

Dépannez le téléphone d'AnyConnect VPN - Téléphones IP, ASA, et CUCM

Contenu

[Introduction](#)

[Informations générales](#)

[Confirmez le permis de téléphone VPN sur l'ASA](#)

[Exportation limitée et exportation CUCM sans restriction](#)

[Problèmes courants sur l'ASA](#)

[Certificats pour l'usage sur l'ASA](#)

[Point de confiance/certificat pour l'exportation ASA et l'importation CUCM](#)

[L'ASA présente le certificat Auto-signé par ECDSA au lieu du certificat configuré RSA](#)

[Base de données externe pour l'authentification des utilisateurs de téléphone IP](#)

[Correspondances d'informations parasites de certificat entre la liste de confiance de certificat ASA et de téléphone VPN](#)

[Informations parasites du contrôle SHA1](#)

[Fichier de configuration de téléphone IP de téléchargement](#)

[Décodage des informations parasites](#)

[Équilibrage de charge et Téléphones IP VPN](#)

[CSD et Téléphones IP](#)

[Logs ASA](#)

[Debugs ASA](#)

[Règles DAP](#)

[Valeurs héritées de DfltGrpPolicy ou d'autres groupes](#)

[Chiffrements pris en charge de cryptage](#)

[Problèmes courants sur le CUCM](#)

[Configurations VPN non appliquées au téléphone IP](#)

[Méthode d'authentification de certificat](#)

[Contrôle d'ID d'hôte](#)

[Dépannage supplémentaire](#)

[Logs et debugs aux utiliser dans l'ASA](#)

[Logs de téléphone IP](#)

[Questions corrélées entre les logs ASA et les logs de téléphone IP](#)

[Logs ASA](#)

[Logs de téléphone](#)

[Envergure à la caractéristique de port PC](#)

[Modifications de configuration de téléphone IP tandis que relié par VPN](#)

[Renouvellement du certificat ssl ASA](#)

Introduction

Ce document décrit comment dépanner des questions avec des Téléphones IP qui emploie le protocole de Secure Sockets Layer (SSL) (Client à mobilité sécurisé Cisco AnyConnect) afin de se connecter à une appliance de sécurité adaptable Cisco (ASA) qui est utilisée comme une passerelle VPN et afin de se connecter à Cisco Unified Communications Manager (CUCM) qui est utilisée en tant que serveur de Voix.

Pour des exemples de configuration d'AnyConnect avec des téléphones VPN, référez-vous à ces documents :

- [SSLVPN avec l'exemple de configuration de Téléphones IP](#)
- [Téléphone d'AnyConnect VPN avec l'exemple de configuration d'authentification de certificat](#)

Informations générales

Avant que vous déployiez le VPN SSL avec des Téléphones IP, confirmez que vous avez répondu à ces exigences initiales pour des permis d'AnyConnect pour l'ASA et pour la version limitée par exportation des États-Unis du CUCM.

Confirmez le permis de téléphone VPN sur l'ASA

Le permis de téléphone VPN active la caractéristique dans l'ASA. Afin de confirmer le nombre d'utilisateurs qui peuvent se connecter à l'AnyConnect (si c'est un téléphone IP), vérifiez le permis de la meilleure qualité SSL d'AnyConnect. Référez-vous [quel permis ASA est nécessaire pour le téléphone IP et les connexions VPN mobiles ?](#) pour plus de détails.

Sur l'ASA, employez la commande de **show version** afin de vérifier si la caractéristique est activée. Le nom de permis diffère avec la release ASA :

- Release 8.0.x ASA : le nom de permis est AnyConnect pour le téléphone de Linksys.
- Version 8.2.x et ultérieures ASA : le nom de permis est AnyConnect pour le téléphone de Cisco VPN.

Voici un exemple pour la release 8.0.x ASA :

```
ASA5505(config)# show ver

Cisco Adaptive Security Appliance Software Version 8.0(5)
Device Manager Version 7.0(2)
<snip>
Licensed features for this platform:
VPN Peers : 10
WebVPN Peers : 2
AnyConnect for Linksys phone : Disabled
<snip>
This platform has a Base license.
```

Voici un exemple pour des versions 8.2.x et ultérieures ASA :

```
ASA5520-C(config)# show ver

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(1)
<snip>
Licensed features for this platform:
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
<snip>
This platform has an ASA 5520 VPN Plus license.
```

Exportation limitée et exportation CUCM sans restriction

Vous devriez déployer une version limitée par exportation des États-Unis de CUCM pour la caractéristique de téléphone VPN.

Si vous utilisez une version sans restriction d'exportation des États-Unis de CUCM, notez cela :

- Des configurations de sécurité de téléphone IP sont modifiées afin de désactiver le cryptage de signalisation et de medias ; ceci inclut le cryptage fourni par la caractéristique de téléphone VPN.
- Vous ne pouvez pas exporter des détails VPN par l'importation/exportation.

- Les cases configuration pour le profil VPN, la passerelle VPN, le groupe VPN, et VPN caractéristique ne sont pas affichées.

Note: Une fois que vous améliorez à la version sans restriction d'exportation des États-Unis de CUCM, vous ne pouvez pas améliorer plus tard à, ou exécutez un frais installent de, la version limitée par exportation des États-Unis de ce logiciel.

Problèmes courants sur l'ASA

Note: Vous pouvez employer l'[analyseur de Cisco CLI](#) (clients [enregistrés](#) seulement) afin de visualiser des analyses de sortie de commande show. Vous devriez également se référer aux [informations importantes sur le](#) document Cisco de [commandes de debug](#) avant que vous utilisiez des commandes de **débogage**.

Certificats pour l'usage sur l'ASA

Sur l'ASA, vous pouvez utiliser les Certificats auto-signés SSL, les tiers Certificats SSL, et les Certificats de masque ; l'un de ces sécurisé la transmission entre le téléphone IP et l'ASA.

Seulement un certificat d'identité peut être utilisé parce que seulement un certificat peut être assigné à chaque interface.

Pour de tiers Certificats SSL, installez la chaîne complète dans l'ASA, et incluez tous les intermédiaire et certificats racine.

Point de confiance/certificat pour l'exportation ASA et l'importation CUCM

Le certificat que l'ASA présente au téléphone IP pendant la négociation SSL doit être exporté de l'ASA et être importé dans le CUCM. Vérifiez le point de confiance assigné à l'interface à laquelle les Téléphones IP se connectent afin de connaître quel certificat à exporter de l'ASA.

Employez la commande **SSL de passage d'exposition** afin de vérifier le point de confiance (certificat) à exporter. Référez-vous au [téléphone d'AnyConnect VPN avec le d'exemple de configuration d'authentification de certificat](#).

Note: Si vous avez déployé un tiers certificat vers un ou plusieurs ASA, vous devez exporter chaque certificat d'identité de chaque ASA et puis l'importer au CUCM comme téléphone-VPN-confiance.

L'ASA présente le certificat Auto-signé par ECDSA au lieu du certificat configuré RSA

Quand cette question se produit, les téléphones de plus nouveau modèle ne peuvent pas se connecter, alors que les téléphones modèles plus anciens n'éprouvent aucune question. Voici les logs le téléphone quand cette question se produit :

```
ASA5520-C(config)# show ver

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(1)
<snip>
Licensed features for this platform:
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
AnyConnect for Cisco VPN Phone      : Disabled      perpetual
<snip>
This platform has an ASA 5520 VPN Plus license.
```

Dans les versions 9.4.1 et ultérieures, le chiffrement elliptique de curve est pris en charge pour SSL/TLS. Quand un client curve-capable elliptique de VPN SSL tel qu'un nouveau modèle de téléphone se connecte à l'ASA, la suite elliptique de chiffrement de curve est négociée, et l'ASA présente le client de VPN SSL avec un certificat elliptique de curve, même lorsque l'interface qui correspond est configurée avec un point de confiance basé sur RSA. Afin d'empêcher l'ASA de présenter un certificat ssl auto-signé, l'administrateur doit retirer les suites de chiffrement qui correspondent par l'intermédiaire de la commande de **chiffrement SSL**. Par exemple, pour une interface qui est configurée avec un point de confiance RSA, l'administrateur peut exécuter cette commande de sorte que seulement des chiffrements basés sur RSA soient négociés :

