Génération d'une demande CSR pour des certificats tiers et téléchargement des certificats chaînés sur le contrôleur de réseau local sans fil

Contenu

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) afin d'obtenir un tiers certificat et comment télécharger un certificat enchaîné à un contrôleur Sans fil du RÉSEAU LOCAL (WLAN) (WLC).

Conditions préalables

Exigences

Avant que vous tentiez cette configuration, vous devriez avoir la connaissance de ces thèmes :

- Comment configurer le WLC, le point d'accès léger (LAP), et la carte de client sans fil pour le fonctionnement de base
- Comment utiliser l'application d'OpenSSL
- Infrastructure de 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 qui exécute la version 8.3.102 de micrologiciels
- Demande d'OpenSSL de Microsoft Windows
- Outil d'inscription qui est spécifique à la tiers autorité de certification (le CA)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Certificats enchaînés

Une chaîne de certificat est un ordre des Certificats, où chaque certificat dans la chaîne est signé par le certificat ultérieur. Le but d'une chaîne de certificat est d'établir une chaîne de confiance d'un certificat de pair à un certificat de CA de confiance. Le CA garantit pour l'identité dans le certificat de pair quand il la signe. Si le CA est un au lequel vous faites confiance, qui est indiqué par la présence d'une copie du certificat de CA dans votre répertoire de certificat racine, ceci vous implique peut faire confiance au certificat signé de pair aussi bien.

Souvent, les clients ne reçoivent pas les Certificats parce qu'ils n'ont pas été créés par un CA connu. Le client déclare typiquement que la validité du certificat ne peut pas être vérifiée. C'est le cas quand le certificat est signé par un intermédiaire CA, qui n'est pas connu au navigateur de client. En pareil cas, il est nécessaire d'utiliser un certificat ssl enchaîné ou de délivrer un certificat le groupe.

Soutien de certificat enchaîné

Le contrôleur tient compte pour que le certificat de périphérique soit téléchargé comme certificat enchaîné pour l'authentification Web.

Niveaux de certificat

- Niveau 0 - Utilisation d'un certificat seulement de serveur sur le WLC
- Niveau 1 - Utilisation d'un certificat de serveur sur le WLC et un certificat racine CA
- Niveau 2 - Utilisation d'un certificat de serveur sur le WLC, d'un certificat intermédiaire simple CA, et d'un certificat racine CA
- Niveau 3 - Utilisation d'un certificat de serveur sur le WLC, deux Certificats intermédiaires CA, et un certificat racine CA

Le WLC ne le prend en charge pas enchaîné délivre un certificat plus que 10KB dans la taille sur le WLC. Cependant, cette restriction a été retirée dans la version 7.0.230.0 WLC et plus tard.

> **Note**: Des Certificats enchaînés sont pris en charge pour l'authentification Web seulement ; ils ne sont pas pris en charge pour le certificat de Gestion.

> **Note**: Des Certificats de masque sont entièrement pris en charge pour l'EAP local, la Gestion ou le webauthentication

Les Certificats d'authentification Web peuvent être l'un de ces :

- Enchaîné
- Désenchaîné
- Automatique-généré

Note: Dans la version 7.6 et ultérieures WLC, seulement des Certificats enchaînés sont pris en charge dans le WLC pour l'authentification Web.

Si vous regardez pour générer un certificat désenchaîné pour le but de Gestion, vous pouvez suivre ce document et ignorer les pièces où le certificat est combiné avec le certificat de CA.

Ce document discute comment installer correctement un certificat enchaîné de Protocole SSL (Secure Socket Layer) sur un WLC.

Étape 1. Générez un CSR

Il y a deux manières de générer un CSR. Manuellement avec OpenSSL (la seule manière possible en logiciel pre-8.3 WLC) ou employer le WLC lui-même pour générer le CSR (disponible après 8.3.102).

