Générer et télécharger des certificats CSR sur les WLC Catalyst 9800

Table des matières

Introduction

Ce document décrit le processus global pour générer, télécharger et installer des certificats sur le Catalyst 9800

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le WLC 9800, le point d'accès (AP) pour le fonctionnement de base
- Comment utiliser l’application OpenSSL
- Infrastructure à clé publique (PKI) et certificats numériques

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 9800-L, Cisco IOS® XE version 17.3.3
- Application 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Sur 16.10.X, les 9800 ne prennent pas en charge un certificat différent pour l'authentification Web et l'administration Web. Le portail de connexion Web utilise toujours le certificat par défaut.

Sur 16.11.X, vous pouvez configurer un certificat dédié pour l'authentification Web, définir le point de confiance à l'intérieur de la carte-paramètre globale.

Il y a deux options pour obtenir un certificat pour un WLC 9800.

1. Générez une demande de signature de certificat (CSR) avec OpenSSL ou toute autre application SSL. Obtenez un certificat PKCS12 signé par votre autorité de certification (CA) et chargez-le directement sur le WLC 9800. Cela signifie que la clé privée est fournie avec ce certificat.
2. Utilisez l'interface de ligne de commande du WLC 9800 pour générer un CSR, faites-le signer par une autorité de certification, puis chargez chaque certificat dans la chaîne manuellement vers le WLC 9800.

Utilisez celui qui correspond le mieux à vos besoins.

Option 1 - Charger un certificat signé PKCS12 préexistant

Définir une demande de signature

Si vous ne disposez pas encore du certificat, vous devez générer une demande de signature à transmettre à votre autorité de certification.

Modifiez le fichier **openssl.cnf** à partir de votre répertoire actuel (sur un ordinateur portable sur lequel OpenSSL est installé), copiez et collez ces lignes pour inclure le champ Subject Alternate Names (SAN) dans les nouveaux CSR créés.

```
[ 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
```

Remplacez les noms DNS.X par votre SAN. Remplacez les champs principaux par les détails du certificat dont vous avez besoin. Veillez à répéter le nom commun dans les champs SAN (DNS.x). Google Chrome exige que le nom présent dans l'URL soit dans les champs SAN afin de faire confiance au certificat.

Dans le cas d'un administrateur Web, vous devez également remplir les champs SAN avec des variantes de l'URL (simplement le nom d'hôte ou le nom de domaine complet (FQDN) par exemple) afin que le certificat corresponde, quels que soient les types d'administrateur dans l'URL dans la barre d'adresse du navigateur.

Générez le CSR à partir d'OpenSSL avec cette commande :

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

Le CSR génère comme **myCSR.csr** et sa clé comme **private.key** dans le répertoire où OpenSSL est exécuté à partir de sauf si le chemin complet est fourni à la commande.

Assurez-vous que le fichier **private.key** est sécurisé car il est utilisé pour chiffrer les communications.

Vous pouvez vérifier son contenu avec :

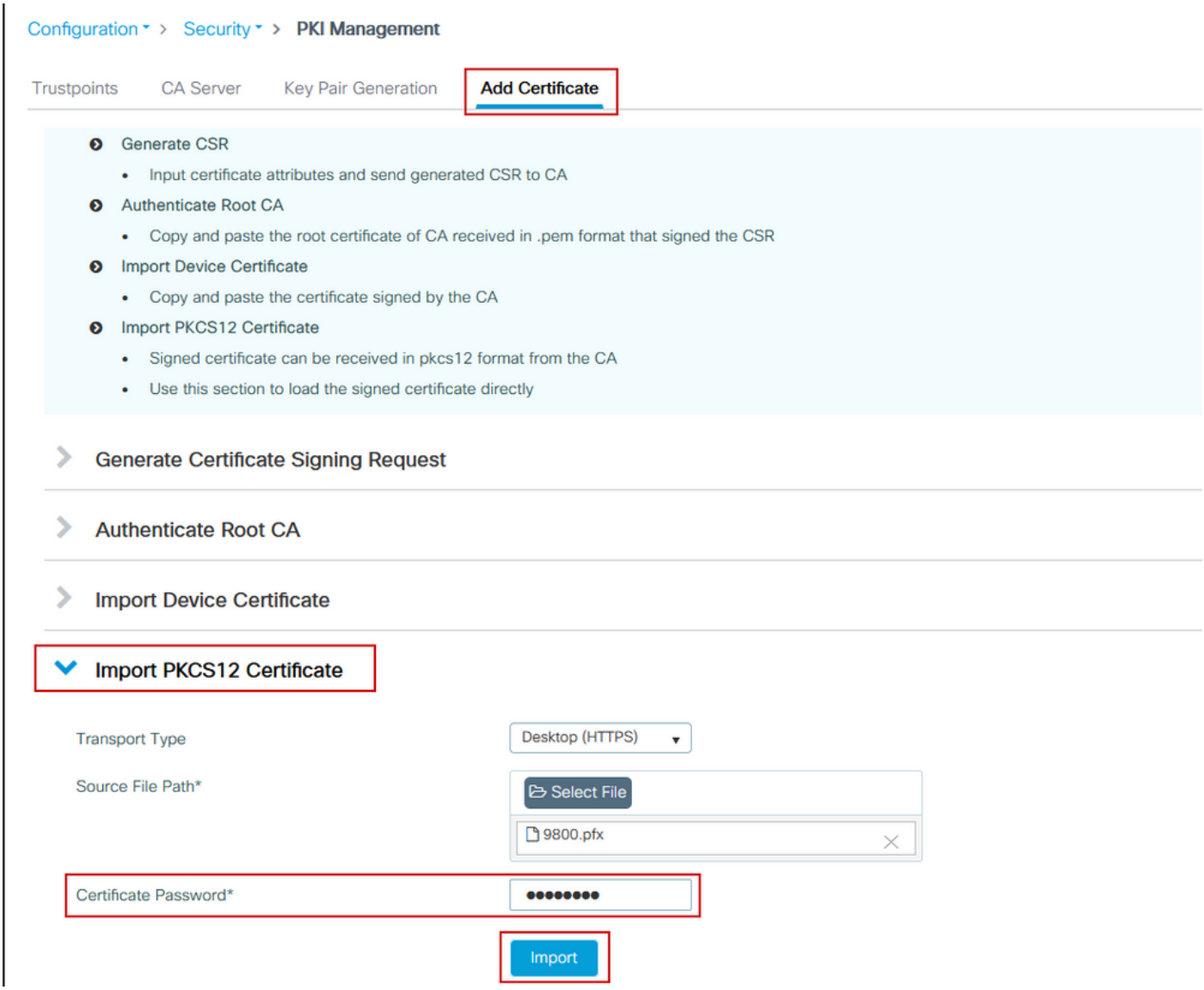
```
openssl req -noout -text -in myCSR.csr
```