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA"
```

Avec l'implémentation de l'ID de bogue Cisco [CSCuu02848](#), la priorité est accordée à la configuration. des Certificats Explicite-configurés sont toujours utilisés. des Certificats Auto-signés sont seulement utilisés faute de certificat configuré.

Chiffrements proposés de client	CERT RSA seulement	CERT EC seulement	Les deux CERT	Aucune
La RSA chiffre seulement	CERT des utilisations RSA Chiffrements des utilisations RSA	CERT auto-signé par RSA d'utilisations Chiffrements des utilisations RSA	CERT des utilisations RSA Chiffrements des utilisations RSA	CERT auto-signé RSA d'utilisations Chiffrements des utilisations RSA
L'EC chiffre seulement (rare)	La connexion échoue	CERT EC d'utilisations Chiffrements EC d'utilisations	CERT EC d'utilisations Chiffrements EC d'utilisations	CERT auto-signé par EC d'utilisation Chiffrements EC d'utilisations
Les deux chiffrements seulement	CERT des utilisations RSA Chiffrements des utilisations RSA	CERT EC d'utilisations Chiffrements EC d'utilisations	CERT EC d'utilisations Chiffrements EC d'utilisations	CERT auto-signé par EC d'utilisation Chiffrements EC d'utilisations

Base de données externe pour l'authentification des utilisateurs de téléphone IP

Vous pouvez employer une base de données externe afin d'authentifier des utilisateurs de téléphone IP. Les protocoles tels que le Protocole LDAP (Lightweight Directory Access Protocol) ou l'authentification à distance se connectent l'utilisateur que le service (RADIUS) peut être utilisé pour l'authentification des utilisateurs du téléphone VPN.

Correspondances d'informations parasites de certificat entre la liste de confiance de certificat ASA et de téléphone VPN

Souvenez-vous que vous devez télécharger le certificat qui est assigné à l'interface SSL ASA et le télécharger comme certificat de Téléphone-VPN-confiance dans le CUCM. Les différentes circonstances pourraient entraîner les informations parasites pour ce certificat présenté par l'ASA pour ne pas appairer les informations parasites que le serveur CUCM génère et pousse au téléphone VPN par le fichier de configuration.

Une fois que la configuration est complète, testez la connexion VPN entre le téléphone IP et l'ASA. Si la connexion continue à échouer, vérifiez si les informations parasites du certificat ASA appairer les informations parasites le téléphone IP prévoit :

1. Vérifiez les informations parasites du Secure Hash Algorithm 1 (SHA1) présentées par l'ASA.
2. Employez le TFTP afin de télécharger le fichier de configuration de téléphone IP du CUCM.
3. Décodez les informations parasites de l'hexadécimal pour baser 64 ou de la base 64 à l'hexadécimal.

Informations parasites du contrôle SHA1

L'ASA présente le certificat appliqué avec la commande de **point de confiance SSL** sur l'interface à laquelle le téléphone IP se connecte. Pour vérifier ce certificat, ouvrez le navigateur (dans cet exemple, Firefox), et écrivez l'URL (le groupe-URL) auquel les téléphones devraient se connecter :

https://10.198.16.140/+CSCOE+/logon.html?fcadbadd=1

Page Info - https://10.198.16.140/+CSCOE+/logon.html?fcadbadd=1

General Media Permissions **Security**

Website Identity

Website: **10.198.16.140**

Owner: **This website does not supply ownership information.**

Verified by: **ASA Temporary Self Signed Certificate**

2 View Certificate

Certificate Viewer: "ASA Temporary Self Signed Certificate"

General Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	ASA Temporary Self Signed Certificate
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	DF:F2:C4:50

Issued By

Common Name (CN)	ASA Temporary Self Signed Certificate
Organization (O)	ASA Temporary Self Signed Certificate
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	12/09/2012
Expires On	12/07/2022

Fingerprints

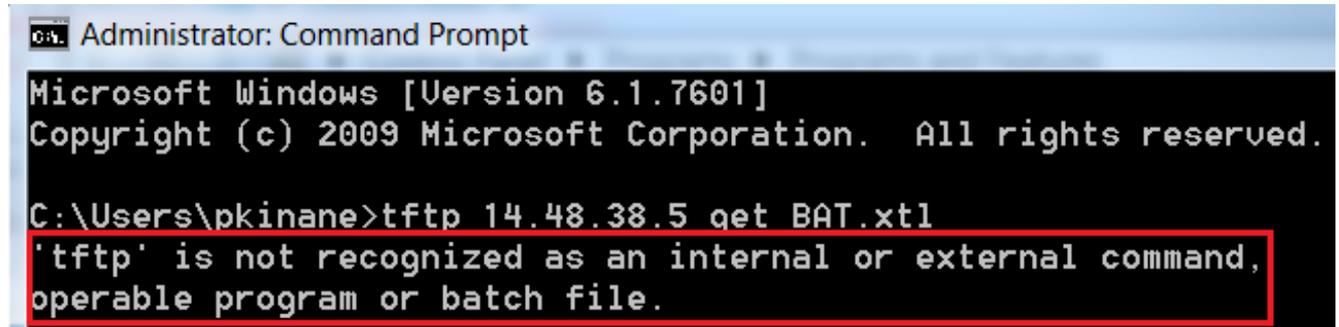
3 SHA1 Fingerprint	E5:7E:81:EA:99:54:C1:44:97:66:78:D0:E2:41:8C:DF:79:A9:31:76
MD5 Fingerprint	D7:10:78:FB:61:A2:F6:C2:01:07:6C:03:DE:17:EF:F9

Fichier de configuration de téléphone IP de téléchargement

D'un PC avec l'accès direct au CUCM, téléchargez le fichier de config TFTP pour le téléphone avec des questions de connexion. Deux méthodes de téléchargement sont :

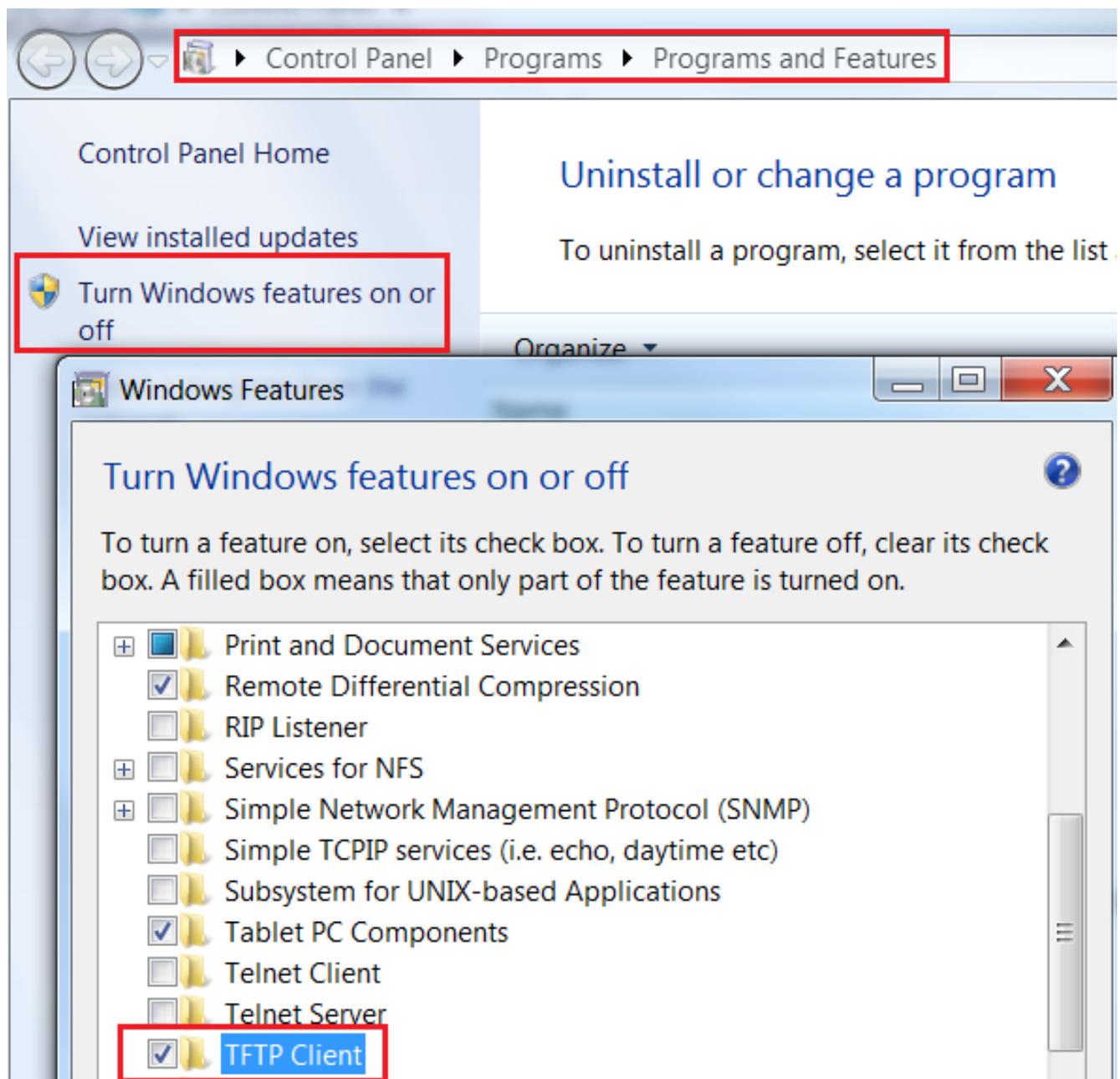
1. Ouvrez une session ILC dans Windows, et utilisez le **tftp -I <TFTP Server> OBTIENNENT la commande du MAC address >.cnf.xml de <Phone de SEPT.**

Note: Si vous recevez une erreur semblable à celle ci-dessous, vous devriez confirmer que la fonctionnalité client TFTP est activée.

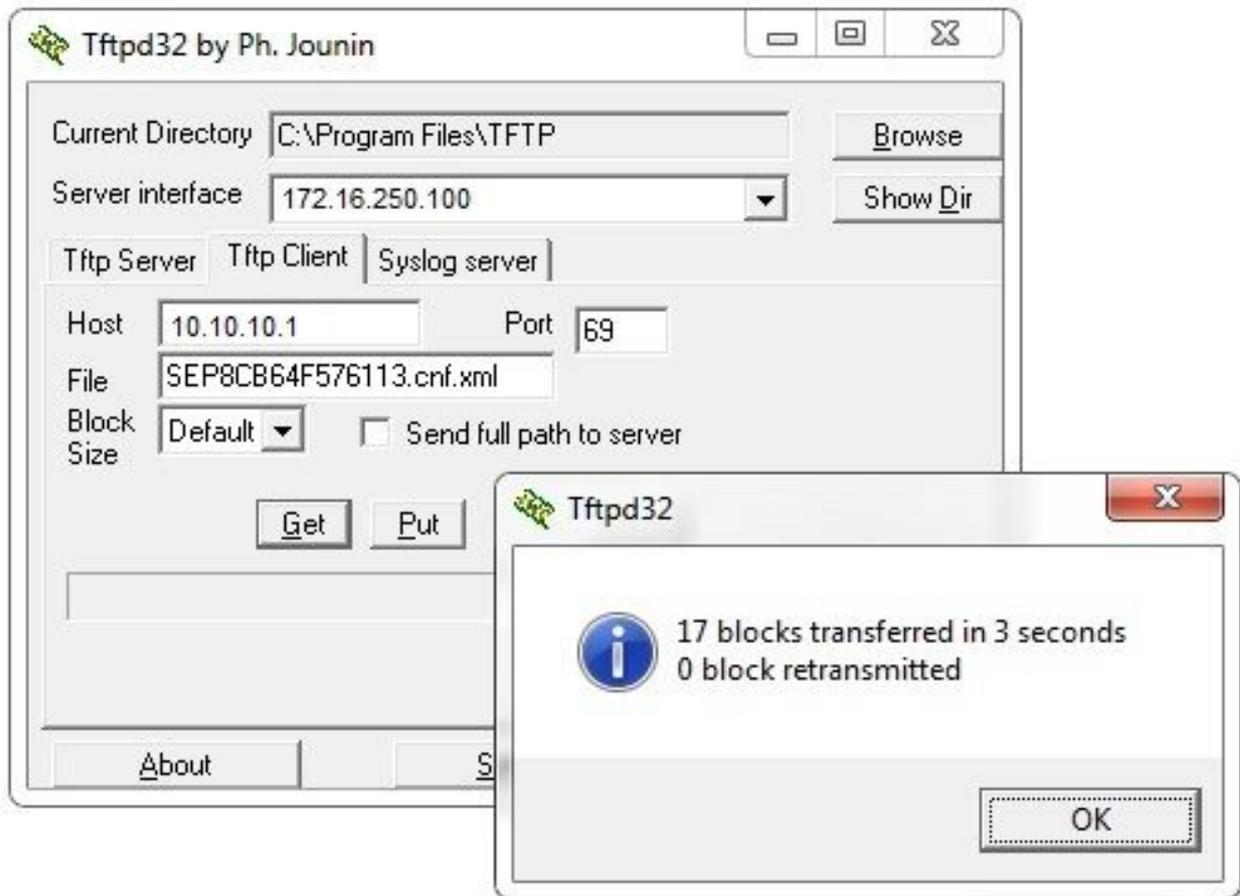


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\pkinane>tftp 14.48.38.5 get BAT.xml
'tftp' is not recognized as an internal or external command,
operable program or batch file.
```