CSR de l'option A. avec OpenSSL

Note: La version 58 et ultérieures de Chrome ne fait pas confiance au nom commun seul du certificat et exige du nom secondaire soumis d'être également présent. La section suivante expliquera comment ajouter des champs SAN au CSR d'OpenSSL qui est une nouvelle condition requise pour ce navigateur.

Terminez-vous ces étapes afin de générer un CSR avec OpenSSL :

1. Installez et ouvrez l'OpenSSL.

   Dans Microsoft Windows, par défaut, openssl.exe se trouve à C:\ **> à l'openssl > au coffre.**

   Note: La version 0.9.8 d'OpenSSL est la version recommandée pour de vieilles versions WLC ; cependant, en date de la version 7.5, le soutien de la version 1.0 d'OpenSSL a été également ajouté (référez-vous à l'ID de bogue Cisco CSCti65315 - soutien du besoin des Certificats générés utilisant OpenSSL v1.0) et est la version recommandée à l'utiliser. OpenSSL 1.1 travail a été également testé et fonctionne grand sur 8.x et releases postérieures WLC.
2. Localisez votre fichier de config d'OpenSSL et tirez une copie de elle afin de l'éditer pour ce CSR. Éditez 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 commençant par "DNS.1", "DNS.2" et ainsi de suite devraient contenir tous les noms secondaires que vos Certificats auront. Vous pouvez alors écrire n'importe quel URL possible que vous utiliserez pour le WLC. Les lignes dans ci-dessus gras n'étaient pas présentes ou ont été commentées dans notre version d'openSSL de laboratoire, elle peut varier considérablement selon le système d'exploitation et la version d'openssl. Nous sauvegardons cette version modifiée du config comme **openssl-san.cnf pour** cet exemple.

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

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

Note: Support de WLCs une taille de clé maximum de 2,048 bits.

5. Après que vous émettiez la commande, il y a une demande pour quelques informations : nom du pays, état, ville, et ainsi de suite. Fournissez l'information requise.

Note: Il est important que vous fournissiez le nom commun correct. Assurez-vous que le nom d'hôte qui est utilisé pour créer le certificat (nom commun) apparie l'entrée de nom d'hôte de Système de noms de domaine (DNS) pour l'adresse IP d'interface virtuelle sur le WLC et que le nom existe dans les DN aussi bien. En outre, après que vous apportiez la modification à l'interface virtuelle IP (VIP), vous devez redémarrer le système pour que cette modification la prenne effet.

Voici un exemple :

