# Configurer un téléphone VPN AnyConnect avec authentification de certificat sur un ASA

## Contenu



## Introduction

Ce document fournit un exemple de configuration qui montre comment configurer les périphériques ASA (Adaptive Security Appliance) et CallManager pour fournir une authentification de certificat pour les clients AnyConnect qui s'exécutent sur des téléphones IP Cisco. Une fois cette configuration terminée, les téléphones IP Cisco peuvent établir des connexions VPN à l'ASA qui utilisent des certificats afin de sécuriser la communication.

## Conditions préalables

### Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Licence AnyConnect Premium SSL
- Licence AnyConnect pour téléphone VPN Cisco

Selon la version ASA, vous verrez « AnyConnect for Linksys phone » pour ASA version 8.0.x ou « AnyConnect for Cisco VPN Phone » pour ASA version 8.2.x ou ultérieure.

### Components Used

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

logiciel suivantes :

- ASA - Version 8.0(4) ou ultérieure
- Modèles de téléphone IP - 7942 / 7962 / 7945 / 7965 / 7975
- Téléphones - 8961 / 9951 / 9971 avec microprogramme version 9.1(1)
- Téléphone - Version 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) ou ultérieure
- Cisco Unified Communications Manager (CUCM) - Version 8.0.1.10000-4 ou ultérieure

Les versions utilisées dans cet exemple de configuration sont les suivantes :

- ASA - Version 9.1(1)
- CallManager - Version 8.5.1.1000-26

Pour obtenir la liste complète des téléphones pris en charge dans votre version CUCM, procédez comme suit :

1. Ouvrez cette URL : https:// *<Adresse IP du serveur CUCM>* :8443/cucreports/systemReports.do
2. Choisissez **Liste des fonctionnalités du téléphone Unified CM > Générer un nouvel état > Fonctionnalité : Réseau privé virtuel**.

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. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Types de certificat téléphonique

Cisco utilise ces types de certificat dans les téléphones :

- Certificat installé du fabricant (MIC) : les MIC sont inclus sur tous les téléphones IP Cisco 7941, 7961 et les modèles plus récents. Les MIC sont des certificats de clé de 2 048 bits signés par l'autorité de certification Cisco. Lorsqu'une carte MIC est présente, il n'est pas nécessaire d'installer un certificat LSC (Certificat d'importance locale). Pour que CUCM puisse faire confiance au certificat MIC, il utilise les certificats CA pré-installés CAP-RTP-001, CAP-RTP-002 et Cisco_Manufacturing_CA dans son magasin de certificats.
- LSC : le LSC sécurise la connexion entre CUCM et le téléphone après avoir configuré le mode de sécurité du périphérique pour l'authentification ou le chiffrement.Le LSC possède la clé publique du téléphone IP Cisco, qui est signée par la clé privée CAPF (Certificate Authority Proxy Function) CUCM. Il s'agit de la méthode préférée (par opposition à l'utilisation de MIC), car seuls les téléphones IP Cisco provisionnés manuellement par un administrateur sont autorisés à télécharger et à vérifier le fichier CTL.**Note:** En raison du risque accru pour la sécurité, Cisco recommande l'utilisation de MIC uniquement pour l'installation de LSC et non pour une utilisation continue. Les clients qui configurent des téléphones IP Cisco pour utiliser des MIC pour l'authentification TLS (Transport Layer Security) ou à toute autre fin le font à

leurs propres risques.

# Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Note:** Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Configurations

Ce document décrit les configurations suivantes :

- Configuration ASA
- Configuration de CallManager
- Configuration VPN sur CallManager
- Installation du certificat sur les téléphones IP

### Configuration ASA

La configuration de l'ASA est presque identique à celle d'un ordinateur client AnyConnect connecté à l'ASA. Toutefois, ces restrictions s'appliquent :

- Le groupe de tunnels doit avoir une url de groupe. Cette URL sera configurée dans CM sous l'URL de la passerelle VPN.
- La stratégie de groupe ne doit pas contenir de tunnel partagé.

Cette configuration utilise un certificat ASA (autosigné ou tiers) préalablement configuré et installé dans le point de confiance SSL (Secure Socket Layer) du périphérique ASA. Pour plus d'informations, référez-vous aux documents suivants :

- Configuration des certificats numériques
- Exemple de configuration de l'installation manuelle de certificats de fournisseurs tiers dans ASA 8.x pour une utilisation avec WebVPN
- ASA 8.x : Exemple de configuration de l'accès VPN avec le client VPN AnyConnect à l'aide d'un certificat auto-signé

La configuration appropriée de l'ASA est la suivante :

