

Générer et importer des CSR pour les certificats tiers

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Certificats en chaîne](#)

[Prise en charge des certificats en chaîne](#)

[Niveaux de certificat](#)

[Étape 1. Générer une requête de signature de certificat \(CSR\)](#)

[Option A. CSR avec OpenSSL](#)

[Option B. CSR généré par le WLC](#)

[Étape 2. Obtenir la signature du certificat](#)

[Option A : Obtenez le fichier Final.pem auprès de l'autorité de certification de votre entreprise](#)

[Option B : Obtenir le fichier Final.pem d'une autorité de certification tierce](#)

[Étape 3 Interface de commande en ligne \(CLI\). Télécharger le certificat tiers sur le contrôleur WLC avec l'interface de commande en ligne \(CLI\)](#)

[Étape 3 Interface graphique utilisateur \(GUI\). Télécharger le certificat tiers sur le contrôleur WLC avec l'interface graphique utilisateur \(GUI\)](#)

[Dépannage](#)

[Considérations relatives à la haute disponibilité \(haute disponibilité SSO\)](#)

[Informations connexes](#)

Introduction

Ce document décrit comment générer et importer des certificats sur des WLC AireOS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le contrôleur WLC, le point d'accès allégé (LAP) et la carte client sans fil pour le fonctionnement de base.
- Comment utiliser l'application OpenSSL.
- Infrastructures à clé publique et certificats numériques

Composants utilisés

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

- Cisco 5508 WLC exécutant la version du micrologiciel 8.3.102
- Application OpenSSL pour Microsoft Windows
- Outil d'inscription propre à l'autorité de certification tierce

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.

Certificats en chaîne

Une chaîne de certificats est une séquence de certificats dans laquelle chaque certificat de la chaîne est signé par le certificat suivant.

L'objectif d'une chaîne de certificats est d'établir une chaîne de confiance entre un certificat homologue et un certificat d'autorité de certification de confiance. L'autorité de certification se porte garante de l'identité dans le certificat homologue lorsqu'il est signé.

Si l'autorité de certification est de confiance (indiquée par la présence d'une copie du certificat de l'autorité de certification dans votre répertoire de certificat racine), cela implique que vous pouvez également faire confiance au certificat homologue signé.

Souvent, les clients n'acceptent pas les certificats, car ces derniers n'ont pas été créés par une autorité de certification connue. Le client indique généralement que la validité du certificat ne peut pas être vérifiée.

C'est le cas lorsque le certificat est signé par une autorité de certification intermédiaire, qui n'est pas connue du navigateur client. Dans ce cas, vous devez utiliser un certificat SSL ou un groupe de certificats en chaîne.

Prise en charge des certificats en chaîne

Le contrôleur permet de télécharger le certificat d'appareil en tant que certificat en chaîne pour l'authentification Web.

Niveaux de certificat

- Niveau 0 - Utilisation d'un seul certificat de serveur sur le contrôleur WLC
- Niveau 1 - Utilisation d'un certificat de serveur sur le contrôleur WLC et d'un certificat racine de l'autorité de certification
- Niveau 2 - Utilisation d'un certificat de serveur sur le contrôleur WLC, d'un seul certificat intermédiaire de l'autorité de certification et d'un certificat racine de l'autorité de certification
- Niveau 3 - Utilisation d'un certificat de serveur sur le contrôleur WLC, de deux certificats intermédiaires de l'autorité de certification et d'un certificat racine de l'autorité de certification

Le contrôleur WLC ne prend pas en charge les certificats en chaîne de plus de 10 Ko sur le

contrôleur WLC. Toutefois, cette restriction a été supprimée dans la version 7.0.230.0 et les versions ultérieures du contrôleur WLC.

 Remarque : les certificats enchaînés sont pris en charge et réellement requis pour l'authentification Web et l'administration Web.

 Remarque : les certificats génériques sont entièrement pris en charge pour l'authentification EAP, la gestion ou Web locale.

Les certificats d'authentification Web peuvent être soit :

- En chaîne
- Non en chaîne
- Générés automatiquement

 Remarque : dans les versions 7.6 et ultérieures du WLC, seuls les certificats chaînés sont pris en charge (et donc requis).