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
```

```
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:OpenSSL>
```

6. Vous pouvez vérifier le CSR (particulièrement pour le SAN attribue la présence) avec le **req d'openssl - texte - noout - dans le csrfilename**
7. Après que vous fournissiez tous les détails priés, deux fichiers sont générés :

   une nouvelle clé privée qui inclut le nom **mykey.pem**un CSR qui inclut le nom **myreq.pem**

Option B. CSR Generated par le WLC

Si votre WLC exécute la version de logiciel 8.3.102 ou plus tard, le plus option (et le plus facile sécurisés trop) est d'employer le WLC pour générer le CSR. L'avantage est que la clé est générée sur le WLC et ne laisse jamais le WLC ; ainsi n'est jamais exposé dans le monde extérieur.

Dorénavant, cette méthode ne laisse pas configurer le SAN dans le CSR qui pourrait mener aux questions avec certains navigateurs qui exige la présence d'un attribut SAN. Un certain CA laissent insérer des champs SAN au temps de signature, ainsi c'est une bonne idée de vérifier avec votre CA.

Générant le CSR par le WLC lui-même utilisera une taille de clé de 2048 bits et la taille de clé d'ecdsa sera 256 bits.

> **Note**: Si vous exécutez la commande de génération csr et n'installez pas le certificat en résultant encore, votre WLC sera complètement inaccessible sur HTTPS à la prochaine réinitialisation, car le WLC utilisera la clé nouvellement générée CSR après que la réinitialisation mais n'ait pas le certificat qui est assorti à elle.

Afin de générer un CSR pour l'authentification Web, sélectionnez cette commande :

Le certificat du >config (WLC) **génèrent le csr-webauth SOIT BR Bruxelles Cisco TAC mywebauthportal.wireless.com tac@cisco.com**

-----COMMENCEZ LA DEMANDE DE CERTIFICAT-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=

-----DEMANDE DE CERTIFICAT D'EXTRÉMITÉ-----

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

Le certificat du >config (WLC) **génèrent le csr-webadmin SOIT BR Bruxelles Cisco TAC mywebauthportal.wireless.com tac@cisco.com**