2. Employez une application telle que [Tftpd32](#) pour télécharger le fichier :



3. Une fois le fichier est téléchargé, ouvre le XML et trouve la configuration de *vpnGroup*. Cet exemple affiche la section et le *certHash* à vérifier :

```

<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>0</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.198.16.140/VPNPhone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
</credentials>
</vpnGroup>

```

Décodez les informations parasites

Confirmez que les deux valeurs de hachage s'assortissent. Le navigateur présente les informations parasites dans le format hexadécimal, alors que le fichier XML utilise la base 64, ainsi convertissent un format en autre afin de confirmer la correspondance. Il y a beaucoup de convertisseurs disponibles ; un exemple est le [CONVERTISSEUR, BINAIRE](#).



Note: Si la valeur de hachage précédente ne s'assortit pas, le téléphone VPN ne fait pas confiance à la connexion qui est étée en pourparlers avec l'ASA, et la connexion échoue.

Équilibrage de charge et Téléphones IP VPN

le VPN SSL Chargement-équilibré n'est pas pris en charge pour des téléphones VPN. Les téléphones VPN n'exécutent pas la vraie validation de certificat mais utiliser à la place hache abaissé par le CUCM pour valider les serveurs. Puisque l'Équilibrage de charge VPN est fondamentalement une redirection HTTP, il exige des téléphones de valider de plusieurs Certificats, qui mène à la panne. Les symptômes de la panne d'Équilibrage de charge VPN incluent :

- Le téléphone alterne entre les serveurs et prend exceptionnellement un longtemps de se connecter ou échoue par la suite.
- Les logs de téléphone contiennent des messages de ce type :

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>0</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.198.16.140/VPNPhone</url1>
</addresses>
```

```
<credentials>
<hashAlg>0</hashAlg>
<certHash1>5X6B6p1UwUSXZnjQ4kGM33mpMY=</certHash1>
</credentials>
</vpnGroup>
```

CSD et Téléphones IP

Actuellement, les Téléphones IP ne prennent en charge pas le Cisco Secure Desktop (CSD) et ne se connectent pas quand le CSD est activé pour le groupe de tunnels ou globalement dans l'ASA.

D'abord, confirmez si l'ASA a le CSD activé. Sélectionnez la commande de **webvpn de passage d'exposition** dans l'ASA CLI :

```
ASA5510-F# show run webvpn
webvpn
enable outside
  csd image disk0:/csd_3.6.6210-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect enable
ASA5510-F#
```

Afin de vérifier des questions CSD pendant une connexion de téléphone IP, vérifiez les logs ou les mettez au point dans l'ASA.

Logs ASA

```
ASA5510-F# show run webvpn
webvpn
enable outside
  csd image disk0:/csd_3.6.6210-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect enable
ASA5510-F#
```

Debugs ASA

```
debug webvpn anyconnect 255
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

