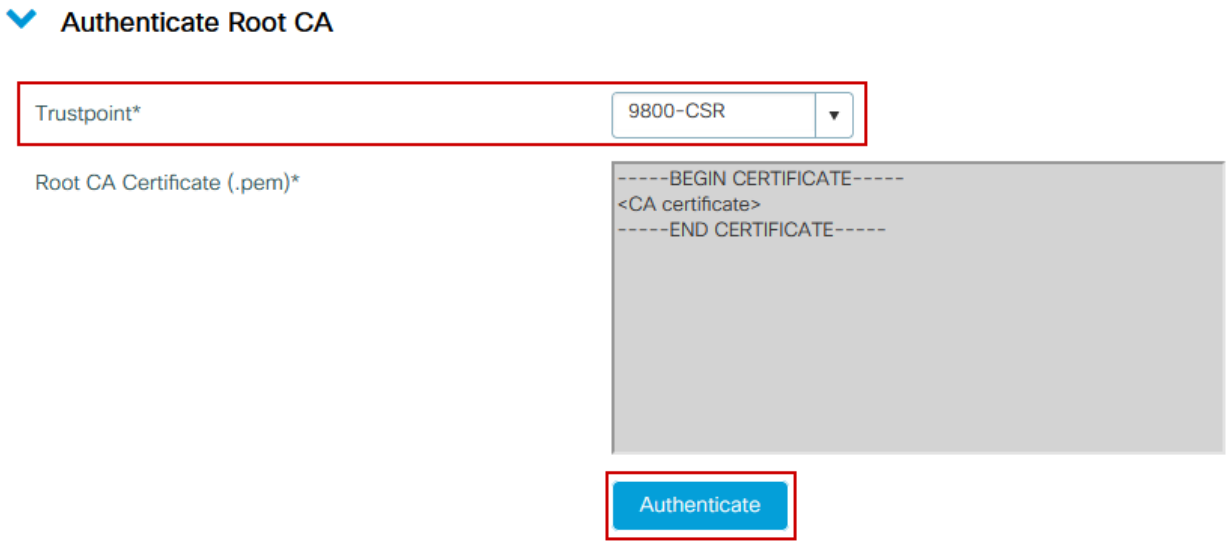
```
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Se você usar uma CA do Windows Server para assinar o certificado, baixe o certificado assinado no formato Base64. Caso contrário, você precisa exportar com utilitários como o gerenciador de certificado do Windows.



> **Note**: O processo de autenticação do ponto confiável depende do número de CAs que assinaram seu CSR. Se houver CA de nível único, siga a **Etapa 4a.** Se houver CA multiníveis, siga a **Etapa 4b**. Isso é necessário porque um ponto confiável só pode armazenar dois certificados por vez (o certificado de requerente e o certificado do emissor).

Passo 4a. Faça com que 9800 confie na CA do emissor. Baixe o certificado CA do emissor no formato .pem (Base64). Expanda a seção **Authentication Root CA** no mesmo menu, escolha o ponto confiável definido anteriormente na lista suspensa **Trustpoint** e cole o certificado CA do emissor. Verifique se os detalhes estão configurados corretamente e clique em **Authenticate**.



Configuração de CLI:

```
9800(config)# crypto pki authenticate 9800-CSR

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
Certificate has the following attributes: Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809 % Do you accept this certificate?
[yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