> **Note**: Le CSR est imprimé sur le terminal après que vous sélectionniez la commande. Il n'y a aucune autre manière de le récupérer ; il n'est pas possible de le télécharger du WLC ni est il possible de le sauvegarder. Vous devez copier/pâte il sur un fichier sur votre ordinateur après que vous sélectionniez la commande. La clé générée reste sur le WLC jusqu'à ce que le prochain CSR soit généré (la clé est ainsi remplacée). Si vous jamais devez changer le matériel WLC plus tard (RMA), vous ne pourrez pas réinstaller le même certificat qu'une nouveaux clé et CSR devront être généré sur le nouveau WLC.

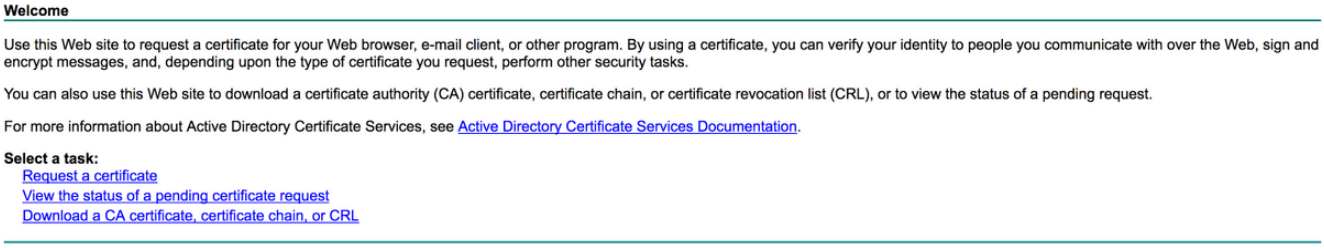
Vous alors devez remettre ce CSR à votre tiers autorité de signature ou à votre Infrastructure à clés publiques (PKI) d'entreprise.

Étape 2. Obtenez le certificat signé

Option A : Obtenez le fichier Final.pem de votre entreprise CA

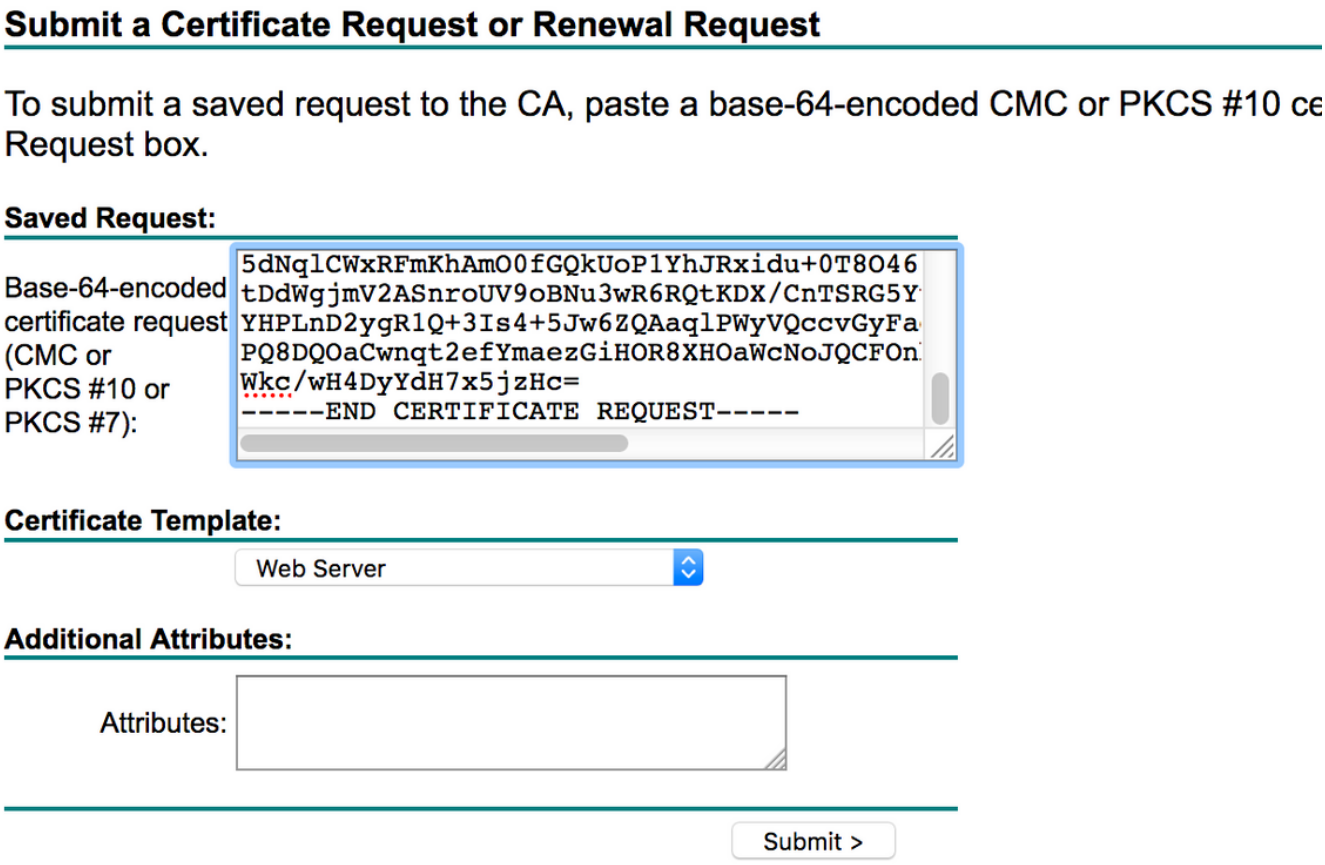
Cet exemple présente seulement une entreprise existante CA (Windows Server 2012 dans cet exemple) et ne couvre pas les étapes pour installer un à partir de zéro des Windows Server CA.

1. Allez à votre page de l'enteprrise CA dans le navigateur (habituellement https:// <CA-ip>/certsrv) et cliquez sur la **demande un certificat**.

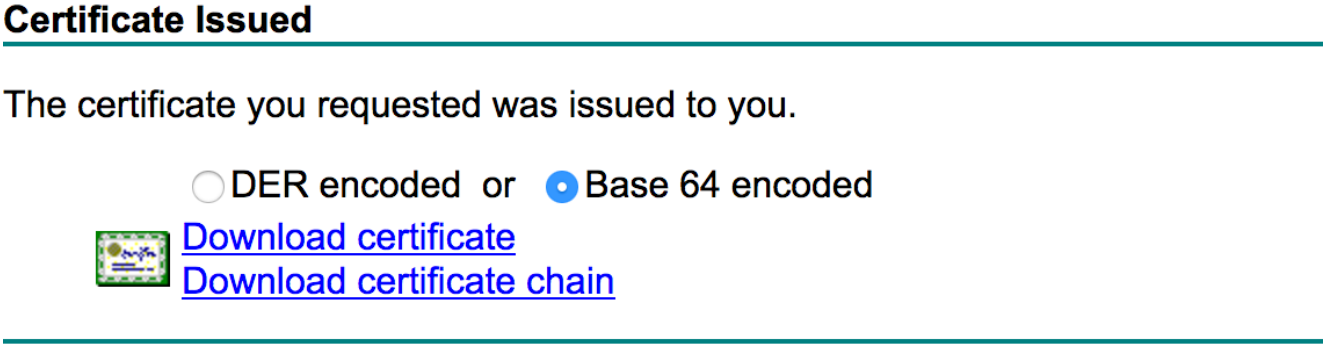


2. **Demande de certificat avancée par** clic.

3. Écrivez le CSR que vous avez obtenu du WLC ou de l'OpenSSL. Dans la liste déroulante de modèle de certificat, choisissez le **serveur Web**.



4. Cliquez sur la case d'option **encodée de la base 64**.



5. Si le certificat téléchargé est du type PKCS7 (.p7b), alors vous devez le convertir en PEM (dans l'exemple ci-dessous nous avons téléchargé la chaîne de certificat comme nom du fichier "All-certs.p7b") :

openssl pkcs7 - print_certs - dans All-certs.p7b - All-certs.pem

6. Combinez Certificats de chaîne de certificat (dans cet exemple, c'est nommé les « All-certs.pem ») avec la clé privée que vous avez générée avec le CSR (la clé privée du certificat de périphérique, qui est mykey.pem dans cet exemple) si vous alliez de pair avec l'option A (c'est-à-dire, vous avez utilisé OpenSSL pour générer le CSR), et sauvegardez le fichier comme final.pem. **Si vous** généries le CSR directement du WLC (option B) vous pouvez ignorer cette étape.

Émettez ces commandes dans l'application d'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
```