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

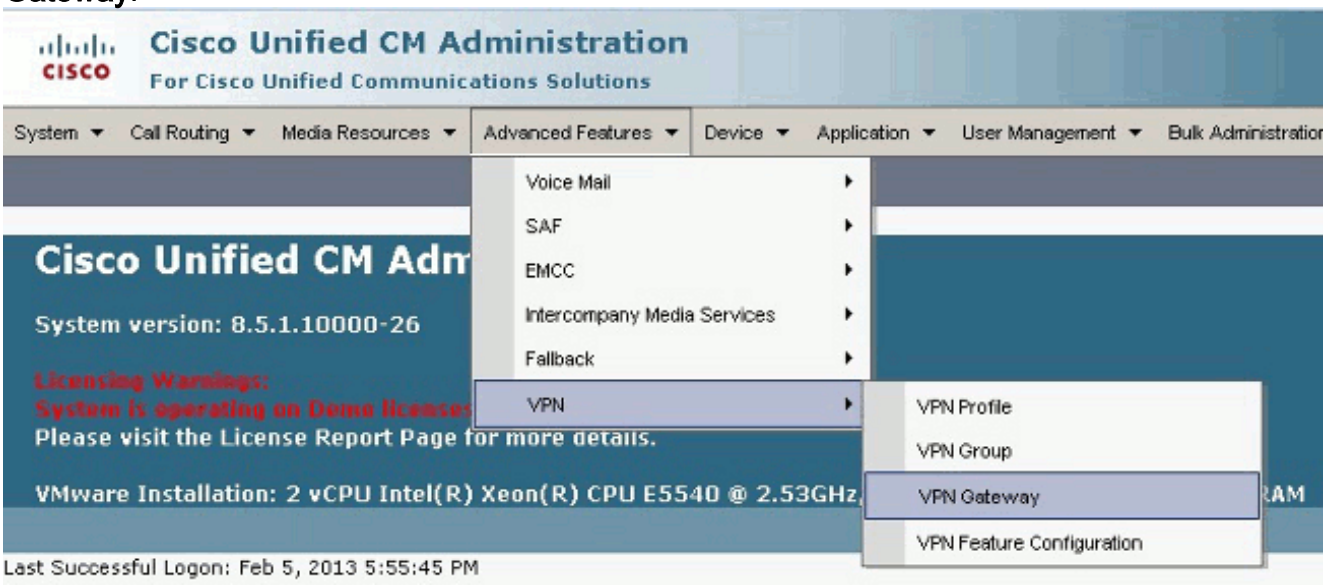
## Configuration de CallManager

Afin d'exporter le certificat de l'ASA et d'importer le certificat dans CallManager en tant que certificat Phone-VPN-Trust, procédez comme suit :

1. Enregistrez le certificat généré avec CUCM.
2. Vérifiez le certificat utilisé pour SSL.
   ```
   ASA(config)#show run ssl
   ssl trust-point SSL outside
   ```
3. Exporter le certificat.
   ```
   ASA(config)#crypto ca export SSL identity-certificate
   ```
   Le certificat d'identité codé PEM (Privacy Enhanced Mail) est le suivant :
   ```
   -----BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
   MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
   NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR
   FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
   wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1
   -----END CERTIFICATE-----
   ```
4. Copiez le texte à partir du terminal et enregistrez-le en tant que fichier .pem.
5. Connectez-vous à CallManager et choisissez **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust** afin de télécharger le fichier de certificat enregistré à l'étape précédente.

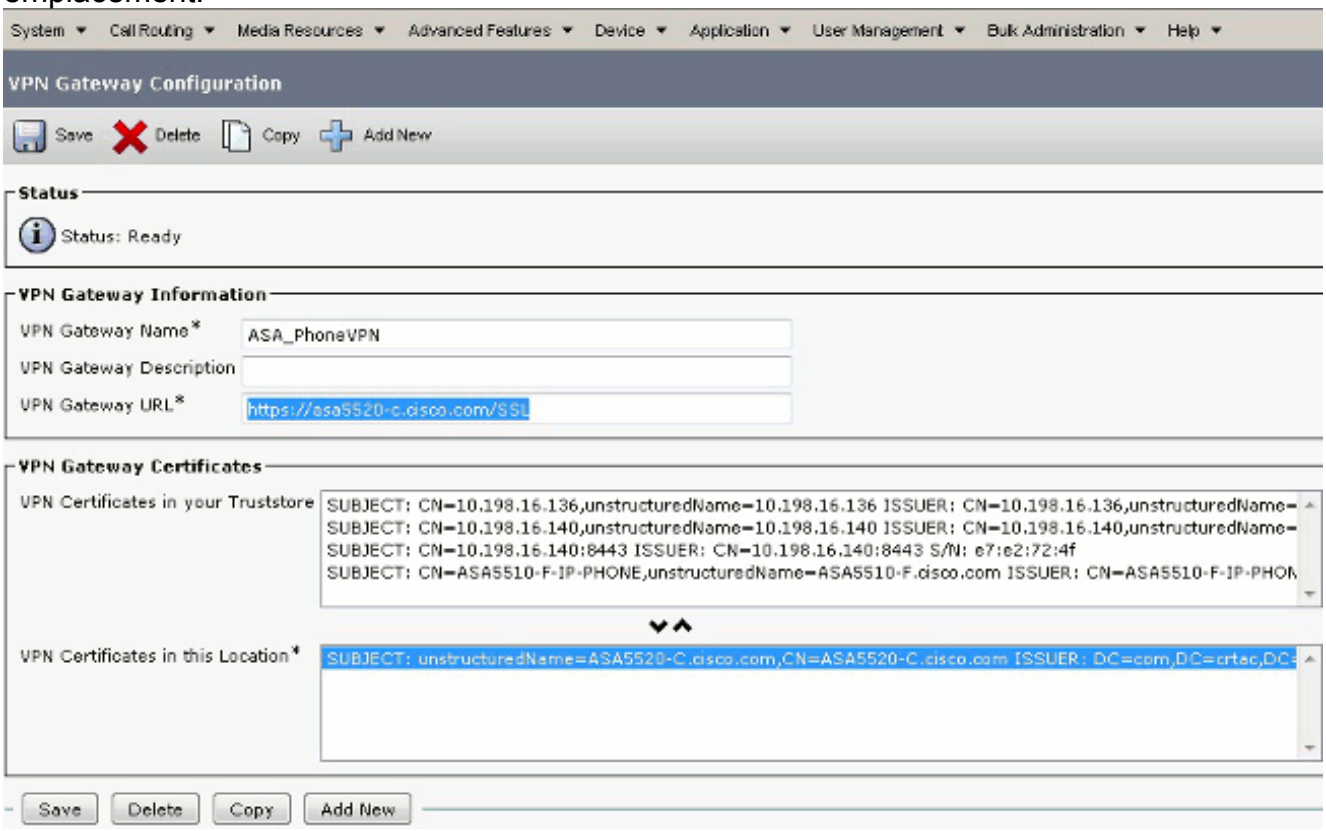
## Configuration VPN sur CallManager

1. Accédez à Cisco Unified CM Administration.
2. Dans la barre de menus, sélectionnez **Advanced Features > VPN > VPN Gateway**.