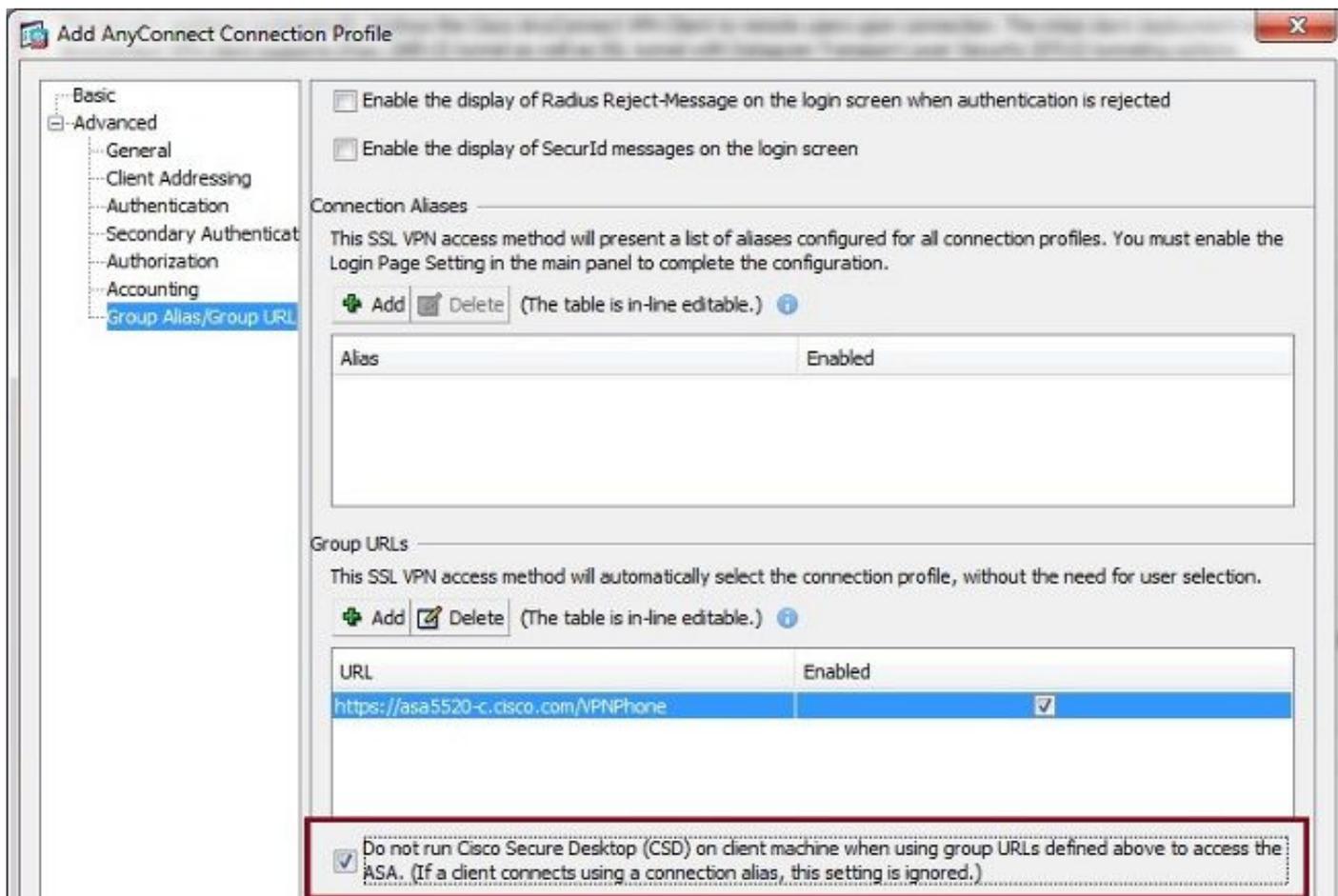
Note: Dans un grand déploiement avec une charge élevée des utilisateurs d'AnyConnect, Cisco recommande que vous n'activiez pas l'**anyconnect de debug webvpn**. Sa sortie ne peut pas être filtrée par l'adresse IP, ainsi un grand nombre d'informations pourraient être créées.

Dans des versions 8.2 et ultérieures ASA, vous devez appliquer la **sans-CDD** commandez sous les webvpn-attributs du groupe de tunnels :

```
tunnel-group VPNPhone webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/VPNPhone enable
without-csd
```

Dans les versions préalables de l'ASA, ce n'était pas possible, ainsi le seul contournement était de désactiver le CSD globalement.

Dans le Cisco Adaptive Security Device Manager (ASDM), vous pouvez désactiver le CSD pour un profil spécifique de connexion suivant les indications de cet exemple :

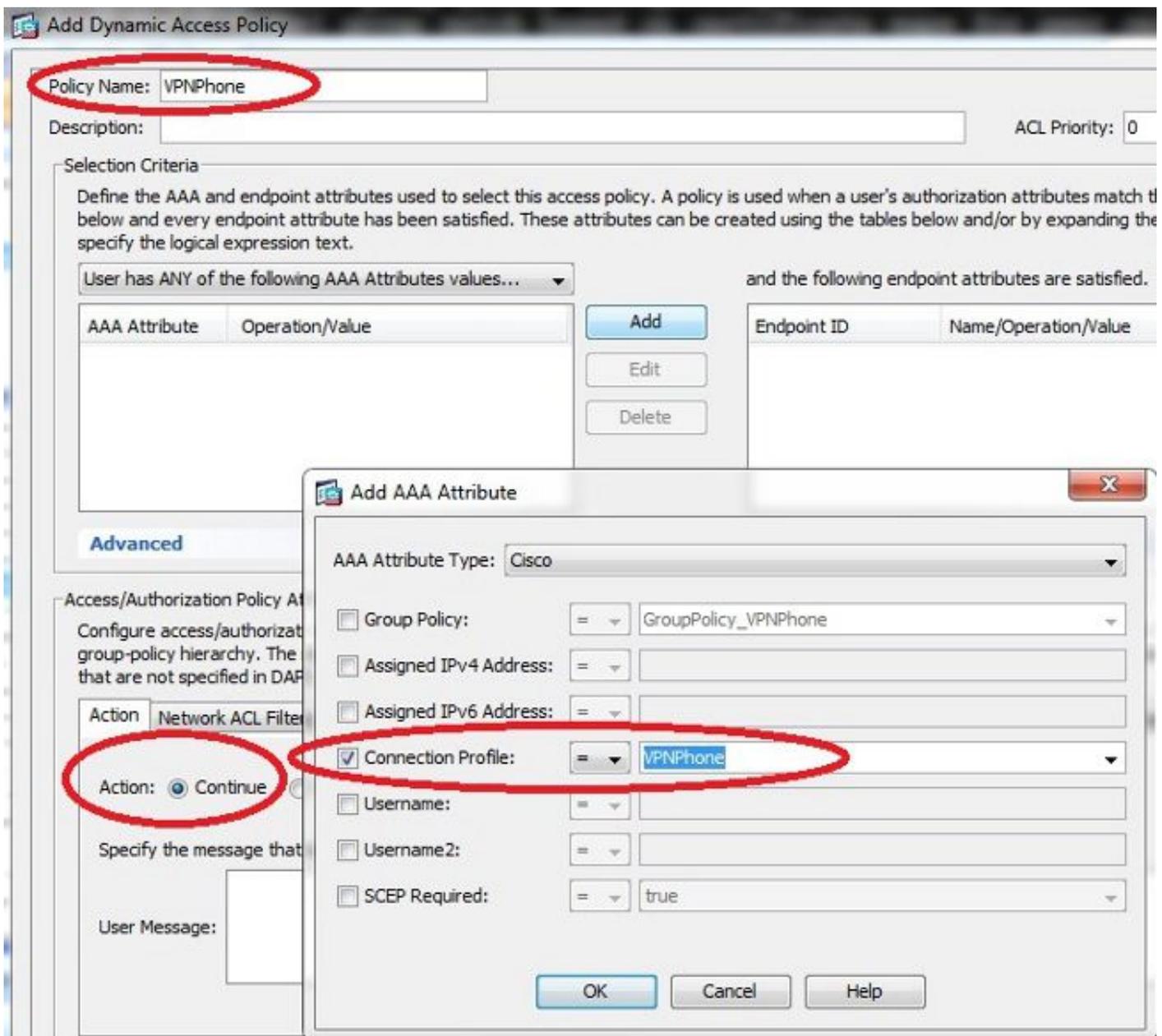


Note: Employez un groupe-URL afin d'arrêter la caractéristique CSD.

Règles DAP

La plupart des déploiements connectent non seulement des Téléphones IP à l'ASA mais connectent également différents types des ordinateurs (Microsoft, Linux, Mac OS) et de périphériques mobiles (Android, IOS). Pour cette raison, il est normal de trouver une configuration existante des règles de la stratégie d'accès dynamique (DAP), où, le plus souvent, l'action par défaut sous le DfltAccessPolicy est arrêt de la connexion.

Si c'est le cas, créez une règle distincte DAP pour les téléphones VPN. Utilisez un paramètre spécifique, tel que le profil de connexion, et placez l'action **de continuer** :



Si vous ne créez pas une stratégie de la particularité DAP pour des Téléphones IP, l'ASA affiche un hit sous le DfltAccessPolicy et une connexion défectueuse :

```
%ASA-6-716038: Group <DfltGrpPolicy> User <CP-7962G-SEP8CB64F576113> IP
<172.16.250.9> Authentication: successful, Session Type: WebVPN.
%ASA-7-734003: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Session
Attribute aaa.cisco.grouppolicy = GroupPolicy_VPNPhone
<snip>
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9,
Connection AnyConnect: The following DAP records were selected for this
connection: DfltAccessPolicy
%ASA-5-734002: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Connection
terminated by the following DAP records: DfltAccessPolicy
```

Une fois que vous créez une stratégie de la particularité DAP pour les Téléphones IP avec le

positionnement d'action **pour continuer**, vous pouvez se connecter :

```
%ASA-7-746012: user-identity: Add IP-User mapping 10.10.10.10 -  
LOCAL\CP-7962G-SEP8CB64F576113 Succeeded - VPN user  
%ASA-4-722051: Group <GroupPolicy_VPNPhone> User <CP-7962G-SEP8CB64F576113> IP  
<172.16.250.9> Address <10.10.10.10> assigned to session  
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9, Connection  
AnyConnect: The following DAP records were selected for this connection: VPNPhone
```

Valeurs héritées de DfltGrpPolicy ou d'autres groupes

Dans de nombreux cas, le DfltGrpPolicy est installé avec plusieurs options. Par défaut, ces configurations sont héritées pour la session de téléphone IP à moins qu'elles soient manuellement spécifiées dans la stratégie de groupe que le téléphone IP devrait utiliser.