Pour générer un certificat non chaîné à des fins de gestion, ce document et ignorent les parties où le certificat est combiné avec le certificat CA.

Ce document explique comment installer correctement un certificat SSL en chaîne sur un contrôleur WLC.

Étape 1. Générer une requête de signature de certificat (CSR)

Il existe deux façons de générer une requête de signature de certificat (CSR). Soit manuellement avec OpenSSL (le seul moyen possible dans le logiciel WLC pré-8.3) ou aller sur le WLC lui-même pour générer le CSR (Disponible après 8.3.102).

Option A. CSR avec OpenSSL

 Remarque : Chrome version 58 et ultérieure ne fait pas confiance au nom commun du certificat seul et nécessite un autre nom de sujet pour être également présent. La section suivante explique comment ajouter des champs SAN au CSR OpenSSL, une nouvelle exigence pour ce navigateur.

Terminez ces étapes afin de générer une requête de signature de certificat (CSR) avec OpenSSL :

1. Installez et ouvrez OpenSSL.

Dans Microsoft Windows, par défaut, openssl.exe se trouve à l'adresse C:\ > openssl > bin.



Remarque : OpenSSL Version 0.9.8 est la version recommandée pour les anciennes versions de WLC ; cependant, à partir de la version 7.5, la prise en charge d'OpenSSL Version 1.0 a également été ajoutée (référez-vous à l'ID de bogue Cisco [CSCti65315](#) - Besoin de prise en charge pour les certificats générés avec OpenSSL v1.0) et est la version recommandée à utiliser. OpenSSL 1.1 fonctionne également et fonctionne sur les versions 8.x et ultérieures du WLC.

2. Localisez votre fichier de configuration OpenSSL et faites-en une copie afin de le modifier pour cette requête de signature de certificat (CSR). Modifiez la copie pour ajouter les sections suivantes :

3.

```
[req]
req_extensions = v3_req

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

Les lignes qui commencent par "DNS.1", "DNS.2" (et ainsi de suite) doivent contenir tous les noms secondaires de vos certificats. Ensuite, écrivez toute URL possible utilisée pour le WLC. Les lignes en gras de l'exemple précédent n'étaient pas présentes ou ont été commentées dans notre version openssl de travaux pratiques. Il peut varier considérablement selon le système d'exploitation et la version d'openssl. Nous enregistrons cette version modifiée de la configuration sous le nom openssl-san.cnf pour cet exemple.

4. Entrez cette commande afin de générer un nouveau CSR :

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



Remarque : les WLC prennent en charge une taille de clé maximale de 4 096 bits à partir de la version 8.5 du logiciel.

5. Une invite vous invite à saisir des informations : nom du pays, état, ville, etc. Fournissez les renseignements requis.



Remarque : il est important de fournir le nom commun correct. Assurez-vous que le nom d'hôte utilisé pour créer le certificat (nom commun) correspond à l'entrée de nom d'hôte du système de noms de domaine (DNS) pour l'adresse IP de l'interface virtuelle sur le contrôleur WLC et que le nom existe également dans le DNS. En outre, après avoir apporté les modifications à l'interface IP virtuelle (VIP), vous devez redémarrer le système pour que ces modifications prennent effet.

Voici un exemple :

```
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. Vous pouvez vérifier le CSR (en particulier pour les attributs SAN presenceE) avec `openssl req -text -noout -in csrfilename`.
7. Une fois que vous avez fourni tous les détails requis, deux fichiers sont générés :
 - Nouvelle clé privée qui inclut le nom `mykey.pem`.
 - Un CSR qui inclut le nom `myreq.pem`.

Option B. CSR généré par le WLC

Si votre WLC exécute le logiciel version 8.3.102 ou ultérieure, l'option la plus sécurisée est d'utiliser le WLC pour générer le CSR. L'avantage est que la clé est générée sur le WLC et ne quitte jamais le WLC ; par conséquent, n'est jamais exposée dans le monde extérieur.

Jusqu'à présent, cette méthode ne permet pas de configurer le SAN dans le CSR, ce qui a conduit à des problèmes avec certains navigateurs qui nécessitent la présence d'un attribut SAN. Certaines autorités de certification permettent d'insérer des champs SAN au moment de la signature. Il est donc conseillé de vérifier auprès de votre autorité de certification.