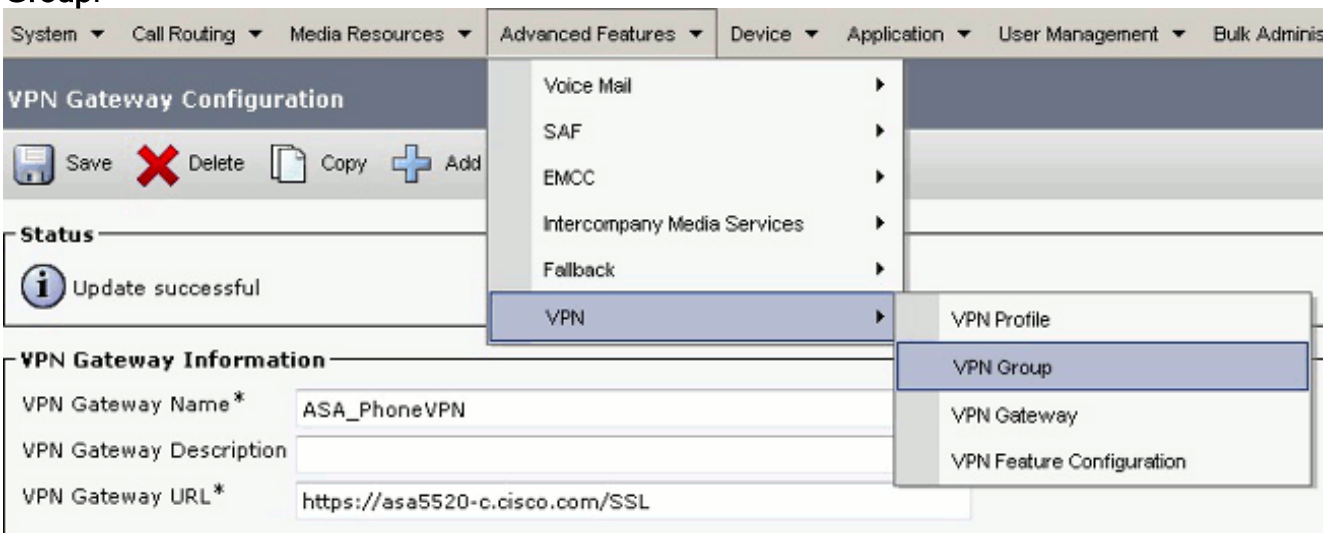



3. Dans la fenêtre VPN Gateway Configuration, procédez comme suit :Dans le champ VPN Gateway Name, saisissez un nom. Il peut s'agir de n'importe quel nom.Dans le champ VPN Gateway Description, saisissez une description (facultatif).Dans le champ VPN Gateway

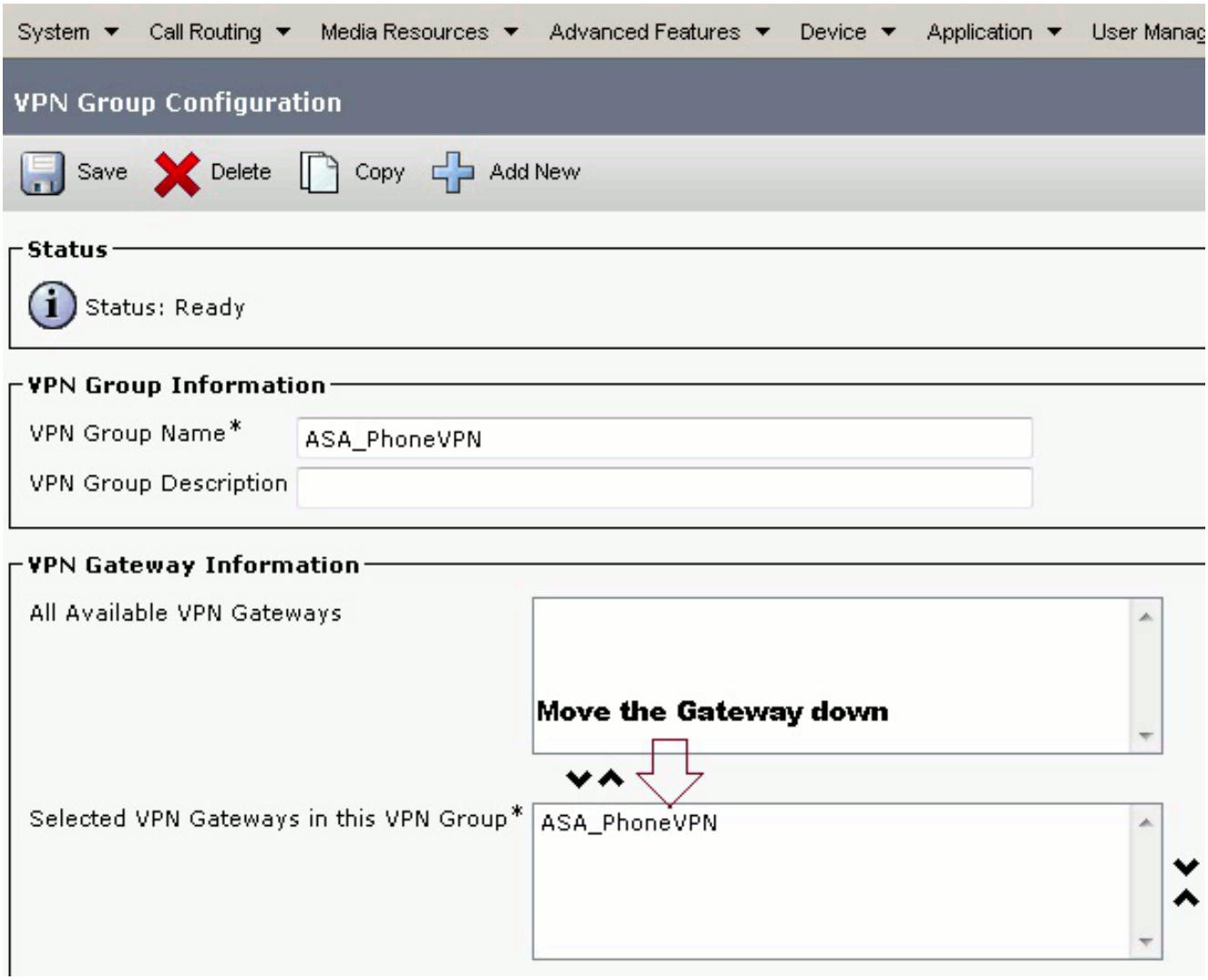
URL, saisissez l'URL de groupe définie sur l'ASA.Dans le champ Certificats VPN de cet emplacement, sélectionnez le certificat qui a été téléchargé précédemment dans CallManager pour le déplacer de la banque de confiance vers cet emplacement.