Quelques paramètres qui pourraient affecter la connexion s'ils sont hérités du DfltGrpPolicy sont :

- group-lock
- VPN-tunnel-Protocol
- VPN-simultané-procédures de connexion
- VPN-filtre

Supposez que vous avez cet exemple de configuration dans le DfltGrpPolicy et le GroupPolicy_VPNPhone :

```
group-policy DfltGrpPolicy attributes  
  vpn-simultaneous-logins 0  
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless  
  group-lock value DefaultWEBVPNGroup  
  vpn-filter value NO-TRAFFIC
```

```
group-policy GroupPolicy_VPNPhone attributes  
wins-server none  
dns-server value 10.198.29.20  
default-domain value cisco.com
```

La connexion hérite des paramètres du DfltGrpPolicy qui n'ont pas été explicitement spécifiés sous le GroupPolicy_VPNPhone et pousse toutes les informations au téléphone IP pendant la connexion.

Afin d'éviter ceci, spécifiez manuellement les valeurs que vous avez besoin directement dans le groupe :

```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
  vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
  vpn-filter none
default-domain value cisco.com
```

Afin de vérifier les valeurs par défaut du DfltGrpPolicy, utilisez l'exposition exécutent toute la commande de **stratégie de groupe** ; cet exemple clarifie la différence entre les sorties :

```
ASA5510-F# show run group-policy DfltGrpPolicy
group-policy DfltGrpPolicy attributes
dns-server value 10.198.29.20 10.198.29.21
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
ASA5510-F#
```

```
ASA5510-F# sh run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
banner none
wins-server none
dns-server value 10.198.29.20 10.198.29.21
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
ipv6-vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
```

Voici la sortie de la stratégie de groupe héritent des attributs par l'ASDM :

Name:	DRIGrpPolicy
Banner:	
SCCP forwarding URL:	
Address Pools:	
IPv6 Address Pools:	
More Options	
Tunneling Protocols:	<input checked="" type="checkbox"/> Clientless SSL VPN <input checked="" type="checkbox"/> SSL VPN Client
Filter:	-- None --
NAC Policy:	-- None --
Access Hours:	-- Unrestricted --
Simultaneous Logins:	3
Restrict access to VLAN:	-- Unrestricted --
Connection Profile (Tunnel Group) Lock:	-- None --
Maximum Connect Time:	<input checked="" type="checkbox"/> Unlimited <input type="text"/> minutes
Idle Timeout:	<input type="checkbox"/> None <input type="text" value="30"/> minutes
On smart card removal:	<input checked="" type="radio"/> Disconnect <input type="radio"/> Keep the connection

Name:	VPNPhone
Banner:	<input checked="" type="checkbox"/> Inherit
SCCP forwarding URL:	<input checked="" type="checkbox"/> Inherit
Address Pools:	<input checked="" type="checkbox"/> Inherit
IPv6 Address Pools:	<input checked="" type="checkbox"/> Inherit
More Options	
Tunneling Protocols:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> Clientless SSL VPN <input type="checkbox"/> SSL VPN Client
Filter:	<input checked="" type="checkbox"/> Inherit
NAC Policy:	<input checked="" type="checkbox"/> Inherit
Access Hours:	<input checked="" type="checkbox"/> Inherit
Simultaneous Logins:	<input checked="" type="checkbox"/> Inherit
Restrict access to VLAN:	<input checked="" type="checkbox"/> Inherit
Connection Profile (Tunnel Group) Lock:	<input checked="" type="checkbox"/> Inherit
Maximum Connect Time:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> Unlimited <input type="text"/> minutes
Idle Timeout:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> None <input type="text"/> minutes
On smart card removal:	<input checked="" type="checkbox"/> Inherit <input type="radio"/> Disconnect <input type="radio"/> Keep the connection

Chiffrements pris en charge de cryptage

Un téléphone d'AnyConnect VPN testé avec le téléphone IP 7962G et les supports de version 9.1.1 de micrologiciels seulement deux chiffrements, qui sont les deux Norme AES (Advanced Encryption Standard) : AES256-SHA et AES128-SHA. Si les chiffrements corrects ne sont pas spécifiés dans l'ASA, la connexion est rejetée, suivant les indications du log ASA :

```
%ASA-7-725010: Device supports the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:172.16.250.9/52684 proposes the following
2 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason: no
shared cipher
```

Afin de confirmer si l'ASA a les chiffrements corrects activés, écrivez l'exposition exécutent toutes les commandes SSL et de show ssl :

```
ASA5510-F# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
```

ASA5510-F#

ASA5510-F# **show ssl**

Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1

Start connections using SSLv3 and negotiate to SSLv3 or TLSv1

Enabled cipher order: rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1

Disabled ciphers: des-sha1 rc4-md5 dhe-aes128-sha1 dhe-aes256-sha1 null-sha1

SSL trust-points:

outside interface: SSL

Certificate authentication is not enabled

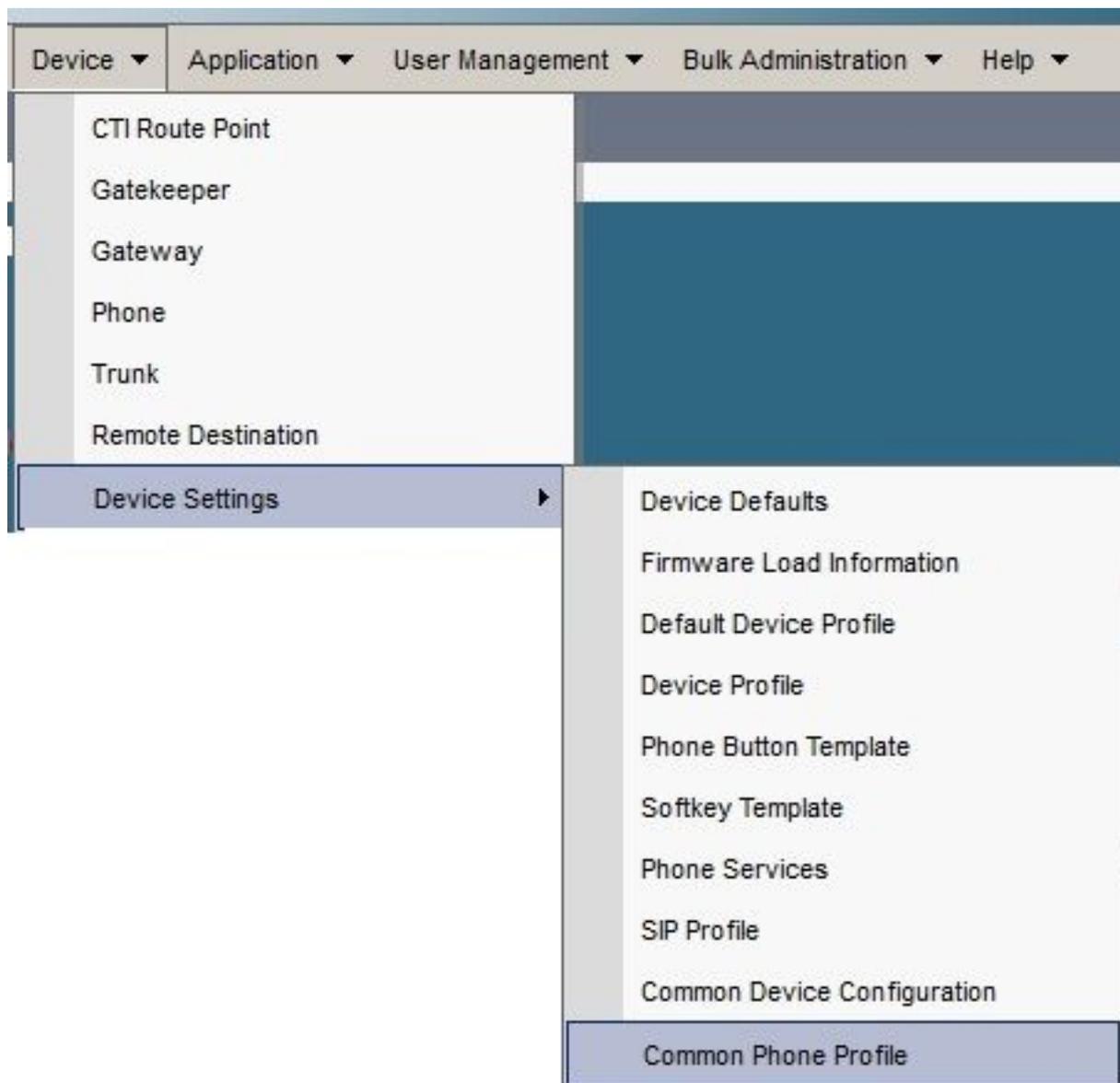
ASA5510-F#

Problèmes courants sur le CUCM

Configurations VPN non appliquées au téléphone IP

Une fois la configuration sur le CUCM est créée (passerelle, groupe, et profil), appliquent les configurations VPN dans le profil téléphonique commun :