Vous pouvez ensuite fournir ce CSR à votre autorité de certification pour qu'elle le signe et qu'elle reçoive un certificat. Assurez-vous que la chaîne complète est téléchargée à partir de l'autorité de certification et que le certificat est au format Base64 au cas où il aurait besoin d'une manipulation supplémentaire.

Importer le certificat

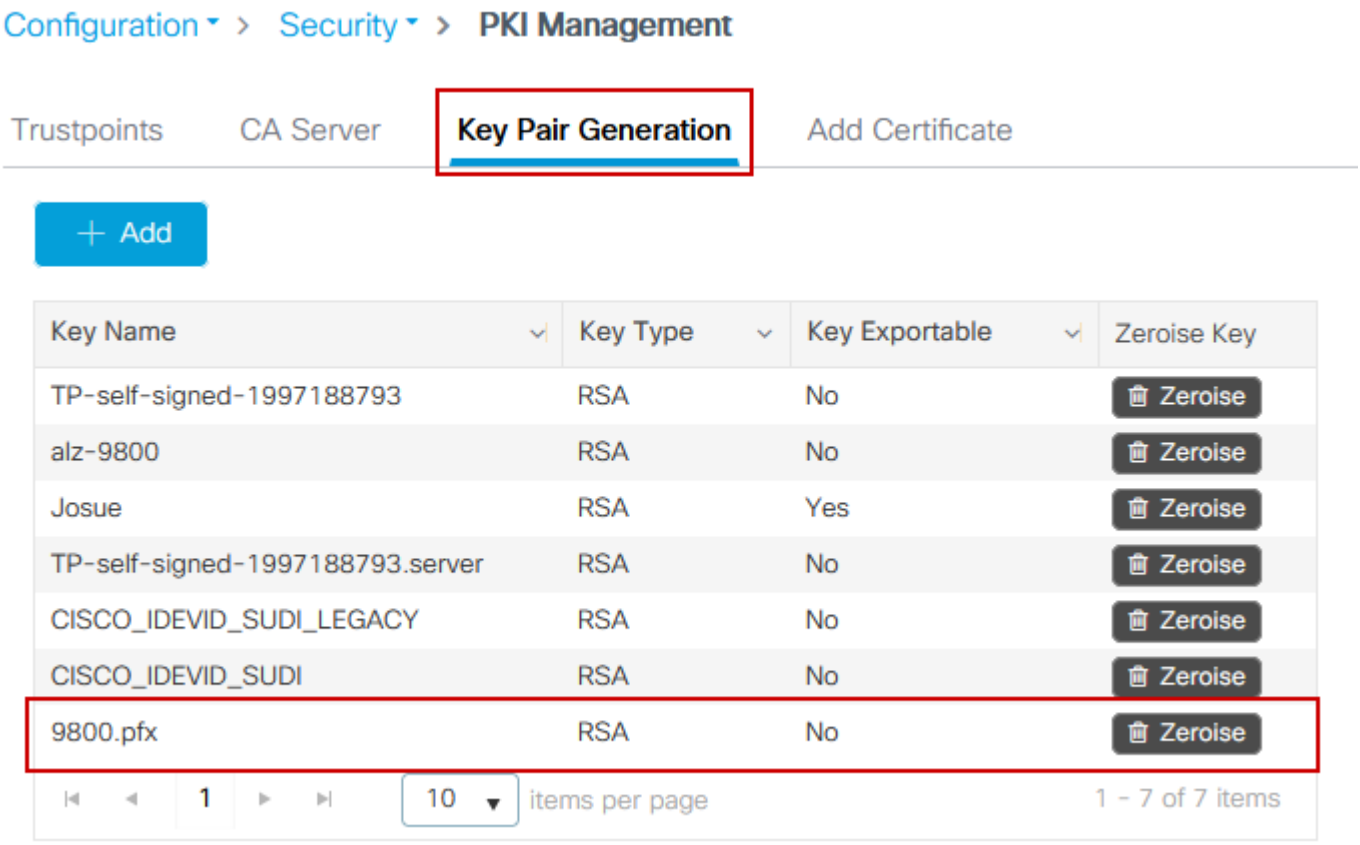
Étape 1. Enregistrez votre certificat PKCS12 sur un serveur TFTP (Trivial File Transfer Protocol) accessible depuis le WLC 9800. Le certificat PKCS12 doit contenir la clé privée ainsi que la chaîne de certificats jusqu'à l'autorité de certification racine.

Étape 2. Ouvrez l'interface graphique utilisateur de votre WLC 9800 et accédez à **Configuration > Security > PKI Management**, cliquez sur l'onglet **Add Certificate. Développez le menu Import PKCS12 Certificate** et renseignez les détails TFTP. L'option **Desktop (HTTPS)** dans la liste déroulante **Transport Type** permet également le téléchargement HTTP via le navigateur. **Le mot de passe du certificat** fait référence au mot de passe qui a été utilisé lors de la génération du certificat PKCS12.



Étape 3. Vérifiez que les informations sont correctes et cliquez sur **Import. Après cela, vous voyez la nouvelle paire de clés de certificat pour ce nouveau point de confiance installé dans l'onglet Génération de paires de clés**. Une fois l'importation réussie, le WLC 9800 crée également un point de confiance supplémentaire pour les autorités de certification à plusieurs niveaux.