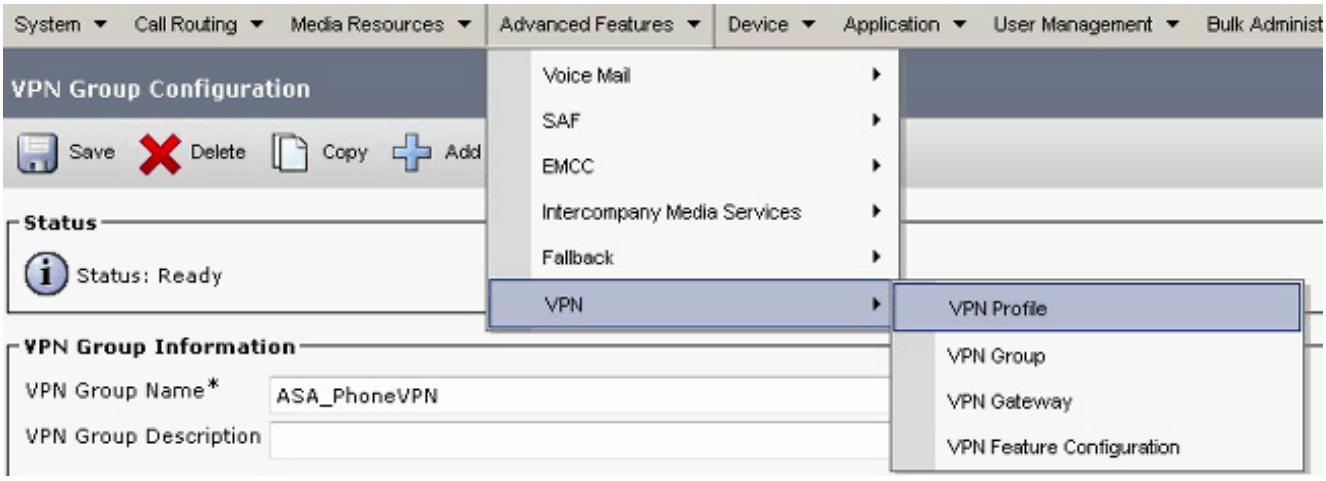

4. Dans la barre de menus, sélectionnez **Advanced Features > VPN > VPN Group**.



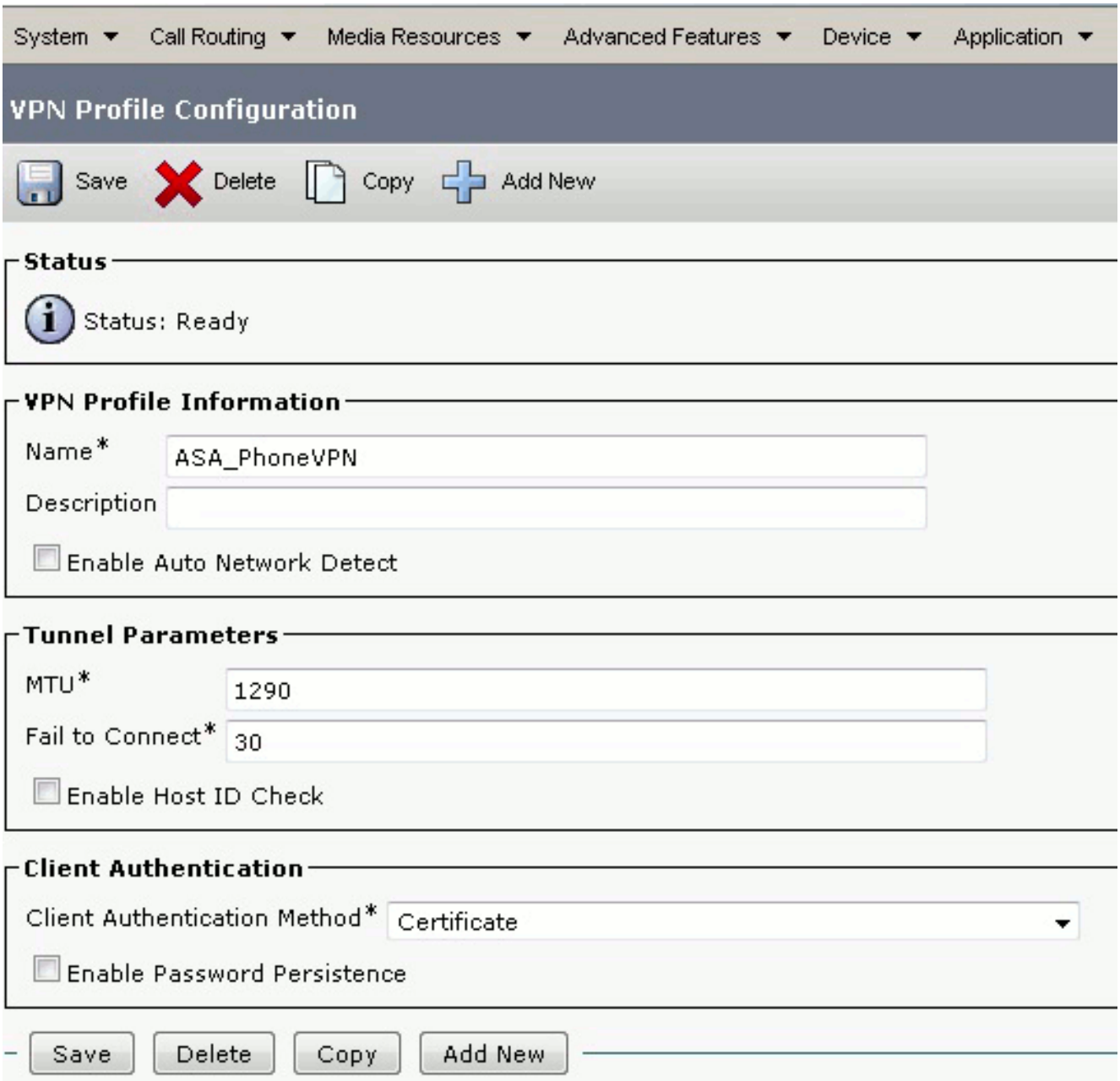

5. Dans le champ Toutes les passerelles VPN disponibles, sélectionnez la passerelle VPN précédemment définie. Cliquez sur la flèche vers le bas afin de déplacer la passerelle sélectionnée vers les passerelles VPN sélectionnées dans ce champ de groupe VPN.