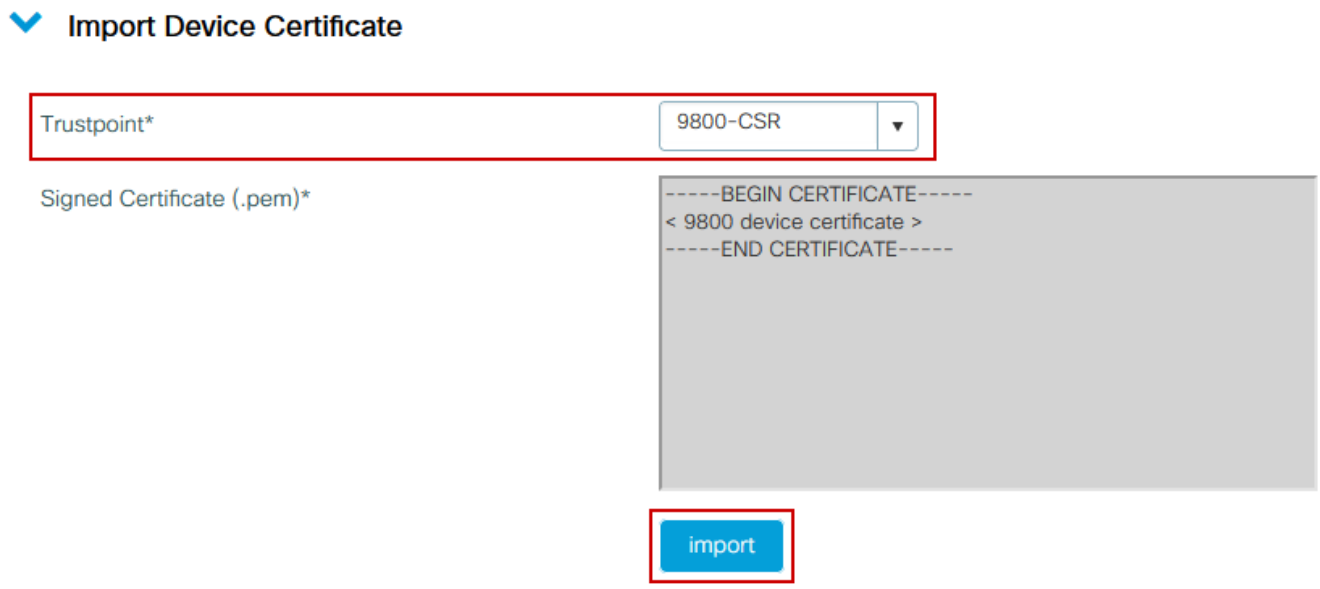
Passo 4b. No cenário em que existem vários níveis de autorização, um novo ponto de confiança é necessário para cada nível de CA. Esses pontos confiáveis contêm apenas o certificado de autenticação e apontam para o próximo nível de autenticação. Esse processo é feito apenas na CLI e, neste exemplo, há duas CAs intermediárias e uma CA raiz:

```
9800(config)#crypto pki trustpoint root
9800(ca-trustpoint)#enrollment terminal
9800(ca-trustpoint)#chain-validation stop
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#exit
9800(config)#crypto pki authenticate root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 6CAC00D5 C5932D01 B514E413 D41B37A8
Fingerprint SHA1: 5ABD5667 26B7BD0D 83BDFC34 543297B7 3D3B3F24

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

9800(config)#crypto pki trustpoint intermediate
9800(ca-trustpoint)#enrollment terminal
9800(ca-trustpoint)#chain-validation continue root
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#exit