> **Remarque** : actuellement, le WLC 9800 ne présente pas la chaîne de certificats complète chaque fois qu'un point de confiance spécifique est utilisé pour webauth ou webadmin, mais il présente plutôt le certificat du périphérique et son émetteur immédiat. Ce problème est suivi avec l'ID de bogue Cisco CSCwa23606 , corrigé dans Cisco IOS® XE 17.8.



CLI :

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

Remarque : il est important que le nom du fichier de certificat et le nom du point de confiance correspondent exactement pour le WLC 9800 pour créer des points de confiance supplémentaires pour les autorités de certification à plusieurs niveaux.

Conversion du format PKCS12 et chaîne de certificats dans les scénarios d'autorité de certification multiniveau.

Il est possible de se retrouver dans une situation où vous avez un fichier de clé privée et un certificat au format PEM ou CRT et que vous voulez les combiner dans un format PKCS12 (.pfx) pour les télécharger vers le WLC 9800. Pour ce faire, entrez la commande suivante :

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

Dans le cas où vous avez une chaîne de certificats (une ou plusieurs CA intermédiaires et CA

racine) tous au format PEM, vous devez alors les combiner dans un seul fichier .pfx.

Tout d'abord, combinez manuellement les certificats d'autorité de certification dans un seul fichier. Copiez et collez le contenu (enregistrez le fichier au format .pem) :

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

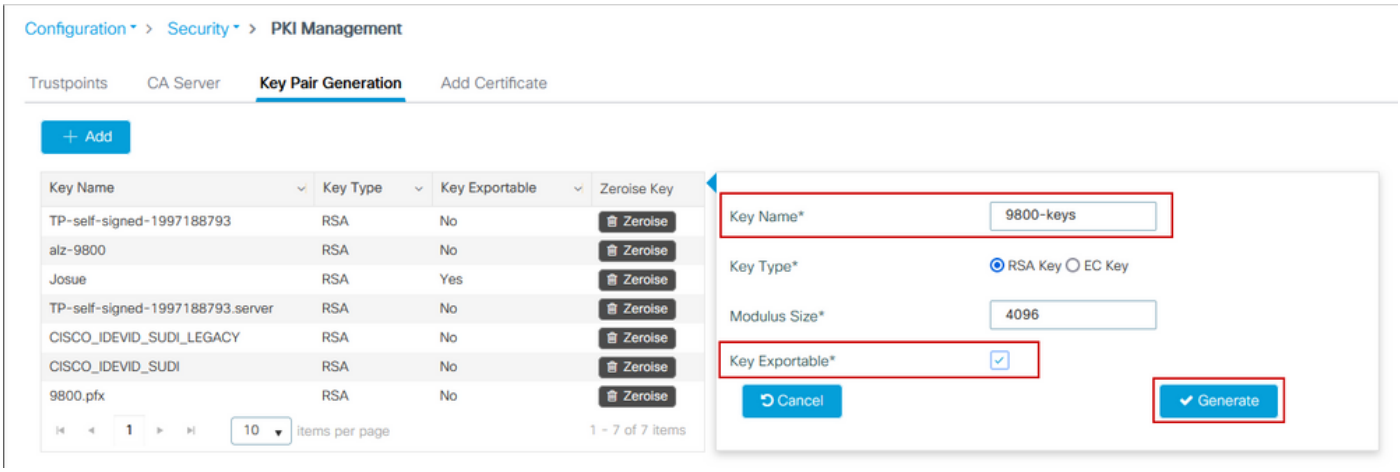
Vous pourrez ensuite combiner tous les éléments dans un fichier de certificat PKCS12 avec :

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

Reportez-vous à la section Vérifier à la fin de l'article pour voir à quoi ressemble le certificat final.

Option 2 - Définir une clé et une demande de signature (CSR) sur le WLC 9800

Étape 1. Générez une paire de clés RSA à usage général. Accédez à **Configuration > Security > PKI Management**, choisissez l'onglet **Key Pair Generation**, puis cliquez sur **+ Add**. Entrez les détails, assurez-vous que la case **Key Exportable** est cochée, puis cliquez sur **Generate**.