6. Dans la barre de menus, sélectionnez **Advanced Features > VPN > VPN Profile**.

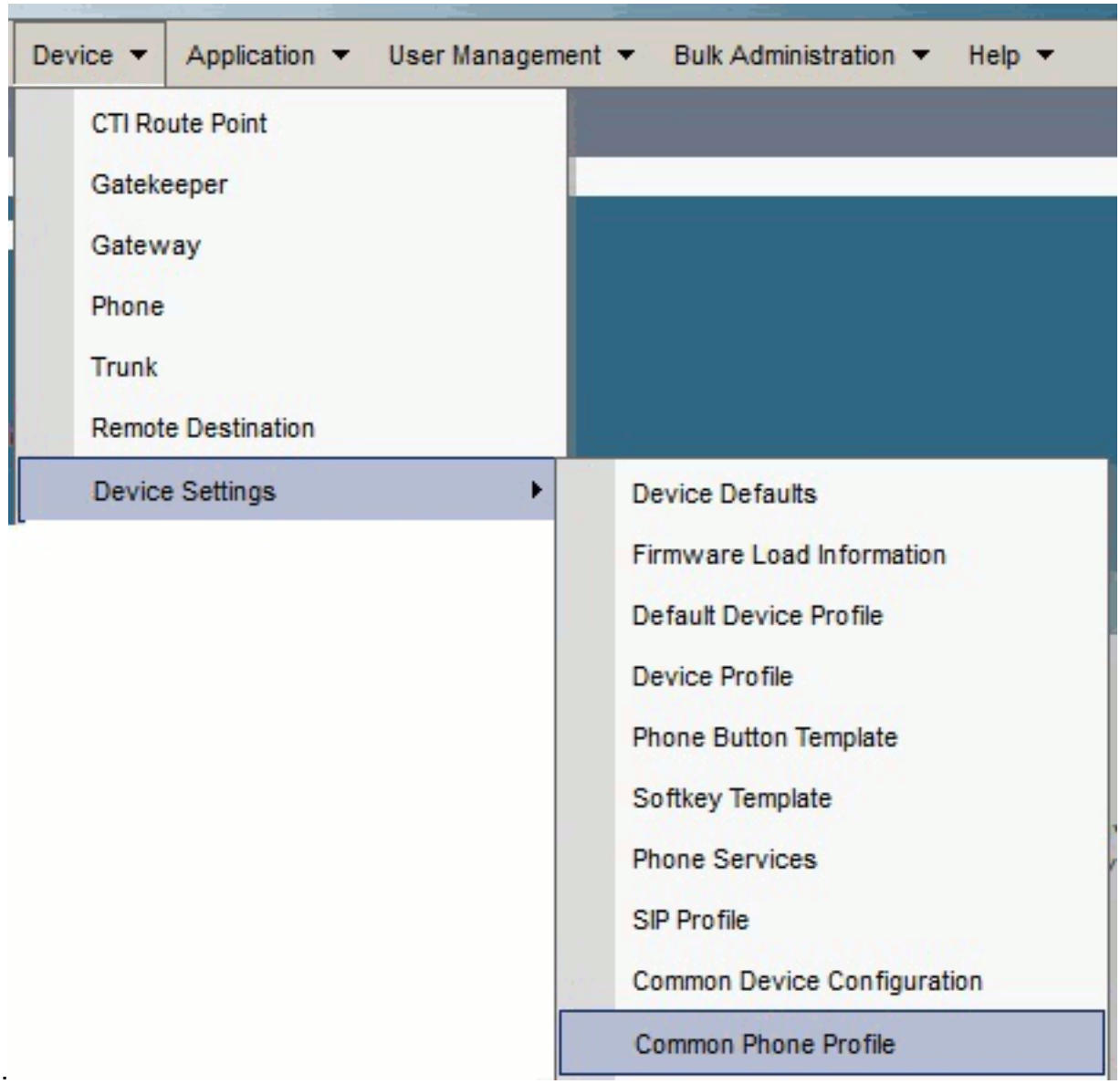



7. Afin de configurer le profil VPN, renseignez tous les champs marqués d'un astérisque (*).

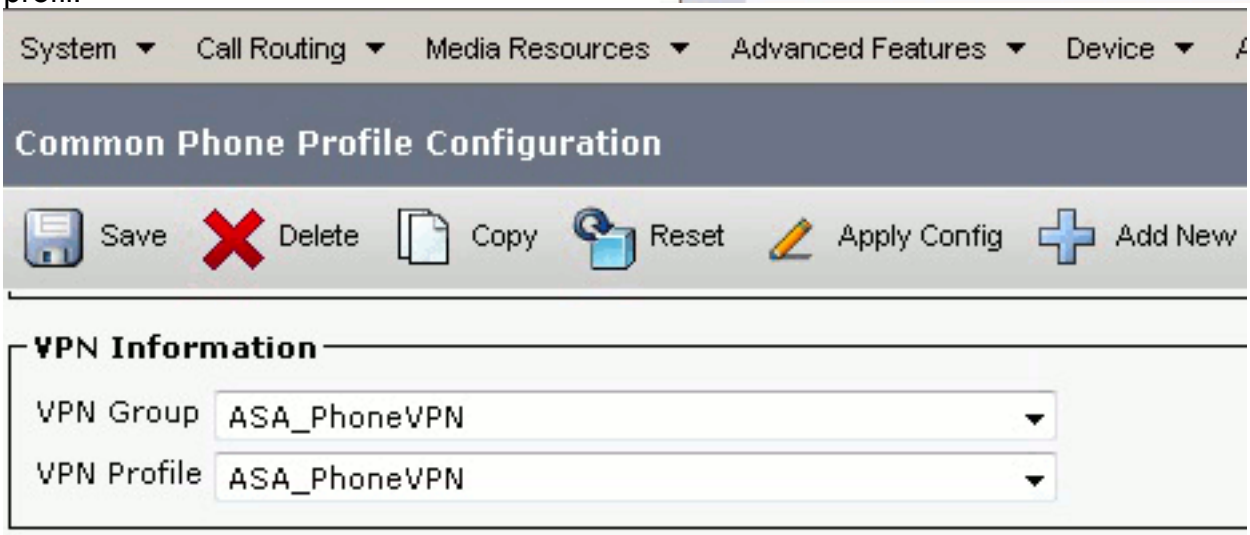



**Activer la détection automatique du réseau :** Si cette option est activée, le téléphone VPN envoie une requête ping au serveur TFTP et si aucune réponse n'est reçue, il initie automatiquement une connexion VPN.**Activer la vérification de l'ID d'hôte :** Si cette option est activée, le téléphone VPN compare le nom de domaine complet de l'URL de la passerelle VPN au CN/SAN du certificat. Le client ne parvient pas à se connecter s'il ne correspond pas ou si un certificat générique avec un astérisque (*) est utilisé.**Activer la persistance du mot de passe :** Cela permet au téléphone VPN de mettre en cache le nom d'utilisateur et le mot de passe pour la prochaine tentative VPN.