La génération CSR par le WLC lui-même utilise une taille de clé de 2048 bits et la taille de clé ecDSA est de 256 bits.

 Remarque : si vous exécutez la commande `csr generation` et n'installez pas encore le certificat suivant, votre WLC est rendu complètement inaccessible sur HTTPS au prochain redémarrage, car le WLC utilise la clé CSR nouvellement générée après le redémarrage mais n'a pas le certificat qui va avec.

Pour générer un CSR pour l'authentification Web, entrez la commande suivante :

```
(WLC)> config certificate generate csr-webauth BE BR Brussels Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwwZTELMAkGA1UECAwCQlIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVVEFDMSUwLwYDVQQDDDBxteXdIYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKC
AQEAnssc0BxIJ2ULa3xgJH5IAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMIhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwdIx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIEIL2DSwVzjlb9u7T5JRGgqri1I9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nulnmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3ls4+5Jw6ZQAaqIPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

Afin de générer un CSR pour le webadmin, la commande passe à :

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

 Remarque : le CSR est imprimé sur le terminal après que vous ayez entré la commande. Il n'y a pas d'autres façons de le récupérer ; il n'est pas possible de le télécharger à partir du WLC ni de l'enregistrer. Vous devez la copier/coller dans un fichier sur votre ordinateur après avoir saisi la commande. La clé générée reste sur le contrôleur WLC jusqu'à ce que la prochaine requête de signature de certificat (CSR) soit générée (la clé est donc remplacée).

 Si vous devez changer le matériel du WLC ultérieurement (RMA), vous ne pourrez pas réinstaller le même certificat qu'une nouvelle clé et CSR est généré sur le nouveau WLC.

Vous devez ensuite remettre cette requête de signature de certificat (CSR) à votre autorité de signature tierce ou à votre infrastructure à clé publique (PKI).

Étape 2. Obtenir la signature du certificat

Option A : Obtenez le fichier Final.pem auprès de l'autorité de certification de votre entreprise

Cet exemple présente uniquement une autorité de certification d'entreprise actuelle (Windows Server 2012 dans cet exemple) et ne couvre pas les étapes de configuration d'une autorité de certification Windows Server à partir de zéro.

1. Accédez à la page de l'autorité de certification de l'entreprise dans le navigateur (habituellement <https://<CA-ip>/certsrv>) et cliquez sur Request a certificate (demander un certificat).

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

2. Cliquez sur Advanced certificate request (requête de certificat avancée).

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

3. Entrez la requête de signature de certificat (CSR) que vous avez obtenu du contrôleur WLC ou d'OpenSSL. Dans la liste déroulante Certificate Template (modèle de certificat), choisissez Web Server (serveur Web).

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request into the Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5dNq1CWxRFmKhAm00fGQkUoP1YhJRxi du+0T8O46
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc./wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

4. Cliquez sur le bouton radio Base 64 encodedron.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

5. Si le certificat téléchargé est de type PKCS7 (.p7b), convertissez-le en PEM (dans l'exemple suivant, la chaîne de certificats a été téléchargée sous le nom de fichier « All-certs.p7b ») :

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

6. Combinez les certificats de la chaîne de certificats (dans cet exemple, il s'appelle « All-certs.pem ») avec la clé privée générée avec le CSR (la clé privée du certificat de périphérique, qui est mykey.pem dans cet exemple) si vous avez choisi l'option A (OpenSSL pour générer le CSR), et enregistrez le fichier sous le nom final.pem. Si vous avez généré le CSR directement à

partir du WLC (option B), ignorez cette étape.

Entrez ces commandes dans l'application OpenSSL afin de créer les fichiers All-certs.pem et final.pem :

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem  
-out All-certs.p12 -clcerts -passin pass:check123  
-passout pass:check123
```

```
openssl>pkcs12 -in All-certs.p12 -out final.pem  
-passin pass:check123 -passout pass:check123
```

 Remarque : dans cette commande, vous devez entrer un mot de passe pour les paramètres -passin et -passout. Le mot de passe configuré pour le paramètre -passout doit correspondre au paramètre certpassword configuré sur le contrôleur WLC. Dans cet exemple, le mot de passe configuré pour les paramètres -passin et -passout est check123.