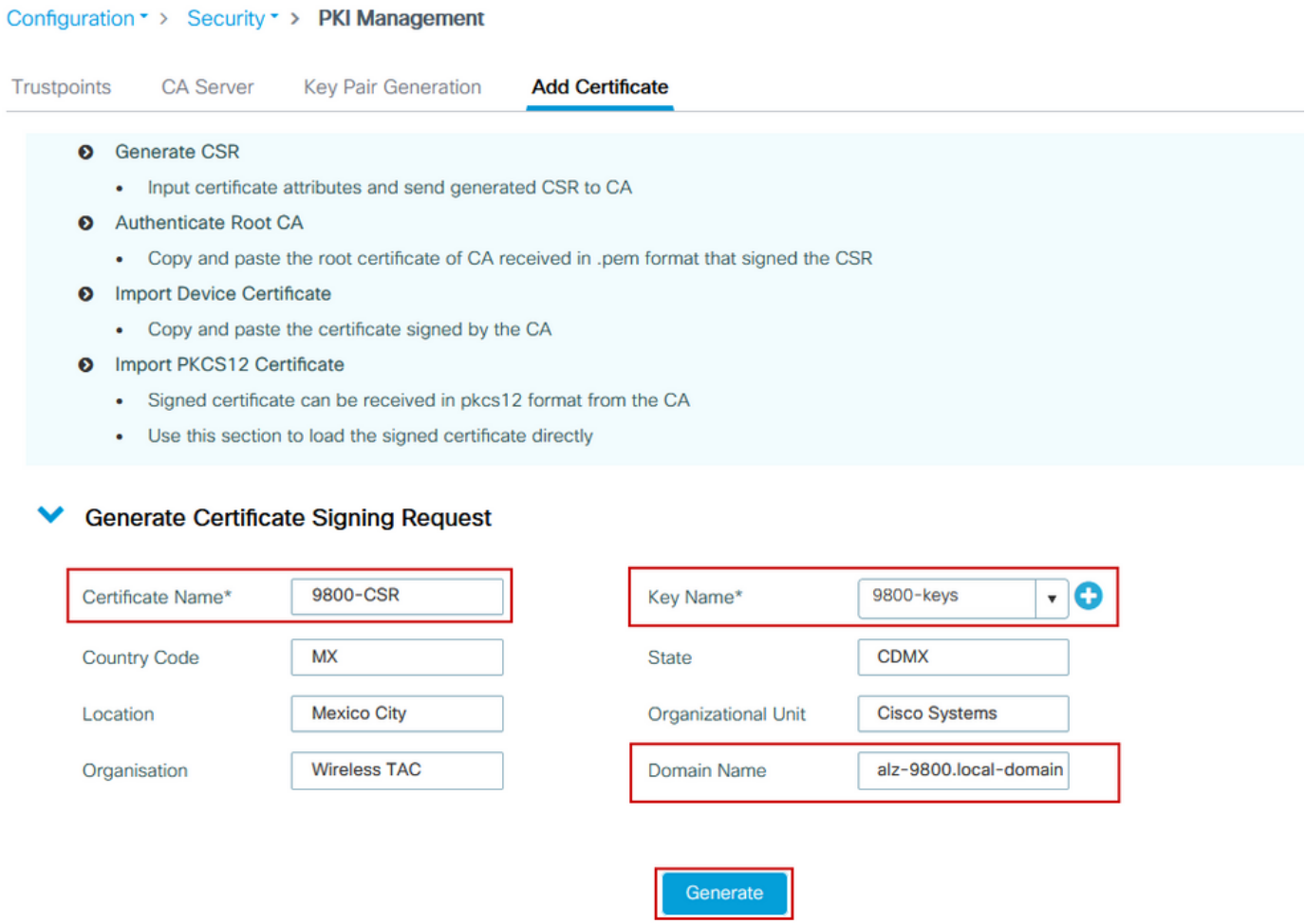
Configuration CLI :

```
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)
```

Étape 2.Générez un CSR pour votre WLC 9800. Accédez à l'onglet **Add Certificate** et développez **Generate Certificate Signing Request**, remplissez les détails et choisissez la paire de clés

précédemment créée dans la liste déroulante. Il est important que le **nom de domaine** corresponde à l'URL qui est définie pour l'accès client sur le WLC 9800 (page d'administration Web, page d'authentification Web, etc.), **Certificate Name** est le nom du point de confiance afin que vous puissiez attribuer un nom en fonction de son utilisation.

> **Remarque** : les WLC 9800 prennent en charge les certificats avec des paramètres génériques dans leur nom commun.



Vérifiez que les informations sont correctes, puis cliquez sur **Generate**. Le CSR s'affiche dans une zone de texte en regard du formulaire d'origine.

Copier enregistre une copie dans le Presse-papiers afin que vous puissiez la coller dans un éditeur de texte et enregistrer le CSR. Si **Save to device** est sélectionné, le WLC 9800 crée une copie du CSR et la stocke dans **bootflash:**/csr. Par exemple, exécutez ces commandes :

```
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-----
```