9800(config)#crypto pki authenticate intermediate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----




-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 2F3F1EF7 EDF66BE0 F4C9BDA1 01D8FFBA
Fingerprint SHA1: 1651F5C7 5D6F7A6B F411D529 34E980B1 D629A2B9
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported

9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#chain-validation continue intermediate
9800(config)#crypto pki authenticate 9800-CSR

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----




-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Etapa 5. Carregue o certificado assinado na WLC 9800. Expanda a seção **Importar certificado do dispositivo** no mesmo menu. Escolha o **ponto confiável** definido anteriormente e cole o certificado

de dispositivo assinado fornecido pela CA. Em seguida, clique em **importar** quando as informações do certificado forem verificadas.



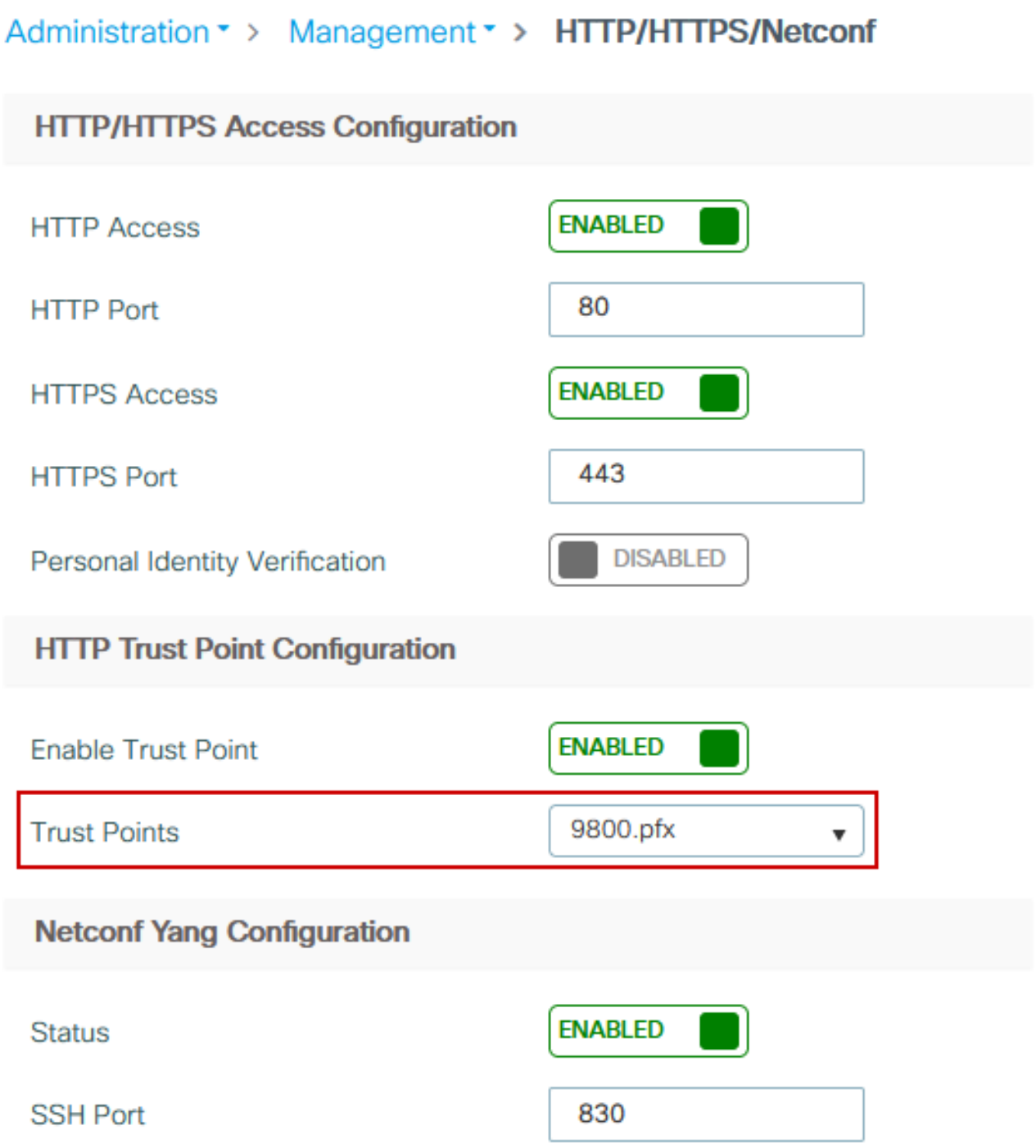
Configuração de CLI:

```
9800(config)#crypto pki import 9800-CSR certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
<9800 device certificate >
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

Usar o novo certificado

Administração da Web

Navegue até **Administration > Management > HTTP/HTTPS/Netconf** e escolha o certificado importado na lista suspensa **Trust Points**.

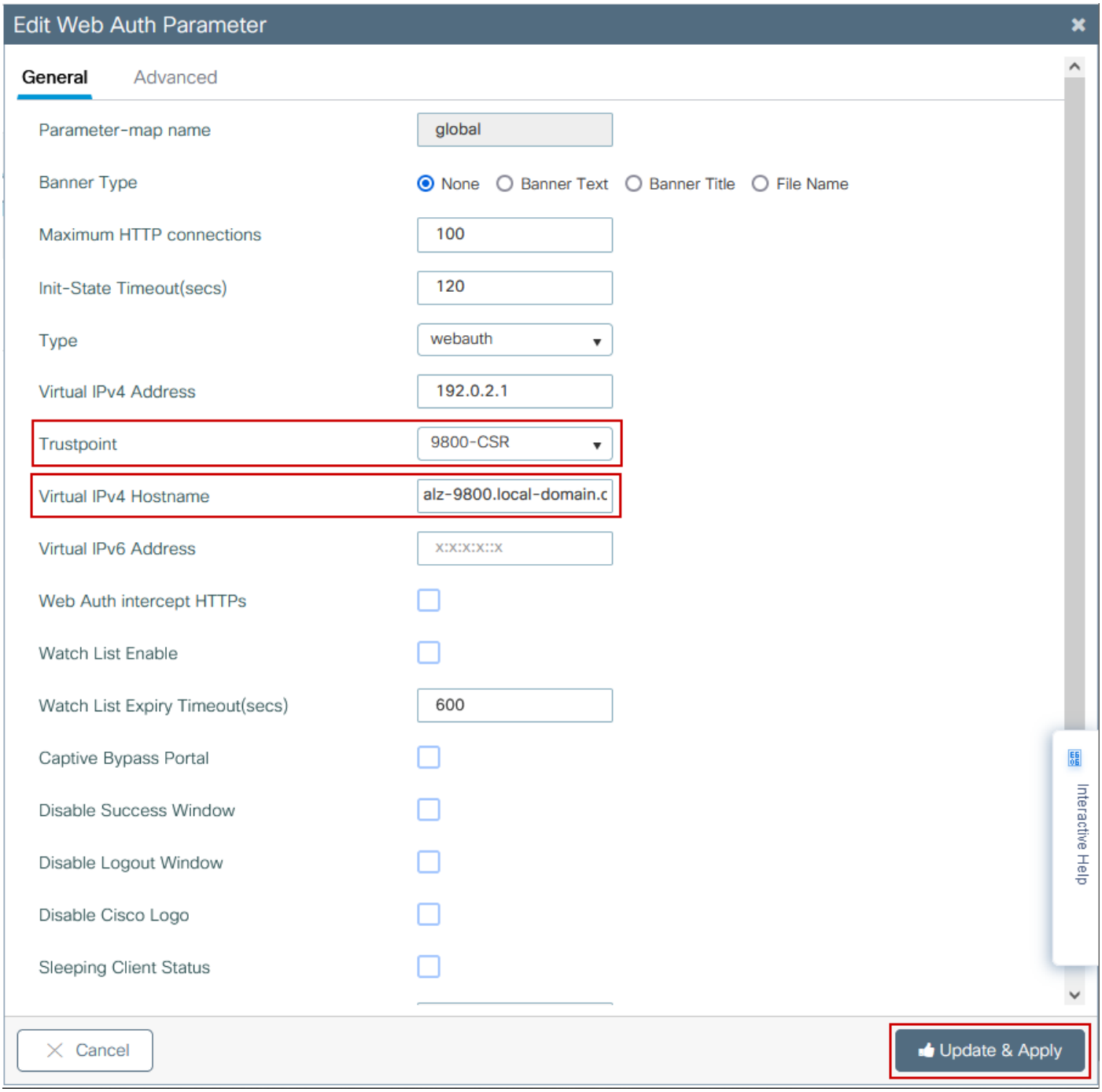


Configuração de CLI:

```
9800(config)#ip http secure-trustpoint 9800.pfx
9800(config)#no ip http secure-server
9800(config)#ip http secure-server
```

Autenticação Web local

Navegue para **Configuration > Security > Web Auth**, escolha o mapa de parâmetros **global** e escolha o ponto de confiança importado na lista suspensa **Trustpoint**. Clique em **Update & Apply** para salvar as alterações. Certifique-se de que o **nome de host IPv4 virtual** corresponda ao nome comum no certificado.



Configuração de CLI:

```
9800(config)#parameter-map type webauth global
9800(config-params-parameter-map)#type webauth
9800(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1 virtual-host alz-9800.local-domain.com
9800(config-params-parameter-map)#trustpoint 9800-CSR
```

Para atualizar o uso do certificado, reinicie os serviços HTTP:

```
9800(config)#no ip http server
9800(config)#ip http server
```

.

Considerações sobre alta disponibilidade

Em um par 9800 configurado para HA SSO (Stateful Switchover High Availability), todos os certificados são replicados do primário para o secundário na sincronização inicial em massa. Isso inclui certificados em que a chave privada foi gerada no próprio controlador, mesmo que a chave RSA esteja configurada para não ser exportável. Depois que o par HA é estabelecido, qualquer novo certificado instalado é instalado nas duas controladoras e todos os certificados são replicados em tempo real.

Após a falha, o controlador antigo-secundário-agora-ativo usa os certificados herdados do primário de forma transparente.

Como garantir que o certificado seja confiável para navegadores da Web

Há algumas considerações importantes para garantir que um certificado seja confiável para navegadores da Web:

- Seu nome comum (ou um campo SAN) deve corresponder à URL visitada pelo navegador.
- Deve estar dentro do seu período de validade.
- Ele deve ser emitido por uma CA ou cadeia de CA cuja raiz seja confiável pelo navegador. Para isso, o certificado fornecido pelo servidor Web deve conter todos os certificados da cadeia até (não necessariamente incluído) um certificado confiável pelo navegador do cliente (normalmente a CA raiz).
- Se ele contiver listas de revogação, o navegador precisará ser capaz de baixá-las e o certificado CN não deverá estar listado.