> **Note**: Dans cette commande, vous devez entrer un mot de passe pour les paramètres **- passin** et **- passout**. Le mot de passe qui est configuré pour **-** paramètre de **passout** doit apparier le paramètre de **certpassword** qui est configuré sur le WLC. Dans cet exemple, le mot de passe qui est configuré pour **- passin** et **- les** paramètres de **passout** est **check123**.

Final.pem est le fichier que vous devez télécharger au WLC si vous suiviez le « CSR de l'option A. avec OpenSSL ». Si vous suiviez le « CSR de l'option B. généré par le WLC lui-même », alors All-certs.pem est le fichier que vous devez télécharger au WLC. L'étape suivante est de télécharger ce fichier au WLC.

> **Note**: Si le téléchargement du certificat au WLC échoue, il se peut que vous n'ayez pas la chaîne entière dans le fichier PEM. Référez-vous à l'étape 2 de l'option B (obtenez le final.pem d'un tiers CA) ci-dessous de voir comment il devrait ressembler à. Si vous voyez seulement un certificat dans le fichier, alors vous le besoin de télécharger manuellement tous les fichiers de certificat de CA d'intermédiaire et de racine et de les ajouter (par la pâte de simple copie) au fichier pour créer la chaîne.

Option B : Obtenez le fichier Final.pem d'une tierce partie CA

1. Copiez et collez les informations CSR dans n'importe quel outil d'inscription CA.

   Après que vous soumettiez le CSR à la tierce partie CA, la tierce partie CA digitalement signe le certificat et envoie de retour la chaîne de certificat signé par l'email. Dans le cas des Certificats enchaînés, vous recevez la chaîne entière des Certificats du CA. Si vous avez seulement un comme indiqué dans cet exemple intermédiaire de certificat, vous recevez ces trois Certificats du CA :

   Racine certificate.pemIntermédiaire certificate.pemPériphérique certificate.pem**Note**: Assurez-vous que le certificat est Apache-compatible avec le cryptage du Secure Hash Algorithm 1 (SHA1).
2. Une fois que vous avez chacun des trois Certificats, copiez et collez le contenu de chaque fichier .pem dans un autre fichier dans cette commande :

   ```
   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
```

3. Sauvegardez le fichier comme **All-certs.pem.**

4. Combinez le certificat All-certs.pem avec la clé privée que vous avez générée avec le CSR (la clé privée du certificat de périphérique, qui est mykey.pem dans cet exemple) si vous alliez de pair avec l'option A (c'est-à-dire, vous avez utilisé OpenSSL pour générer le CSR), et sauvegardez le fichier comme final.pem**. Si vous** généries le CSR directement du WLC (option B) vous pouvez ignorer cette étape.