Configuration 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
```

Paramètres disponibles pour la configuration du nom du sujet :

C : Pays, il ne doit y avoir que deux lettres majuscules.

ST : Certains États font référence au nom de l'État ou de la province.

L : Nom du lieu, fait référence à la ville.

O : Nom de l'organisation, fait référence à la société.

OU : Nom de l'unité d'organisation, peut se référer à la section.

CN : (Common Name)Désigne l'objet auquel le certificat est délivré. Vous devez spécifier l'adresse IP spécifique à laquelle accéder (adresse IP de gestion sans fil, adresse IP virtuelle, etc.) ou le nom d'hôte configuré avec le nom de domaine complet.

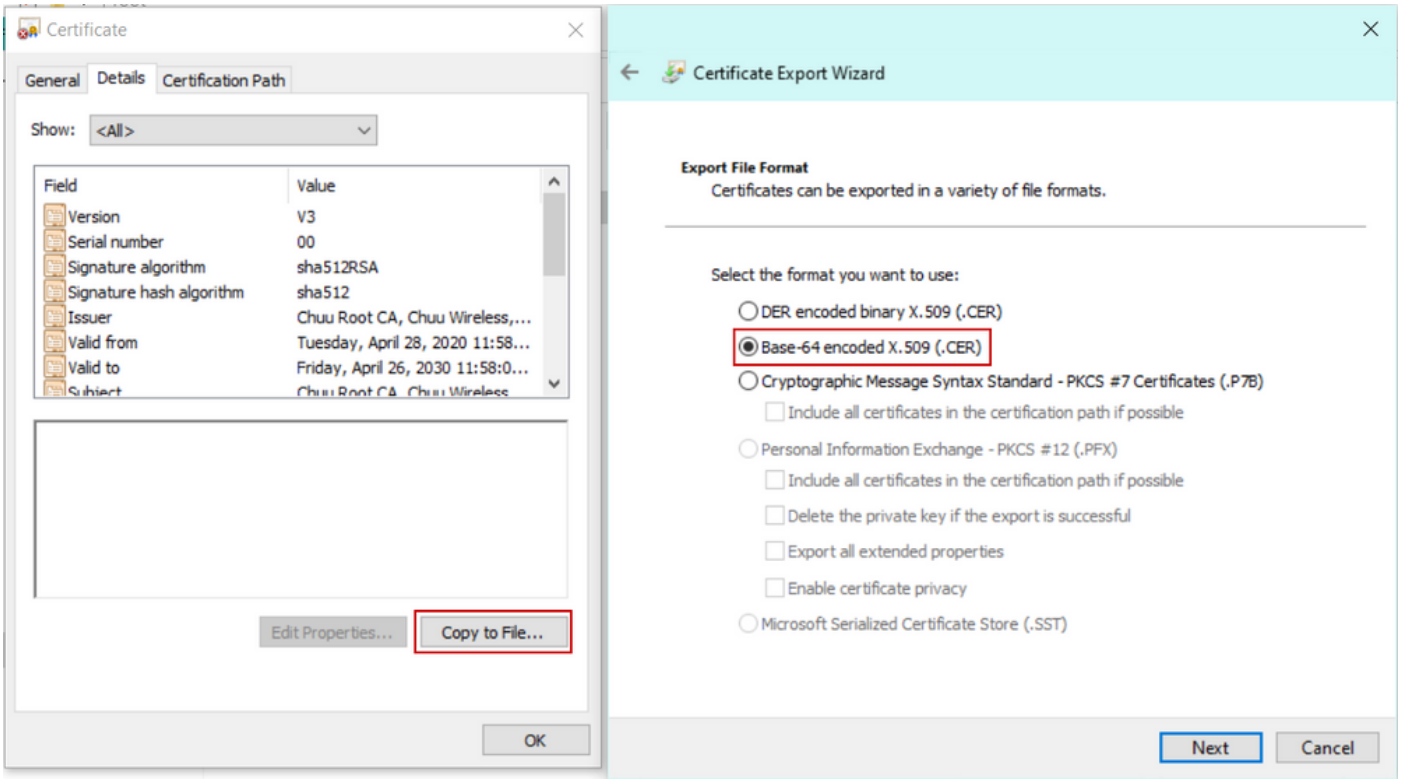
> **Remarque** : si vous souhaitez ajouter un autre nom d'objet, cela n'est pas possible sur les versions de Cisco IOS XE antérieures à la version 17.8.1 en raison de l'ID de bogue Cisco

CSCvt15177 . Ce scénario peut entraîner certaines alertes du navigateur en raison de l'absence de SAN. Pour éviter cela, créez la clé et le CSR en désactivant la boîte, comme indiqué dans l'option 1.

Étape 3. Faites signer votre CSR par votre autorité de certification (CA). La chaîne complète doit être envoyée à l'autorité de certification pour être signée.

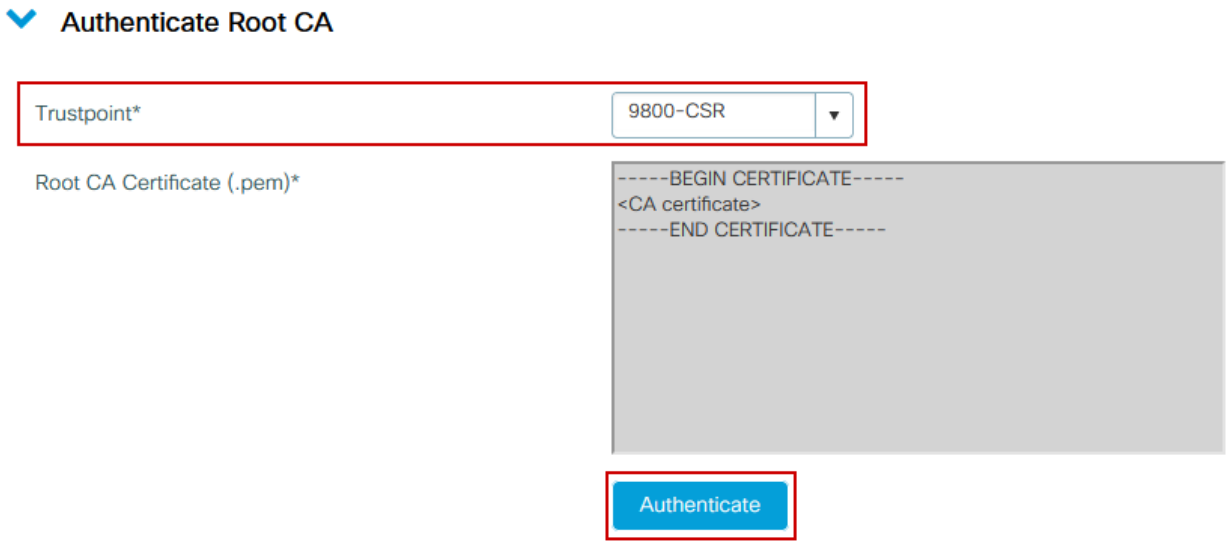
```
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Si vous utilisez une autorité de certification Windows Server pour signer le certificat, téléchargez le certificat signé au format Base64. Sinon, vous devez exporter avec des utilitaires comme le gestionnaire de certificats Windows.



Remarque : le processus d'authentification par point de confiance dépend du nombre d'autorités de certification qui ont signé votre CSR. S'il existe une autorité de certification de niveau unique, vérifiez l'**étape 4a.** S'il y a une autorité de certification à plusieurs niveaux, passez à l'**étape 4b**. Cela est nécessaire car un point de confiance ne peut stocker que deux certificats à la fois (le certificat d'objet et le certificat d'émetteur).

Étape 4a. Faites confiance au 9800 à l'autorité de certification émettrice. Téléchargez le certificat CA émetteur au format .pem (Base64). Développez la section **Authentication Root CA** dans le même menu, choisissez le point de confiance précédemment défini dans la liste déroulante **Trustpoint**, et collez le certificat de l'autorité de certification émettrice. Vérifiez que les détails sont correctement configurés et cliquez sur **Authenticate**.