Final.pem est le fichier à télécharger sur le WLC si vous avez suivi «Option A. CSR avec OpenSSL».

Si vous avez suivi « Option B. CSR généré par le WLC lui-même », alors All-certs.pem est le fichier à télécharger sur le WLC. L'étape suivante consiste à télécharger ce fichier sur le contrôleur WLC.

 Remarque : si le téléchargement du certificat vers le WLC échoue, vérifiez qu'il y a toute la chaîne dans le fichier pem. Reportez-vous à l'étape 2 de l'option B (obtenir le fichier final.pem auprès d'une autorité de certification tierce) pour voir à quoi il doit ressembler. Si vous ne voyez qu'un seul certificat dans le fichier, vous devez télécharger manuellement tous les fichiers de certificat d'autorité de certification intermédiaire et racine, et les ajouter (par simple copier-coller) au fichier pour créer la chaîne.

Option B : Obtenir le fichier Final.pem d'une autorité de certification tierce

1. Copiez et collez les informations de la requête de signature de certificat (CSR) dans n'importe quel outil d'inscription d'une autorité de certification.

Après votre soumission de la requête de signature de certificat (CSR) à l'autorité de certification tierce, cette dernière signe numériquement le certificat et renvoie la chaîne de certificats signée par courriel. Dans le cas de certificats en chaîne, vous recevez toute la

chaîne de certificats de l'autorité de certification. Si vous n'avez qu'un seul certificat intermédiaire, comme dans cet exemple, vous recevez ces trois certificats de l'autorité de certification :

- Root certificate.pem
- Intermediate certificate.pem
- Device certificate.pem



Remarque : assurez-vous que le certificat est compatible Apache avec le cryptage SHA1 (Secure Hash Algorithm 1).

2. Une fois que vous avez les trois certificats, copiez et collez le contenu de chaque fichier .pem dans un autre fichier dans cet ordre :

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

3. Enregistrez le fichier sous All-certs.pem.

4. Combinez le certificat All-certs.pem avec la clé privée générée avec le CSR (la clé privée du certificat du périphérique, qui est mykey.pem dans cet exemple) si vous avez utilisé l'option A (OpenSSL pour générer le CSR) et enregistrez le fichier sous le nom final.pem. Si vous avez généré le CSR directement à partir du WLC (option B), ignorez cette étape.

Entrez ces commandes dans l'application OpenSSL afin de créer les fichiers All-certs.pem et final.pem :

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123
```

```
openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```



Remarque : dans cette commande, vous devez entrer un mot de passe pour les paramètres -passin et -passout. Le mot de passe configuré pour le paramètre -passout

 doit correspondre au paramètre certpassword configuré sur le contrôleur WLC. Dans cet exemple, le mot de passe configuré pour les paramètres -passin et -passout est check123.

Final.pem est le fichier à télécharger sur le WLC si vous avez suivi «Option A. CSR avec OpenSSL». Si vous avez suivi « Option B. CSR généré par le WLC lui-même », alors All-certs.pem est le fichier que vous devez télécharger sur le WLC. L'étape suivante consiste à télécharger ce fichier sur le contrôleur WLC.

 Remarque : SHA2 est également pris en charge. L'ID de bogue Cisco [CSCuf20725](#) est une demande de prise en charge de SHA512.

Étape 3 Interface de commande en ligne (CLI). Télécharger le certificat tiers sur le contrôleur WLC avec l'interface de commande en ligne (CLI)

Complétez ces étapes pour télécharger le certificat enchaîné sur le WLC avec l'interface de ligne de commande :

1. Déplacez le fichier final.pem vers le répertoire par défaut sur votre serveur TFTP.
2. Dans l'interface de ligne de commande, entrez ces commandes afin de modifier les paramètres de téléchargement :

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

3. Saisissez le mot de passe pour le fichier .pem afin que le système d'exploitation puisse décrypter la clé et le certificat SSL.

```
>transfer download certpassword password
```

 Remarque : assurez-vous que la valeur de certpassword est identique au mot de passe du paramètre -passout qui a été défini à l'étape 4 (ou 5) de la section [Generate a CSR](#). Dans cet exemple, le mot de passe de certification doit être check123. Si vous



avez choisi l'option B (c'est-à-dire, utiliser le WLC lui-même pour générer le CSR), laissez le champ certpassword vide.