Verificar

Você pode usar estes comandos para verificar a configuração dos certificados:

```
9800#show crypto pki certificate 9800.pfx

Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx
```

```
CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx
```

```
9800#show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: 9800.pfx
HTTP secure server active session modules: ALL
```

Você pode verificar sua cadeia de certificados no 9800. No caso de um certificado de dispositivo emitido por uma CA intermediária, ele próprio emitido por uma CA raiz, você tem um ponto confiável por grupos de dois certificados, de modo que cada nível tem seu próprio ponto confiável. Nesse caso, a WLC 9800 tem 9800.pfx com o certificado do dispositivo (certificado da WLC) e sua CA de emissão (CA intermediária). Em seguida, outro ponto confiável com a CA raiz que emitiu essa CA intermediária.

```
9800#show crypto pki certificate 9800.pfx
Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
```

```
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx

CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx

9800#show crypto pki certificate 9800.pfx-rrr1
CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Validity Date:
start date: 04:58:05 Pacific Apr 29 2020
end date: 04:58:05 Pacific Apr 27 2030
Associated Trustpoints: 9800-CSR 9800.pfx-rrr1
```

Verificação de certificado com OpenSSL

O OpenSSL pode ser útil para verificar o próprio certificado ou para realizar algumas operações de conversão.

Para exibir um certificado com OpenSSL:

```
openssl x509 -in
```

Para exibir o conteúdo de um CSR:

```
openssl req -noout -text -in
```

Se você quiser verificar o certificado final na WLC 9800, mas quiser usar algo diferente do seu navegador, o OpenSSL pode fazer isso e fornecer muitos detalhes.

```
openssl s_client -showcerts -verify 5 -connect
```

Você pode substituir <wlcURL> pelo URL do webadmin do 9800 ou pelo URL do portal do convidado (IP virtual). Você também pode colocar um endereço IP lá. Ele informa qual cadeia de certificados é recebida, mas a validação do certificado nunca pode estar 100% correta quando um endereço IP é usado em vez do nome do host.

Para exibir o conteúdo e verificar um certificado PKCS12 (.pfx) ou uma cadeia de certificados:

```
openssl pkcs12 -info -in
```

Aqui está um exemplo desse comando em uma cadeia de certificados em que o certificado do dispositivo é emitido para o Centro de Assistência Técnica (TAC) por uma CA intermediária chamada "intermediate.com", ela mesma emitida por uma CA raiz chamada "root.com" :

```
openssl pkcs12 -info -in chainscript2.pfx
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/CN=TAC
issuer=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
-----BEGIN CERTIFICATE-----
<Device certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
-----BEGIN CERTIFICATE-----
```

```
<Intermediate certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
-----BEGIN CERTIFICATE-----
<Root certificate >
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Private key >
-----END ENCRYPTED PRIVATE KEY-----
```

Troubleshoot

Use esse comando para solucionar problemas. Se for feito em uma sessão remota (SSH ou telnet), o **monitor de terminal** será necessário para exibir as saídas:

```
9800#debug crypto pki transactions
```