   Émettez ces commandes dans l'application d'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
```

   Note: Dans cette commande, vous devez entrer un mot de passe pour les paramètres **- passin** et **- passout**. Le mot de passe qui est configuré pour **-** paramètre de **passout** doit apparier le paramètre de **certpassword** qui est configuré sur le WLC. Dans cet exemple, le mot de passe qui est configuré pour **- passin** et **- les** paramètres de **passout** est **check123**.Final.pem est le fichier que vous devez télécharger au WLC si vous suiviez le « CSR de l'option A. avec OpenSSL ». Si vous suiviez le « CSR de l'option B. généré par le WLC lui-même », alors All-certs.pem est le fichier que vous devez télécharger au WLC. L'étape suivante est de télécharger ce fichier au WLC.

   Note: SHA2 est également pris en charge. L'ID de bogue Cisco CSCuf20725 est une demande du support SHA512.

Étape 3 CLI. Téléchargez le tiers certificat au WLC avec le CLI

Terminez-vous ces étapes afin de télécharger le certificat enchaîné au WLC avec le CLI :

1. Déplacez le **fichier final.pem au** répertoire par défaut sur votre serveur TFTP.

2. Dans le CLI, émettez ces commandes afin de changer les configurations 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. Entrez le mot de passe pour le fichier .pem de sorte que le système d'exploitation puisse

déchiffrer la clé et le certificat SSL.

```
>transfer download certpassword password
```

Note: Soyez que la valeur pour le **certpassword** est identique que **- le** mot de passe sûr de paramètre de **passout** qui a été placé dans l'étape 4 (ou 5) du [générer par](#) section [CSR](#). Dans cet exemple, le **certpassword** doit être **check123**. Si vous aviez choisi l'option B (c'est-à-dire, employez le WLC lui-même pour générer le CSR) que vous pouvez laisser le champ vide de certpassword.

4. Émettez la commande de **transfer download start** afin de visualiser les configurations mises à jour. Écrivez alors **y au** prompt afin de confirmer les configurations en cours de téléchargement et commencer le téléchargement de certificat et de 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 starting.

Certificate installed.
Reboot the switch to use new certificate.
```