4. Entrez la `transfer download start` commande afin d'afficher les paramètres mis à jour. Ensuite, entrez `y` lorsque vous serez invité à le faire afin de confirmer les paramètres de téléchargement actuels et de commencer le téléchargement du certificat et de la clé. Voici un exemple :

```
(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. Redémarrez le contrôleur WLC pour que les modifications prennent effet.

Étape 3 Interface graphique utilisateur (GUI). Télécharger le certificat tiers sur le contrôleur WLC avec l'interface graphique utilisateur (GUI)

Complétez ces étapes pour télécharger le certificat enchaîné sur le WLC avec l'interface graphique utilisateur :

1. Copiez le certificat de périphérique `final.pem` dans le répertoire par défaut de votre serveur TFTP.
2. Choisissez `Security > Web Auth > Cert` pour ouvrir la page `Web Authentication Certificate`.
3. Cochez la case `Download SSL Certificate` (télécharger le certificat SSL) pour afficher les paramètres `Download SSL Certificate From TFTP Server` (télécharger le certificat SSL à partir du serveur TFTP).
4. Dans le champ `IP Adress` (adresse IP), saisissez l'adresse IP du serveur TFTP.



5. Dans le champ File Path (chemin d'accès au fichier), saisissez le chemin d'accès au répertoire du certificat.
6. Dans le champ File Name (nom de fichier), saisissez le nom du certificat.
7. Dans le champ Certificate Password (mot de passe du certificat), saisissez le mot de passe utilisé pour protéger le certificat.
8. Cliquez sur Apply.
9. Une fois le téléchargement terminé, choisissez Commands > Reboot > Reboot (commandes > redémarrer > redémarrer).
10. Si vous êtes invité à enregistrer vos modifications, cliquez sur Save and Reboot (enregistrer et redémarrer).
11. Cliquez sur OK pour confirmer votre décision de redémarrer le contrôleur.

Dépannage

Afin de dépanner l'installation du certificat sur le WLC, ouvrez une ligne de commande sur le WLC et entrez `debug transfer all enable debug pm pki enable` puis terminez la procédure de téléchargement du certificat.

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.
```

Vérifiez le format et la chaîne du certificat. N'oubliez pas que les WLC ultérieurs à la version 7.6 nécessitent la présence de toute la chaîne, de sorte que vous ne pouvez pas télécharger votre certificat WLC seul. La chaîne jusqu'à l'autorité de certification racine doit être présente dans le fichier.

Voici un exemple de débogage lorsque l'autorité de certification intermédiaire est inexacte :

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using password check1
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password check1
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*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 1
*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: unabl
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 dept
*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 (verifyC
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

Considérations relatives à la haute disponibilité (haute disponibilité SSO)

Comme expliqué dans le guide de déploiement de la haute disponibilité SSO du contrôleur WLC, les certificats ne sont pas répliqués du contrôleur principal au contrôleur secondaire dans un scénario de haute disponibilité SSO.

Cela signifie que vous devez importer tous les certificats dans le secondaire avant de former la paire haute disponibilité.

Une autre mise en garde est que cela ne fonctionne pas si vous avez généré le CSR (et donc créé la clé localement) sur le WLC principal parce que cette clé ne peut pas être exportée.

La seule manière est de générer la requête de signature de certificat CSR pour le contrôleur WLC primaire avec OpenSSL (et donc avoir la clé attachée au certificat) et d'importer cette combinaison

certificat/clé sur les deux contrôleurs WLC.

Informations connexes

- [Générer une requête de signature de certificat \(CSR\) pour un certificat de tiers sur un système Wireless Control System \(WCS\)](#)
- [Exemple de configuration d'une demande de signature de certificat \(CSR\) pour un contrôleur de réseau local sans fil \(WCS\) sur un serveur Linux](#)
- [Assistance et documentation techniques - Cisco Systems](#)
- [Guide de haute disponibilité SSO du contrôleur WLC](#)

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.