Configuration 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
```

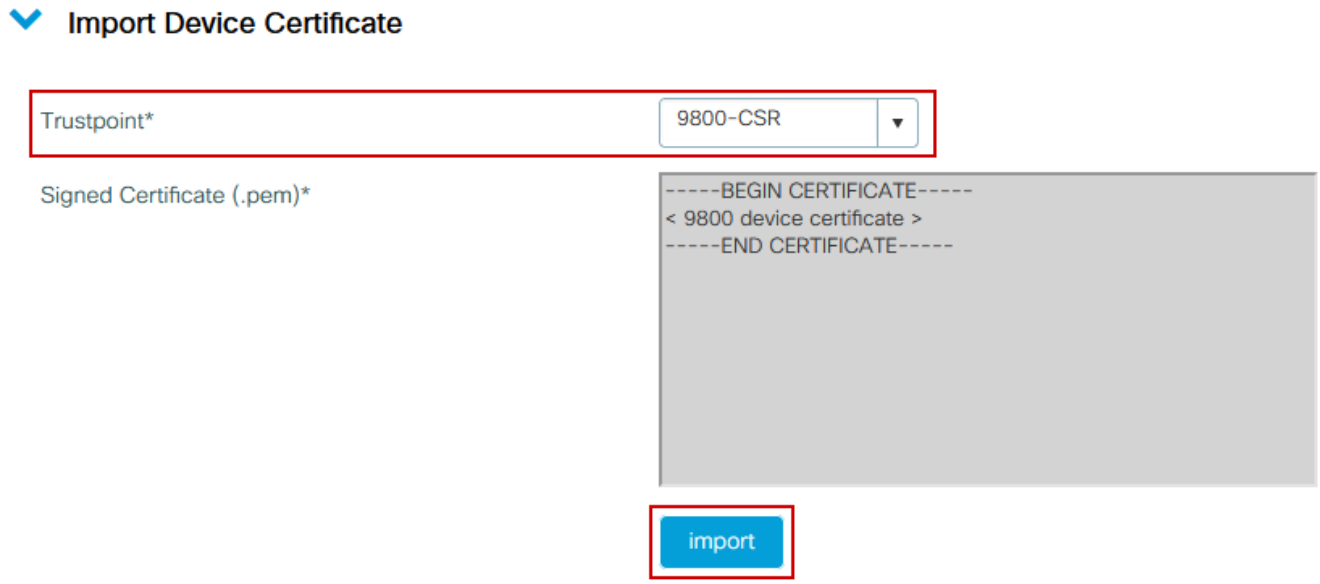
Étape 4b. Dans le scénario où plusieurs niveaux d'autorisation existent, un nouveau point de confiance est requis pour chaque niveau d'autorité de certification. Ces points de confiance contiennent uniquement le certificat d'authentification et pointent vers le niveau d'authentification suivant. Ce processus est effectué dans l'interface de ligne de commande uniquement et dans cet exemple, il y a une autorité de certification intermédiaire et une autorité de certification racine :

```
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 9800-CSR
9800(ca-trustpoint)#chain-validation continue root
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
```

> **Remarque** : s'il existe plusieurs autorités de certification intermédiaires dans la chaîne de certification, un nouveau point de confiance doit être généré par niveau de certification supplémentaire. Ces points de confiance doivent faire référence au point de confiance qui contient le niveau de certification suivant avec la commande **chain-validation continue <trustpoint-name>**.

Étape 5. Chargez le certificat signé dans le WLC 9800. Développez la section **Import Device Certificate** dans le même menu. Choisissez le **Trustpoint** précédemment défini et collez le certificat de périphérique signé fourni par l'autorité de certification. Cliquez ensuite sur **import** une fois les informations de certificat vérifiées.



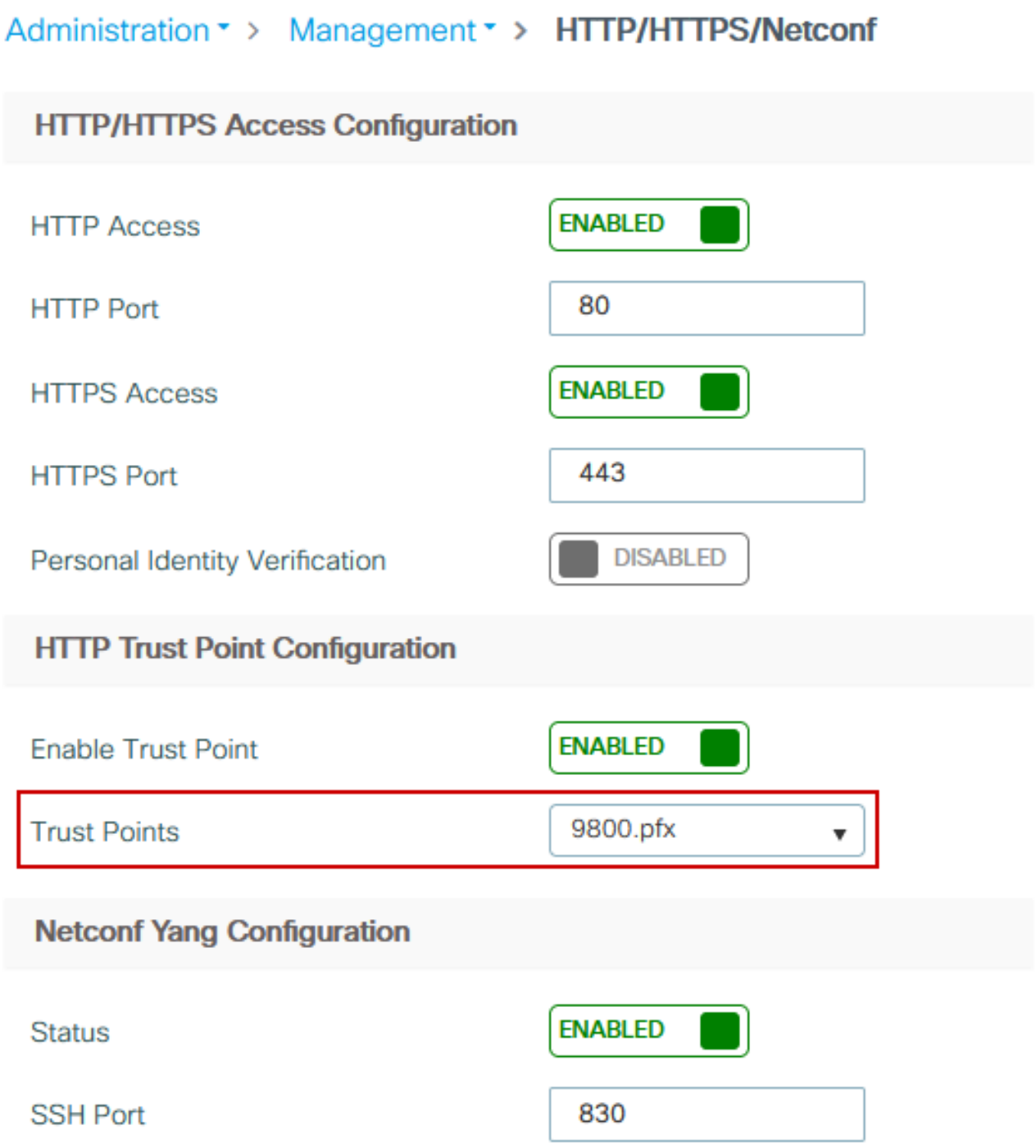
Configuration CLI :