5. Redémarrez le WLC pour que les modifications les prennent effet.

Étape 3 GUI. Téléchargez le tiers certificat au WLC avec le GUI

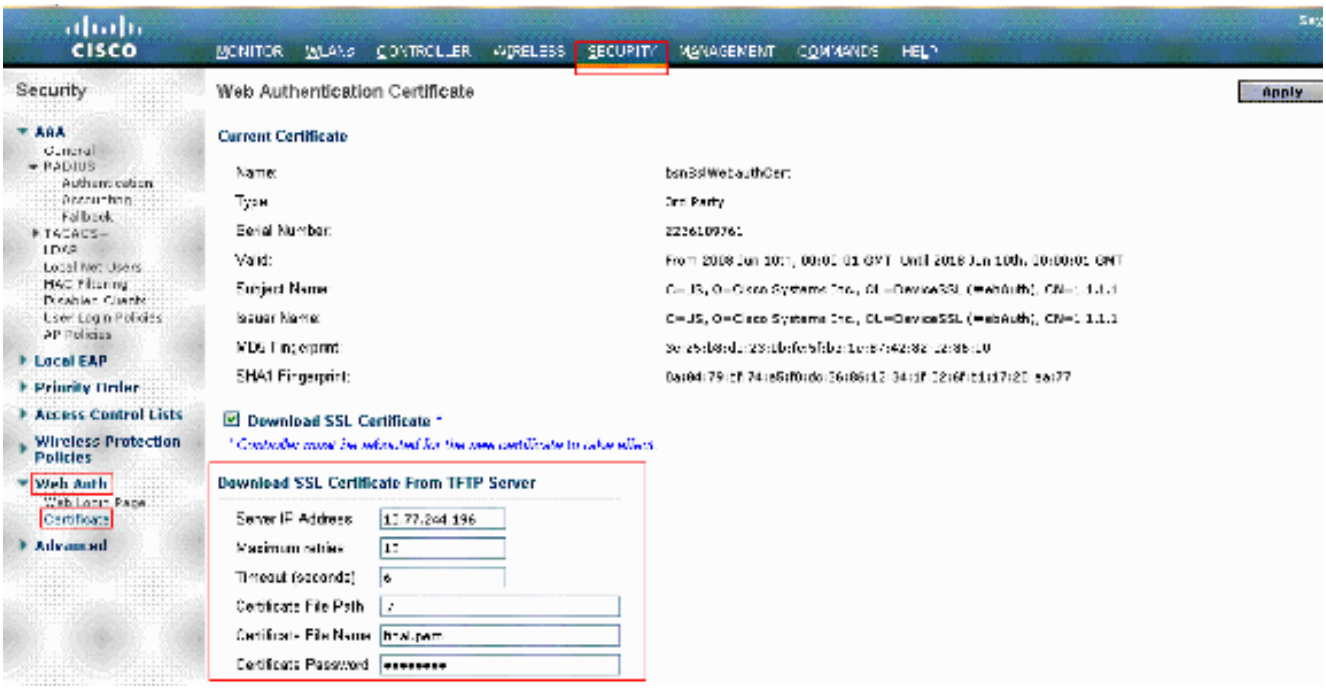
Terminez-vous ces étapes afin de télécharger le certificat enchaîné au WLC avec le GUI :

1. Copiez le certificat final.pem de périphérique sur le répertoire par défaut sur votre serveur TFTP.

2. Choisissez la **Sécurité > le Web authentiques > CERT** afin d'ouvrir la page de certificat d'authentification Web.

3. Cochez la case de **certificat ssl de téléchargement** afin de visualiser le certificat ssl de téléchargement des paramètres de serveur TFTP.

4. Dans le champ IP Address, écrivez l'adresse IP du serveur TFTP.



5. Dans le domaine de chemin de fichier, entrez dans le chemin du répertoire du certificat.

6. Dans le domaine de nom du fichier, écrivez le nom du certificat.

7. Dans le domaine de mot de passe de certificat, entrez le mot de passe qui a été utilisé pour protéger le certificat.

8. Cliquez sur **Apply**.

9. Après que le téléchargement soit complet, choisissez les **commandes > la réinitialisation > la réinitialisation**.

10. S'incité à sauvegarder vos modifications, **sauvegarde de** clic **et réinitialisation**.

11. Cliquez sur OK afin de confirmer votre décision de redémarrer le contrôleur.

Dépanner

Ce qui posera très probablement un problème est l'installation du certificat sur le WLC. Afin de dépanner, ouvrir une ligne de commande sur le WLC et écrire le **debug transfer tout l'enable** et **enable de PKI de debug pm** remplissent alors la procédure de certificat de téléchargement.

```
(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 starting.

Certificate installed.
Reboot the switch to use new certificate.
```

Vous devez vérifier le format de certificat et puis l'enchaînement. Souvenez-vous que WLCs plus tard que la version 7.6 exigent de la chaîne entière d'être présente, ainsi vous pouvez non seulement télécharger votre seul certificat WLC. La chaîne jusqu'à la racine CA doit être présente dans le fichier.

Voici un exemple de met au point quand l'intermédiaire CA est incorrecte :

```
(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 starting.

Certificate installed.
Reboot the switch to use new certificate.
```

Informations connexes

- Générer une demande CSR pour des certificats tiers et télécharger des certificats déchaînés sur le contrôleur de réseau local sans fil (WLC)
- Génération d'une demande de signature de certificat (CSR) pour un certificat tiers sur un contrôleur de réseau local sans fil (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
- Support et documentation techniques - Cisco Systems