1. Naviguez vers le **périphérique** > les **paramètres de périphérique** > **profil téléphonique commun**.



2. Écrivez les informations VPN :

The image shows a configuration page titled 'Common Phone Profile Configuration'. At the top, there is a toolbar with several icons and labels: 'Save' (floppy disk icon), 'Delete' (red X icon), 'Copy' (document icon), 'Reset' (circular arrow icon), 'Apply Config' (pencil icon), and 'Add New' (plus sign icon). Below the toolbar, there is a section titled 'VPN Information'. This section contains two dropdown menus. The first is labeled 'VPN Group' and has 'Phone' selected. The second is labeled 'VPN Profile' and also has 'Phone' selected.

3. Naviguez vers le **Device > Phone** et confirmez ce profil est assigné à la configuration de téléphone :



Méthode d'authentification de certificat

Il y a deux manières de configurer l'authentification de certificat pour des Téléphones IP : Le fabricant a installé le certificat (MIC) et localement - le certificat significatif (LSC). Référez-vous au [téléphone d'AnyConnect VPN avec l'exemple de configuration d'authentification de certificat](#) afin de choisir la meilleure option pour votre situation.

Quand vous configurez l'authentification de certificat, exportez les certificats (racine CA) du serveur CUCM et importez-les à l'ASA :

1. Procédure de connexion au CUCM.
2. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION > la Gestion unifiées de Sécurité > de certificat**.
3. Trouvez la fonction de proxy d'autorité de certification (CAPF) ou Cisco_Manufacturing_CA ; le type de certificat dépend au moment si vous authentification avez utilisé MIC ou LSC certificat.
4. Téléchargez le fichier à l'ordinateur local.

Une fois que les fichiers sont téléchargés, ouvrez une session à l'ASA par le CLI ou l'ASDM et importez le certificat comme certificat de CA.

Certificate List (1 - 21 of 21)		
Find Certificate List where File Name begins with <input type="text"/> Find Clear Filter + -		
Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco Manufacturing CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

Par défaut, tous les téléphones qui prennent en charge le VPN sont préchargés avec MICs. Les 7960 et 7940 téléphones modèles ne sont pas livré avec une MIC et exigent une procédure d'installation spéciale de sorte que le LSC s'enregistre sécurisé.

Les plus nouveaux Téléphones IP de Cisco (8811, 8841, 8851, et 8861) incluent les Certificats MIC qui sont signés par le nouveau SHA2 de fabrication CA :

- La version 10.5(1) CUCM inclut et fait confiance aux nouveaux Certificats SHA2.
- Si vous exécutez une version plus tôt CUCM, vous pourriez être requis de télécharger le nouveau certificat de CA de fabrication et :

Téléchargez-le à la CAPF-confiance de sorte que les téléphones puissent authentifier avec CAPF afin d'obtenir un LSC.

Téléchargez-le à la CallManager-confiance si vous voulez permettre aux téléphones pour authentifier avec une MIC pour le SIP 5061.

Conseil : Cliquez sur [ce lien](#) afin d'obtenir le SHA2 CA si le CUCM exécute actuellement une version antérieure.

Attention : Cisco recommande que vous utilisiez MICs pour l'installation LSC seulement. Cisco prend en charge des LSC pour l'authentification de la connexion de TLS avec le CUCM. Puisque les certificats racine MIC peuvent être compromis, les clients qui configurent des téléphones pour utiliser MICs pour l'authentification de TLS ou pour n'importe quel autre but font ainsi à leur propre risque. Cisco n'assume aucune

responsabilité si le MICs sont compromis.

Par défaut, si un LSC existe dans le téléphone, l'authentification utilise le LSC, indépendamment de si une MIC existe dans le téléphone. Si une MIC et un LSC existent dans le téléphone, l'authentification utilise le LSC. Si un LSC n'existe pas dans le téléphone, mais une MIC existe, l'authentification utilise la MIC.

Note: Souvenez-vous que, pour l'authentification de certificat, vous devriez exporter le certificat ssl de l'ASA et l'importer au CUCM.

Contrôle d'ID d'hôte

Si le nom commun (NC) dans le sujet du certificat n'apparie pas l'URL (groupe-URL) les téléphones les utilisent afin de se connecter à l'ASA par le VPN, désactiver le contrôle d'ID d'hôte sur le CUCM ou utiliser un certificat dans l'ASA qui correspondance cet URL sur l'ASA.

C'est nécessaire quand le certificat ssl de l'ASA est un certificat de masque, le certificat ssl contient un SAN différent (nom alternatif soumis), ou l'URL a été créé avec l'adresse IP au lieu du nom de domaine complet (FQDN).

C'est un exemple d'un log de téléphone IP quand la NC du certificat n'apparie pas l'URL que le téléphone essaye d'atteindre.

```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

Afin de désactiver l'hôte que l'ID signent le CUCM, naviguez vers la **fonctionnalité avancée** > le **profil VPN** > **VPN** :

Tunnel Parameters	
MTU*	1290
Fail to Connect*	30
<input type="checkbox"/> Enable Host ID Check	

Dépannage supplémentaire

Logs et debugs à utiliser dans l'ASA

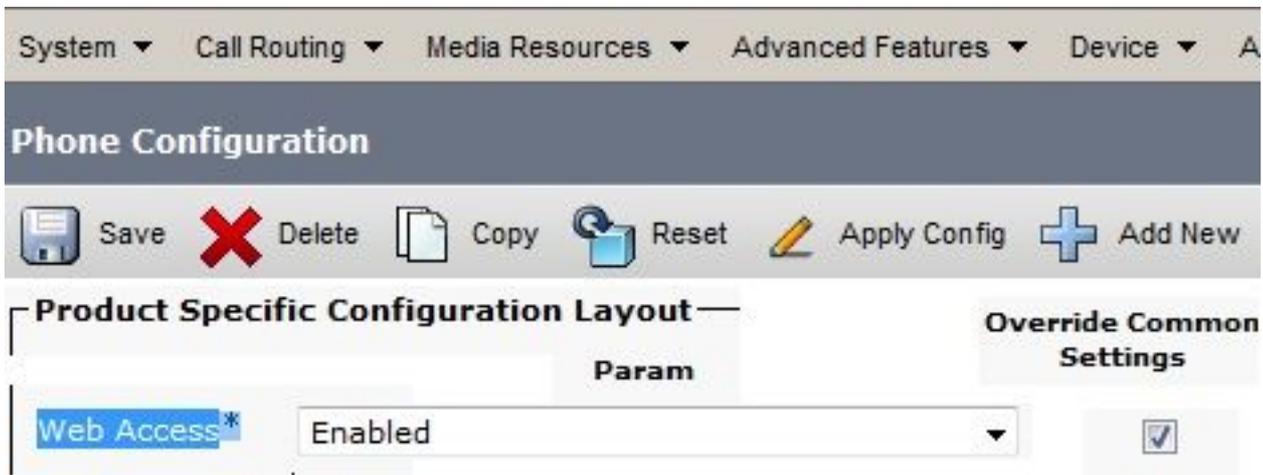
Sur l'ASA, vous pouvez activer ces derniers met au point et se connecte pour le dépannage :

```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

Note: Dans un grand déploiement avec une charge élevée des utilisateurs d'AnyConnect, Cisco recommande que vous n'activiez pas l'**anyconnect de webvpn de débogage**. Sa sortie ne peut pas être filtrée par l'adresse IP, ainsi un grand nombre d'informations pourraient être créées.

Logs de téléphone IP

Afin d'accéder aux logs de téléphone, activez la caractéristique d'accès au Web. Ouvrez une session au CUCM, et naviguez vers le **Device > Phone > la configuration de téléphone**. Trouvez le téléphone IP sur lequel vous voulez activer cette caractéristique, et trouvez la section pour l'accès au Web. Appliquez les modifications de configuration au téléphone IP :



Une fois que vous activez le service et remettez à l'état initial le téléphone afin d'injecter cette nouvelle caractéristique, vous pouvez accéder au téléphone IP ouvre une session le navigateur ; utilisez l'adresse IP du téléphone à partir d'un ordinateur avec l'accès à ce sous-réseau. Allez aux logs de console et vérifiez les cinq fichiers journal. Puisque le téléphone remplace les cinq fichiers, vous devez vérifier tous ces fichiers dans la commande trouvez les informations que vous recherchez.