```
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
```

Utiliser le nouveau certificat

Administration Web

Accédez à **Administration > Management > HTTP/HTTPS/Netconf** et choisissez le certificat importé dans la liste déroulante **Trust Points**.

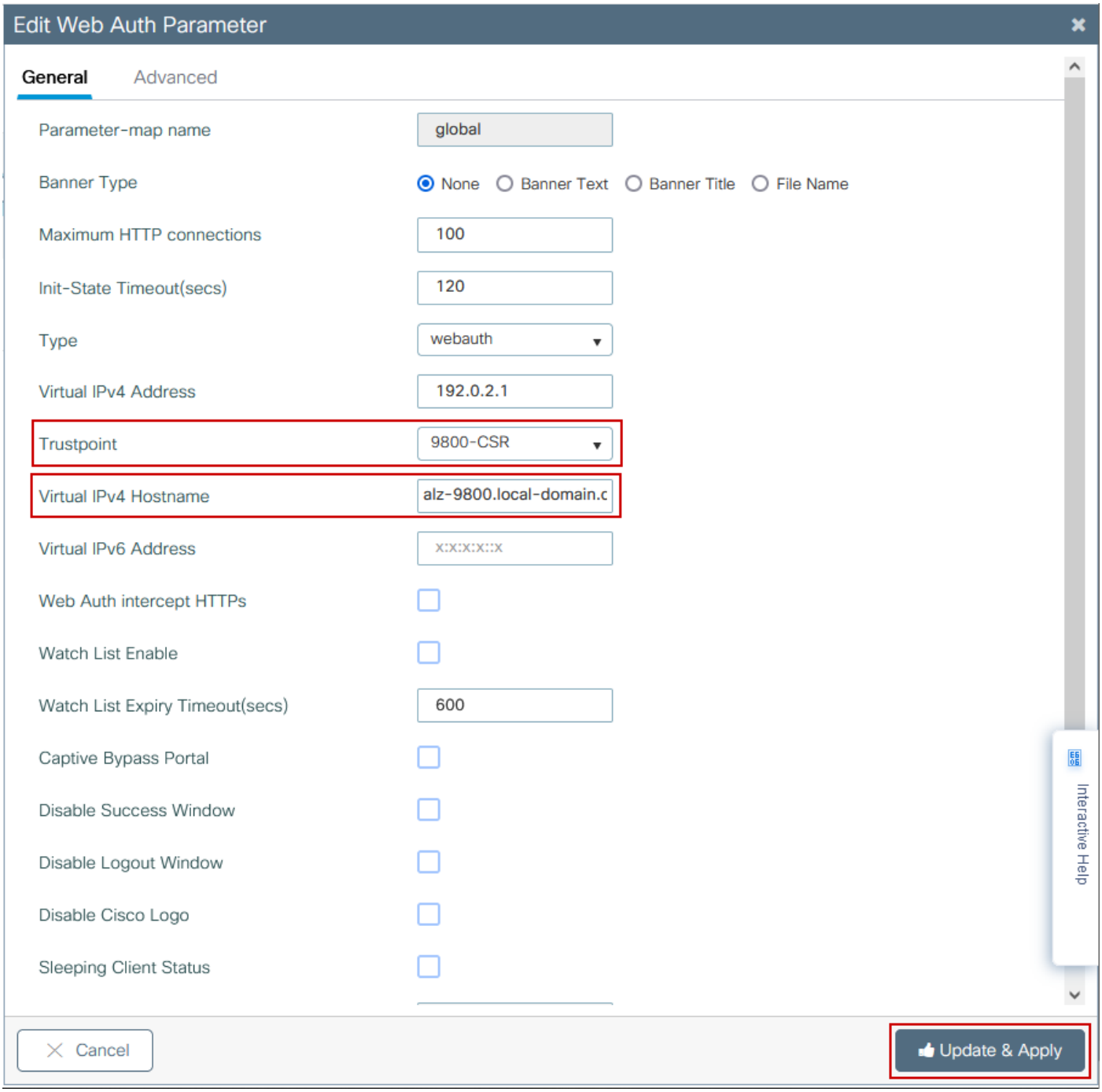


Configuration CLI :

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

Authentification Web locale

Naviguez jusqu'à **Configuration > Security > Web Auth**, choisissez le mappage de paramètre **global** et choisissez le point de confiance importé dans la liste déroulante **Trustpoint**. Cliquez sur **Update & Apply** pour enregistrer les modifications. Assurez-vous que **Virtual IPv4 Hostname** correspond au nom commun dans le certificat.



Configuration 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
```

Afin de mettre à jour l'utilisation du certificat, redémarrez les services HTTP :

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

.

Considérations sur la haute disponibilité

Sur une paire 9800 configurée pour la haute disponibilité de commutation avec état (HA SSO), tous les certificats sont répliqués du principal vers le secondaire lors de la synchronisation en bloc initiale. Cela inclut les certificats où la clé privée a été générée sur le contrôleur lui-même, même si la clé RSA est configurée pour ne pas être exportable. Une fois la paire haute disponibilité établie, tout nouveau certificat installé est installé sur les deux contrôleurs et tous les certificats sont répliqués en temps réel.

Après la panne, l'ancien contrôleur secondaire maintenant actif utilise les certificats hérités du contrôleur principal de manière transparente.