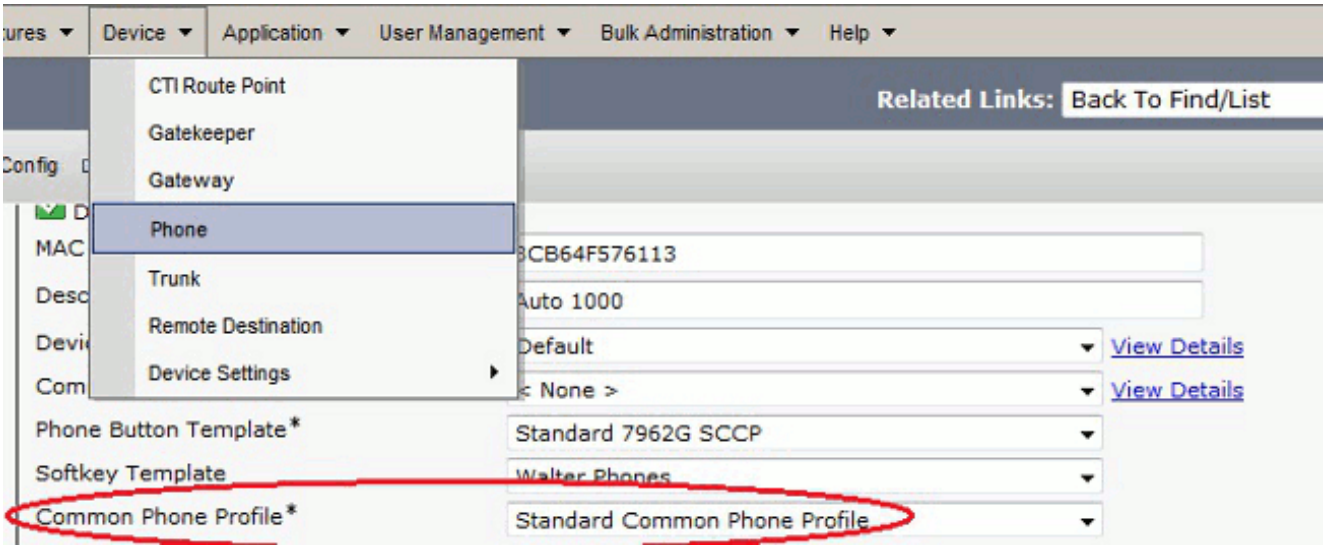
8. Dans la fenêtre Common Phone Profile Configuration, cliquez sur **Apply Config** afin d'appliquer la nouvelle configuration VPN. Vous pouvez utiliser le profil de téléphone commun standard ou créer un nouveau




profil.




9. Si vous avez créé un nouveau profil pour des téléphones/utilisateurs spécifiques, accédez à la fenêtre Configuration du téléphone. Dans le champ Common Phone Profile, sélectionnez **Standard Common Phone Profile**.