Saída de depuração de cenário bem-sucedida

Essa saída exibe a saída esperada quando uma importação de certificado bem-sucedida acontece em um 9800. Use-o como referência e identifique o estado de falha:

```
Sep 28 17:35:23.242: CRYPTO_PKI: Copying pkcs12 from bootflash:9800.pfx
Sep 28 17:35:23.322: CRYPTO_PKI: Creating trustpoint 9800.pfx
Sep 28 17:35:23.322: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx created succesfully
Sep 28 17:35:23.324: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.324: CRYPTO_PKI: issuerName=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: subjectname=e=user@example.com,cn=alz-9800,ou=Cisco
Systems,o=Wireless TAC,l=CDMX,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: adding RSA Keypair
Sep 28 17:35:23.324: CRYPTO_PKI: bitValue of ET_KEY_USAGE = 140
Sep 28 17:35:23.324: CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
Sep 28 17:35:23.324: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named 9800.pfx has been generated or
imported by pki-pkcs12
Sep 28 17:35:23.331: CRYPTO_PKI: adding as a router certificate.Public key in cert and stored
public key 9800.pfx match

Sep 28 17:35:23.333: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.333: CRYPTO_PKI: issuerName=cn=Chuu Root CA,ou=Chuu Wireless,o=Chuu
Inc,l=Iztapalapa,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: subjectname=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: no matching private key presents.

[...]

Sep 28 17:35:23.335: CRYPTO_PKI: Setting the key_type as RSA
```

```
Sep 28 17:35:23.335: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.335: CRYPTO_PKI:Peer's public inserted successfully with key id 21
Sep 28 17:35:23.336: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.337: CRYPTO_PKI: Deleting cached key having key id 31
Sep 28 17:35:23.337: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.337: CRYPTO_PKI:Peer's public inserted successfully with key id 32
Sep 28 17:35:23.338: CRYPTO_PKI: (A0323) Session started - identity selected (9800.pfx)
Sep 28 17:35:23.338: CRYPTO_PKI: Rcvd request to end PKI session A0323.
Sep 28 17:35:23.338: CRYPTO_PKI
alz-9800#: PKI session A0323 has ended. Freeing all resources.
Sep 28 17:35:23.338: CRYPTO_PKI: unlocked trustpoint 9800.pfx, refcount is 0
Sep 28 17:35:23.338: CRYPTO_PKI: Expiring peer's cached key with key id 32Public key in cert and
stored public key 9800.pfx match

Sep 28 17:35:23.341: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.341: CRYPTO_PKI: cert verified and inserted.
Sep 28 17:35:23.402: CRYPTO_PKI: Creating trustpoint 9800.pfx-rrr1
Sep 28 17:35:23.402: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx-rrr1 created succesfully
Sep 28 17:35:23.403: CRYPTO_PKI: Setting the key_type as RSA
Sep 28 17:35:23.404: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.404: CRYPTO_PKI:Peer's public inserted successfully with key id 22
Sep 28 17:35:23.405: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.406: CRYPTO_PKI: no CRLs present (expected)
Sep 28 17:35:23.406: %PKI-6-PKCS12_IMPORT_SUCCESS: PKCS #12 import in to trustpoint 9800.pfx
successfully imported.
```

Tente importar um certificado PKCS12 que não tenha uma CA

Se você importar um certificado e receber o erro: "Certificado CA não encontrado.", significa que o arquivo .pfx não contém a cadeia inteira ou que uma CA não está presente.

```
9800(config)#crypto pki import pkcs12.pfx pkcs12 bootflash:pks12.pfx password
```

```
% Importing pkcs12...
Source filename [pks12.pfx]?
Reading file from bootflash:pks12.pfx
% Warning: CA cert is not found. The imported certs might not be usable.
```

Se você executar o comando openssl pkcs12 -info -in <caminho para cert> e apenas um certificado com uma chave privada for exibido, significa que a CA não está presente. Como regra prática, esse comando lista idealmente toda a cadeia de certificados. Não é necessário incluir a CA raiz superior se ela já for conhecida pelos navegadores clientes.

Uma maneira de corrigir isso é desconstruir o PKCS12 em PEM e reconstruir a cadeia corretamente. No próximo exemplo, tínhamos um arquivo .pfx que continha apenas o certificado do dispositivo (WLC) e sua chave. Ele foi emitido por uma CA intermediária (que não estava presente no arquivo PKCS12) que, por sua vez, foi assinada por uma CA raiz bem conhecida.

Etapa 1. Exporte a chave privada.

```
openssl pkcs12 -in
```

Etapa 2. Exporte o certificado como PEM.

```
openssl pkcs12 -in
```

Etapa 3. Faça download do certificado intermediário da CA como PEM.

A origem da CA depende da natureza dela. Se for uma CA pública, uma pesquisa on-line será suficiente para localizar o repositório. Caso contrário, o administrador de CA deve fornecer os certificados no formato Base64 (.pem). Se houver vários níveis de CA, agrupe-os em um único arquivo, como o apresentado no final do processo de importação da **Opção 1**.

Etapa 4. Reconstrua o PKCS 12 a partir da chave, certificado do dispositivo e certificado CA.

```
openssl pkcs12 -export -out fixedcertchain.pfx -inkey cert.key -in certificate.pem -certfile CA.pem
```

Agora temos o "fixedcertchain.pfx", que podemos importar com prazer para o Catalyst 9800!

Notas e limitações

- O Cisco IOS® XE não oferece suporte a certificados CA com um válido além de 2099: ID de bug da Cisco CSCvp64208
- O Cisco IOS® XE não suporta o pacote SHA256 message digest PKCS 12 (certificados SHA256 são suportados, mas não se o próprio pacote PKCS12 for assinado com SHA256) : ID de bug Cisco CSCvz41428

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.