Console Logs

Cisco Unified IP Phone CP-7962G (SEP8CB64F576113)

[Device Information](#)

[Network Configuration](#)

Network Statistics

[Ethernet Information](#)

[Access](#)

[Network](#)

Device Logs

[Console Logs](#)

[/FS/cache/fsck.fd0a.log](#)

[/FS/cache/fsck.fd1a.log](#)

[/FS/cache/log181](#)

[/FS/cache/log182](#)

3 [/FS/cache/log178](#)

[/FS/cache/log179](#)

[/FS/cache/log180](#)

Questions corrélées entre les logs ASA et les logs de téléphone IP

C'est un exemple de la façon de corréliser les logs de l'ASA et du téléphone IP. Dans cet exemple, les informations parasites du certificat sur l'ASA n'appartiennent pas aux informations parasites du certificat sur le fichier de configuration du téléphone parce que le certificat sur l'ASA a été remplacé par un certificat différent.

Logs ASA

```
%ASA-7-725012: Device chooses cipher : AES128-SHA for the SSL session with
client outside:172.16.250.9/50091
%ASA-7-725014: SSL lib error. Function: SSL3_READ_BYTES Reason: tlsv1 alert
unknown ca
%ASA-6-725006: Device failed SSL handshake with client outside:172.16.250.9/50091
```

Logs de téléphone

```
902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: cert_vfy_cb: depth:1 of 1, subject:
</CN=10.198.16.140/unstructuredName=10.198.16.140>
906: NOT 10:19:27.365344 VPNC: cert_vfy_cb: depth:1 of 1, pre_err: 18 (self signed certificate)
907: NOT 10:19:27.368304 VPNC: cert_vfy_cb: peer cert saved: /tmp/leaf.crt
908: NOT 10:19:27.375718 SECD: Leaf cert hash = 1289B8A7AA9FFD84865E38939F3466A61B5608FC
909: ERR 10:19:27.376752 SECD: ERROR:secLoadFile: file not found </tmp/issuer.crt>
910: ERR 10:19:27.377361 SECD: Unable to open file /tmp/issuer.crt
911: ERR 10:19:27.420205 VPNC: VPN cert chain verification failed, issuer certificate not found
and leaf not trusted
912: ERR 10:19:27.421467 VPNC: ssl_state_cb: TLSv1: write: alert: fatal:
unknown CA
913: ERR 10:19:27.422295 VPNC: alert_err: SSL write alert: code 48, unknown CA
914: ERR 10:19:27.423201 VPNC: create_ssl_connection: SSL_connect ret -1 error 1
915: ERR 10:19:27.423820 VPNC: SSL: SSL_connect: SSL_ERROR_SSL (error 1)
916: ERR 10:19:27.424541 VPNC: SSL: SSL_connect: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
917: ERR 10:19:27.425156 VPNC: create_ssl_connection: SSL setup failure
918: ERR 10:19:27.426473 VPNC: do_login: create_ssl_connection failed
919: NOT 10:19:27.427334 VPNC: vpn_stop: de-activating vpn
920: NOT 10:19:27.428156 VPNC: vpn_set_auto: auto -> auto
921: NOT 10:19:27.428653 VPNC: vpn_set_active: activated -> de-activated
922: NOT 10:19:27.429187 VPNC: set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
923: NOT 10:19:27.429716 VPNC: set_login_state: VPNC : 1 (LoggingIn) --> 3
(LoginFailed)
924: NOT 10:19:27.430297 VPNC: vpnc_send_notify: notify type: 1 [LoginFailed]
925: NOT 10:19:27.430812 VPNC: vpnc_send_notify: notify code: 37
[SslAlertSrvrCert]
926: NOT 10:19:27.431331 VPNC: vpnc_send_notify: notify desc: [alert: Unknown
```

CA (server cert)]

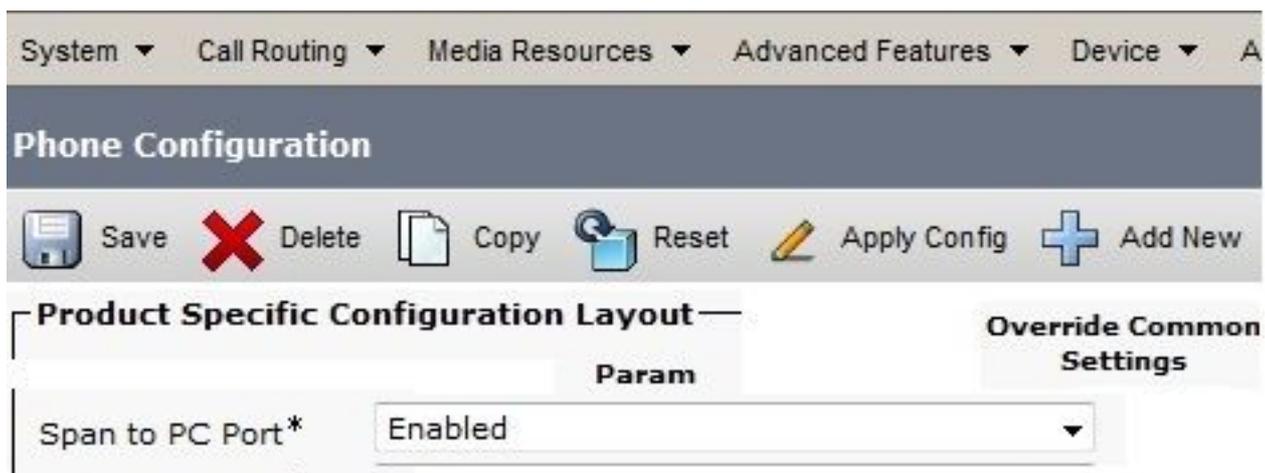
927: NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to pid 14

928: ERR 10:19:27.432467 VPNC: protocol_handler: login failed

Envergure à la caractéristique de port PC

Vous pouvez connecter un ordinateur directement à un téléphone. Le téléphone a un port de commutateur dans l'avion arrière.

Configurez le téléphone comme le faisiez précédemment vous, pour activer l'envergure au port PC sur le CUCM, et pour appliquer la configuration. Le téléphone commence à envoyer une copie de chaque trame au PC. Utilisation Wireshark en mode promiscueux afin de capturer le trafic pour l'analyse.



Modifications de configuration de téléphone IP tandis que relié par VPN

Une question commune est si vous pouvez modifier la configuration du VPN tandis que le téléphone IP est connecté hors du réseau par AnyConnect. La réponse est oui, mais vous devriez confirmer quelques paramètres de configuration.

Apportez les modifications nécessaires du CUCM, puis appliquez les modifications au téléphone. Il y a trois options (appliquez le config, remettent à l'état initial, reprise) de pousser la nouvelle configuration au téléphone. Bien que chacune des trois options démonte le VPN du téléphone et de l'ASA, vous pouvez rebrancher automatiquement si vous utilisez l'authentification de certificat ; si vous utilisez l'Authentification, autorisation et comptabilité (AAA), vous êtes incité pour vos

qualifications de nouveau.



Note: Quand le téléphone IP est dans le côté distant, il reçoit normalement une adresse IP d'un serveur DHCP externe. Pour que le téléphone IP reçoive la nouvelle configuration du CUCM, il devrait contacter le serveur TFTP dans le bureau central. Normalement le CUCM est le même serveur TFTP.