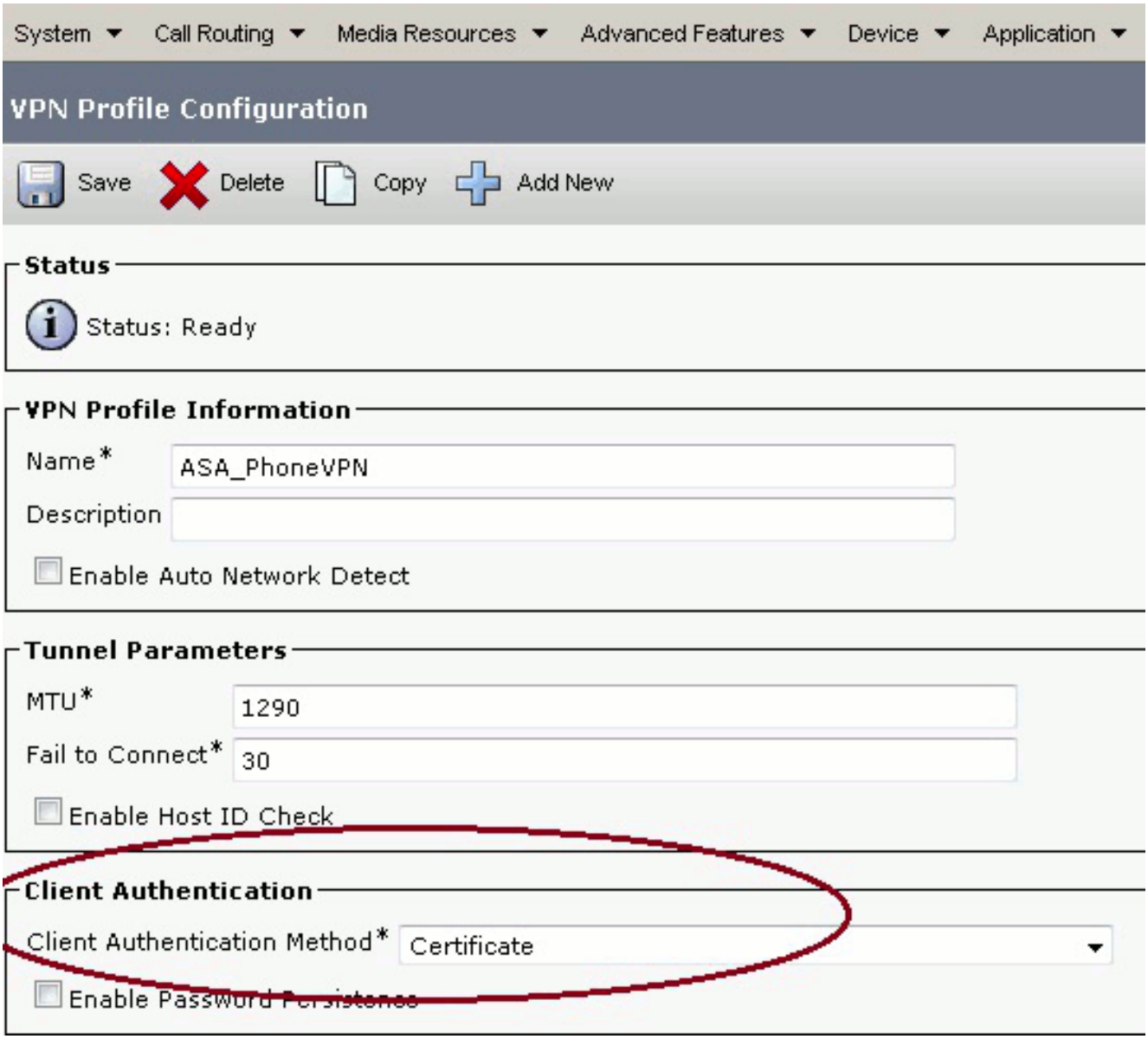



10. Enregistrez à nouveau le téléphone dans CallManager afin de télécharger la nouvelle configuration.

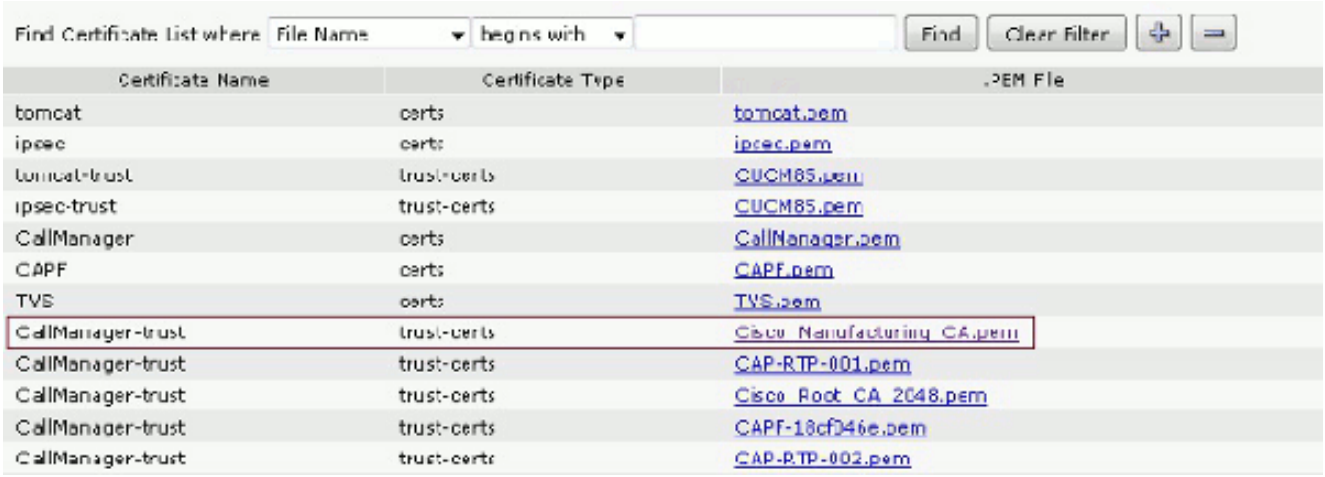
## Configuration de l'authentification de certificat

Afin de configurer l'authentification de certificat, complétez ces étapes dans CallManager et l'ASA :

1. Dans la barre de menus, sélectionnez **Advanced Features > VPN > VPN Profile**.
2. Confirmez que le champ Client Authentication Method est défini sur **Certificate.**




3. Connectez-vous à CallManager. Dans la barre de menus, sélectionnez **Unified OS Administration > Security > Certificate Management > Find**.
4. Exporter le ou les certificats corrects pour la méthode d'authentification de certificat sélectionnée :MIC : Cisco_Manufacturing_CA - Authentification des téléphones IP avec une carte
   MIC




   LSC : Fonction proxy d'autorité de certification Cisco (CAPF) - Authentification des téléphones IP avec un

LSC

| Certificate Name | Certificate Type | .PEM File | |
|---|---|---|---|
| tomcat | certs | tomcat.pem | tomcat.der |
| ipsec | certs | ipsec.pem | ipsec.der |
| tomcat-trust | trust-certs | CUCM85.pem | CUCM85.der |
| ipsec-trust | trust-certs | CUCM85.pem | CUCM85.der |
| CallManager | certs | CallManager.pem | CallManager.der |
| CAPF | certs | CAPF.pem | CAPF.der |
| TVS | certs | TVS.pem | TVS.der |
| CallManager-trust | trust-certs | Cisco_Manufacturing_CA.pem | |

5. Recherchez le certificat, Cisco_Manufacturing_CA ou CAPF. Téléchargez le fichier .pem et enregistrez-le en tant que fichier .txt
6. Créez un nouveau point de confiance sur l'ASA et authentifiez le point de confiance avec le certificat enregistré précédent. Lorsque vous êtes invité à fournir un certificat CA codé en base 64, sélectionnez et collez le texte dans le fichier .pem téléchargé avec les lignes BEGIN et END. Un exemple est montré :