Comment s'assurer que le certificat est approuvé par les navigateurs Web

Il y a quelques considérations importantes pour s'assurer qu'un certificat est approuvé par les navigateurs Web :

- Son nom commun (ou un champ SAN) doit correspondre à l'URL visitée par le navigateur.
- Elle doit être comprise dans sa période de validité.
- Il doit être émis par une autorité de certification ou une chaîne d'autorités de certification dont la racine est approuvée par le navigateur. Pour cela, le certificat fourni par le serveur Web doit contenir tous les certificats de la chaîne jusqu'à ce qu'un certificat approuvé par le navigateur client (généralement l'autorité de certification racine) ne soit (pas nécessairement inclus).
- S'il contient des listes de révocation, le navigateur doit pouvoir les télécharger et le certificat CN ne doit pas être répertorié.

Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration des certificats :

```
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
```

Vous pouvez vérifier votre chaîne de certificats sur le 9800. Dans le cas d'un certificat de périphérique émis par une autorité de certification intermédiaire, elle-même émise par une autorité de certification racine, vous avez un point de confiance par groupes de deux certificats, de sorte que chaque niveau a son propre point de confiance. Dans ce cas, le WLC 9800 a 9800.pfx avec le certificat de périphérique (certificat WLC) et son CA d'émission (CA intermédiaire). Puis un autre point de confiance avec l'autorité de certification racine qui a émis cette autorité de certification intermédiaire.

```
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
```

Vérification de certificat avec OpenSSL

OpenSSL peut être utile pour vérifier le certificat lui-même ou effectuer certaines opérations de conversion.

Afin d'afficher un certificat avec OpenSSL :

```
openssl x509 -in
```

Afin d'afficher le contenu d'un CSR :

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

Si vous voulez vérifier le certificat de fin sur le WLC 9800 mais que vous voulez utiliser autre chose que votre navigateur, OpenSSL peut le faire et vous donner beaucoup de détails.

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

Vous pouvez remplacer <wlcURL> par l'URL du webadmin du 9800 ou l'URL du portail invité (IP virtuelle). Vous pouvez également y ajouter une adresse IP. Il vous indique quelle chaîne de certificats est reçue, mais la validation du certificat ne peut jamais être correcte à 100 % lorsqu'une adresse IP est utilisée à la place du nom d'hôte.

Afin d'afficher le contenu et de vérifier un certificat PKCS12 (.pfx) ou une chaîne de certificats :

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

Voici un exemple de cette commande sur une chaîne de certificats où le certificat du périphérique est délivré au Centre d'assistance technique (TAC) par une autorité de certification intermédiaire appelée « intermediaire.com », elle-même délivrée par une autorité de certification racine appelée « 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-----
```

Dépannage

Utilisez cette commande pour résoudre les problèmes. Si fait sur une session à distance (SSH ou telnet) alors **terminal monitor** est nécessaire pour afficher les sorties :

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

Sortie de débogage de scénario réussie

Cette sortie affiche la sortie attendue lorsqu'une importation de certificat réussie se produit sur un 9800. Utilisez ceci pour référence et identifier l'état d'échec :

```
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.
```

Essayez d'importer un certificat PKCS12 qui n'a pas d'autorité de certification

Si vous importez un certificat et obtenez l'erreur : "CA cert is not found.", cela signifie que votre fichier .pfx ne contient pas toute la chaîne ou qu'une autorité de certification n'est pas présente.

```
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.
```

Si vous exécutez la commande **openssl pkcs12 -info -in <path to cert>** et qu'un seul certificat avec une clé privée s'affiche, cela signifie que l'autorité de certification n'est pas présente. En règle générale, cette commande répertorie idéalement toute votre chaîne de certificats. Il n'est pas nécessaire d'inclure l'autorité de certification racine supérieure si elle est déjà connue par les navigateurs clients.

Une façon de résoudre ce problème consiste à déconstruire le PKCS12 en PEM et à reconstruire la chaîne correctement. Dans l'exemple suivant, nous avions un fichier .pfx qui contenait uniquement le certificat du périphérique (WLC) et sa clé. Il a été émis par une autorité de certification intermédiaire (qui n'était pas présente dans le fichier PKCS12) qui, à son tour, a été signée par une autorité de certification racine connue.

Étape 1. Exportez la clé privée.

```
openssl pkcs12 -in
```

Étape 2. Exportez le certificat en tant que PEM.

```
openssl pkcs12 -in
```

Étape 3. Téléchargez le certificat CA intermédiaire en tant que PEM.

La source de l'autorité de certification dépend de sa nature. S'il s'agit d'une autorité de certification publique, une recherche en ligne suffit pour trouver le référentiel. Sinon, l'administrateur de l'autorité de certification doit fournir les certificats au format Base64 (.pem). S'il existe plusieurs niveaux d'autorité de certification, regroupez-les dans un seul fichier, comme celui présenté à la fin du processus d'importation de l'**option 1**.

Étape 4. Reconstruisez le PKCS 12 à partir de la clé, du certificat de périphérique et du certificat CA.

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

Nous avons maintenant "fixedcertchain.pfx" que nous pouvons heureusement importer sur le Catalyst 9800 !

Remarques et limites

- Cisco IOS® XE ne prend pas en charge les certificats CA dont la valeur est supérieure à 2099 : ID de bogue Cisco CSCvp64208
- Cisco IOS® XE ne prend pas en charge l'offre groupée PKCS 12 de condensation de message SHA256 (les certificats SHA256 sont pris en charge, mais pas si l'offre groupée PKCS12 elle-même est signée avec SHA256) : ID de bogue Cisco CSCvz41428
- Vous pouvez voir la fragmentation si le WLC doit transporter des certificats d'utilisateur et si l'appliance NAC/ISE est accessible via Internet (par exemple, dans un déploiement SD-WAN). Les certificats sont presque toujours supérieurs à 1500 octets (ce qui signifie que plusieurs paquets RADIUS sont envoyés pour transporter le message de certificat) et si vous avez plusieurs MTU différents sur le chemin réseau, une fragmentation excessive des paquets RADIUS eux-mêmes peut se produire. Dans de tels cas, nous vous recommandons d'envoyer tous vos datagrammes UDP pour le trafic WLC sur le même chemin afin d'éviter des problèmes tels que le retard/la gigue qui peut être causé par la météo Internet

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.