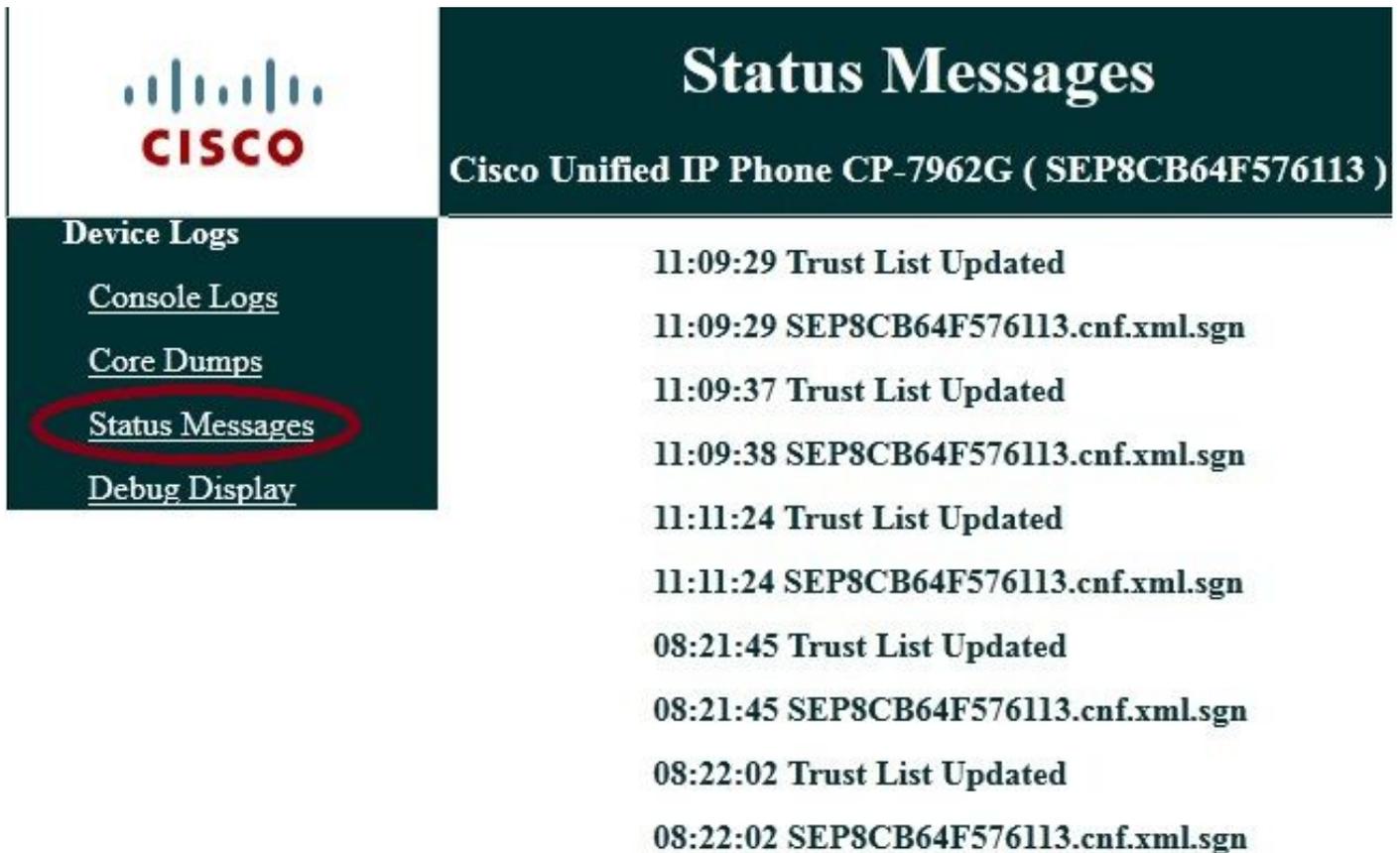
Afin de recevoir les fichiers de configuration avec les modifications, confirmez que l'adresse IP pour le serveur TFTP est installée correctement dans les paramètres réseau dans le téléphone ; pour la confirmation, l'option d'utilisation 150 du serveur DHCP ou manuellement réglés le TFTP au téléphone. Ce serveur TFTP est accessible par une session d'AnyConnect.

Si le téléphone IP reçoit le serveur TFTP d'un serveur DHCP local mais cette adresse est incorrecte, vous pouvez employer l'option de serveur alternative TFTP afin d'ignorer l'adresse IP pour serveur TFTP fournie par le serveur DHCP. Cette procédure décrit comment appliquer le serveur alternatif TFTP :

1. Naviguez vers le **Settings > Network Configuration > la configuration d'ipv4**.
2. Défilement à l'option alternative TFTP.
3. Appuyez sur la touche douce d'oui pour le téléphone pour utiliser un serveur de l'alternative TFTP ; autrement, n'appuyez sur l'aucune touche douce. Si l'option est verrouillée, presse * * # afin de la déverrouiller.
4. Appuyez sur la touche **Save**.
5. Appliquez le serveur alternatif TFTP sous l'option du serveur 1 TFTP.

Passez en revue les messages d'état dans le navigateur Web ou dans les menus du téléphone

directement afin de confirmer que le téléphone reçoit les informations correctes. Si la transmission est installée correctement, vous voyez des messages de ce type :



The image shows a screenshot of a Cisco Unified IP Phone interface. On the left, there is a navigation menu with the following items: **Device Logs**, Console Logs, Core Dumps, Status Messages (highlighted with a red oval), and Debug Display. The main area on the right is titled **Status Messages** and displays a list of messages for the phone model **Cisco Unified IP Phone CP-7962G (SEP8CB64F576113)**. The messages are as follows:

- 11:09:29 Trust List Updated
- 11:09:29 SEP8CB64F576113.cnf.xml.sgn
- 11:09:37 Trust List Updated
- 11:09:38 SEP8CB64F576113.cnf.xml.sgn
- 11:11:24 Trust List Updated
- 11:11:24 SEP8CB64F576113.cnf.xml.sgn
- 08:21:45 Trust List Updated
- 08:21:45 SEP8CB64F576113.cnf.xml.sgn
- 08:22:02 Trust List Updated
- 08:22:02 SEP8CB64F576113.cnf.xml.sgn

Si le téléphone ne peut pas récupérer les informations du serveur TFTP, vous recevez des messages d'erreur TFTP :

Status Messages

Cisco Unified IP Phone CP-7962G (SEP8CB64F578B2C)

11:51:10 Trust List Update Failed

11:51:10 TFTP Error : SEP8CB64F578B2C.cnf.xml.sgn

11:53:09 Trust List Update Failed

11:54:10 Trust List Update Failed

11:54:10 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:54:31 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:55:18 Trust List Update Failed

11:55:39 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:58:00 Trust List Update Failed

11:58:00 TFTP Error : SEP8CB64F578B2C.cnf.xml.sgn

Renouvellement du certificat ssl ASA

Si vous faites installer un téléphone fonctionnel d'AnyConnect VPN mais votre certificat ssl ASA est sur le point d'expirer, vous n'avez pas besoin d'apporter tous les Téléphones IP au site principal afin d'injecter les nouveaux Certificats SSL au téléphone ; vous pouvez ajouter les nouveaux Certificats tandis que le VPN est connecté.

Si vous avez exporté ou avez importé le certificat de CA de racine de l'ASA au lieu du certificat d'identité et si vous voulez continuer à utiliser le même constructeur (CA) pendant ce renouvellement, il n'est pas nécessaire de changer le certificat dans le CUCM parce qu'il reste le même. Mais, si vous utilisez le certificat d'identité, cette procédure est nécessaire ; autrement, la valeur de hachage entre l'ASA et le téléphone IP ne s'assortissent pas, et la connexion n'est pas faite confiance par le téléphone.

1. Renouvelez le certificat sur l'ASA.

Note: Pour des détails, référez-vous à [ASA 8.x : Renouvelez et installez le certificat ssl avec](#)

[l'ASDM](#). Créez un point de confiance distinct et n'appliquez pas ce nouveau certificat avec le **<name> de point de confiance SSL en dehors de la** commande jusqu'à ce que vous ayez appliqué le certificat à tous les Téléphones IP VPN.

2. Exportez le nouveau certificat.
3. Importez le nouveau certificat au CUCM comme certificat de Téléphone-VPN-confiance.
Note: Rendez-vous compte de [CSCuh19734](#) téléchargeant des CERT avec la même NC **remplacera le vieux CERT en Téléphone-VPN-confiance**
4. Naviguez vers la configuration de passerelle VPN dans le CUCM, et appliquez le nouveau certificat. Vous avez maintenant les deux Certificats : le certificat qui est sur le point d'expirer et le nouveau certificat qui n'a pas été appliqué à l'ASA encore.
5. Appliquez cette nouvelle configuration au téléphone IP. Naviguez **pour appliquer le config > remis à l'état initial > reprise** afin d'injecter les nouvelles modifications de configuration au téléphone IP par le tunnel VPN. Assurez-vous que tous les Téléphones IP sont connectés par le VPN et qu'ils peuvent accéder le serveur TFTP par le tunnel.
6. Utilisation TFTP de vérifier les messages d'état et le fichier de configuration afin de confirmer que le téléphone IP a reçu le fichier de configuration avec les modifications.
7. Appliquez le nouveau point de confiance SSL dans l'ASA, et remplacez le certificat ancien.

Note: Si le certificat ssl ASA est déjà expiré et si les Téléphones IP ne peuvent pas se connecter par AnyConnect ; vous pouvez pousser les modifications (telles que les nouvelles informations parasites de certificat ASA) au téléphone IP. Placez manuellement le TFTP dans le téléphone IP à une adresse IP publique ainsi le téléphone IP peut récupérer les informations de là. Utilisez un serveur du public TFTP pour héberger le fichier de configuration ; un exemple est de créer une transmission du port sur l'ASA et de réorienter le trafic au serveur interne TFTP.