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#

<base-64 encoded CA certificate>

quit
```

7. Confirmez que l'authentification sur le groupe de tunnels est définie sur l'authentification de certificat.

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

## Installation du certificat sur les téléphones IP

Les téléphones IP peuvent fonctionner avec des MIC ou des LSC, mais le processus de configuration est différent pour chaque certificat.

### Installation MIC

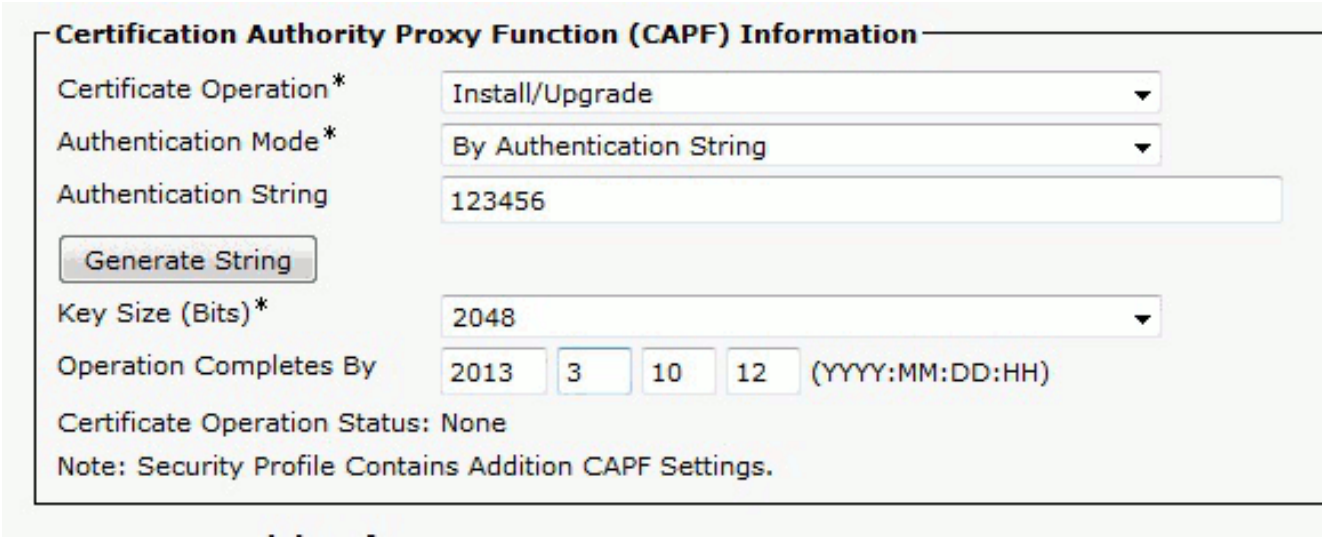
Par défaut, tous les téléphones prenant en charge le VPN sont préchargés avec des MIC. Les téléphones 7960 et 7940 ne sont pas équipés d'un MIC et nécessitent une procédure d'installation spéciale pour que le LSC s'enregistre en toute sécurité.

**Note:** Cisco vous recommande d'utiliser des MIC pour l'installation de LSC uniquement. Cisco prend en charge les LSC pour authentifier la connexion TLS avec CUCM. Comme les certificats racine MIC peuvent être compromis, les clients qui configurent des téléphones pour utiliser des MIC pour l'authentification TLS ou à toute autre fin le font à leurs propres risques. Cisco n'assume aucune responsabilité si les MIC sont compromis.

### Installation LSC

1. Activez le service CAPF sur CUCM.
2. Une fois le service CAPF activé, affectez les instructions téléphoniques pour générer un LSC dans CUCM. Connectez-vous à Cisco Unified CM Administration et choisissez **Device > Phone**. Sélectionnez le téléphone que vous avez configuré.
3. Dans la section Informations CAPF (Certificate Authority Proxy Function), assurez-vous que tous les paramètres sont corrects et que l'opération est définie sur une date

future.




4. Si le mode d'authentification est défini sur Chaîne nulle ou Certificat existant, aucune autre action n'est requise.
5. Si le mode d'authentification est défini sur une chaîne, sélectionnez manuellement **Paramètres > Configuration de la sécurité > **# > LSC > Mettre à jour** dans la console du téléphone.

# Vérification

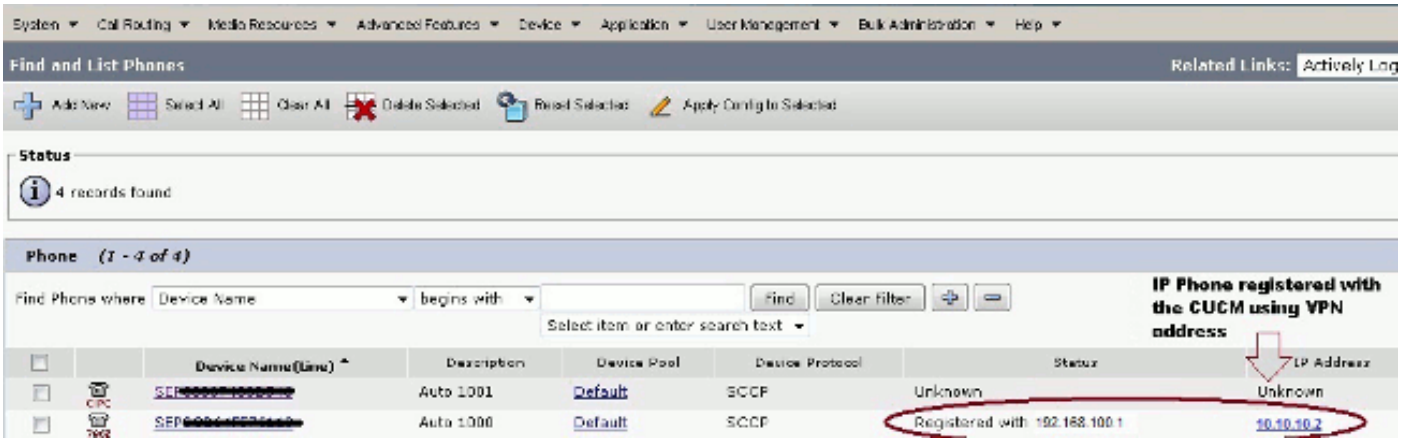
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

### Vérification ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : CP-7962G-SEPXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
```

```
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

### Vérification CUCM




# Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

### Bogues associés

- ID de bogue Cisco CSCtf09529, ajout de la prise en charge de la fonctionnalité VPN dans

CUCM pour les téléphones 8961, 9951 et 9971
- ID de bogue Cisco CSCuc71462, basculement VPN du téléphone IP en 8 minutes
- ID de bogue Cisco CSCtz42052, prise en charge VPN SSL du téléphone IP pour les numéros de port non par défaut
- ID de bogue Cisco CSCth96551, tous les caractères ASCII ne sont pas pris en charge lors de la connexion utilisateur VPN du téléphone + mot de passe.
- ID de bogue Cisco CSCuj71475, entrée TFTP manuelle requise pour VPN de téléphone IP
- ID de bogue Cisco CSCum10683, téléphones IP non connectés appels manqués, passés ou reçus

## Informations connexes

- Support et documentation techniques - Cisco Systems