

# AnyConnect VPN فتاه عاطخأ فاشكتسأ اهحالصإو CUCM و ASA و IP فتاوه

## المحتويات

[المقدمة](#)

[معلومات أساسية](#)

[تأكيد ترخيص هاتف VPN على ASA](#)

[تصدير CUCM غير المقيد وتصديره](#)

[القضايا المشتركة في هيئة المعايير المالية](#)

[شهادات الاستخدام في ASA](#)

[TrustPoint/Certificate لتصدير ASA واستيراد CUCM](#)

[يقدم ASA شهادة ECDSA موقعة ذاتيا بدلا من شهادة RSA التي تم تكوينها](#)

[قاعدة بيانات خارجية لمصادقة مستخدمي هاتف IP](#)

[تطابقات الشهادة بين شهادة ASA وقائمة ثقة هاتف VPN](#)

[فحص تجزئة SHA1](#)

[تنزيل ملف تكوين هاتف IP](#)

[فك ترميز التجزئة](#)

[موازنة حمل شبكة VPN وهواتف بروتوكول الإنترنت \(IP\)](#)

[هواتف CSD و IP](#)

[ASA LOG](#)

[تصحيح أخطاء ASA](#)

[قواعد DAP](#)

[القيم الموروثة من DfltGrpPolicy أو مجموعات أخرى](#)

[شفرات التشفير المدعومة](#)

[القضايا المشتركة في إتفاقية حفظ السلام في القرن الأفريقي](#)

[إعدادات VPN غير مطبقة على هاتف IP](#)

[أسلوب مصادقة الشهادة](#)

[التحقق من معرف المضيف](#)

[أستكشاف الأخطاء وإصلاحها بشكل إضافي](#)

[السجلات وتصحيح الأخطاء لاستخدامها في ASA](#)

[سجلات هاتف IP](#)

[المشاكل المرتبطة بين سجلات ASA وسجلات هاتف IP](#)

[ASA LOG](#)

[سجلات الهاتف](#)

[فسحة بين دعامين إلى pc ميناء سمة](#)

[تغييرات تكوين هاتف IP أثناء الاتصال بشبكة VPN](#)

[تحديد شهادة ASA SSL](#)

## المقدمة

يصف هذا المستند كيفية أكتشاف أخطاء هواتف IP التي تستخدم بروتوكول طبقة مأخذ التوصيل الآمنة ((SSL)) باستخدامه كبوابة شبكة VPN ويهدف الاتصال بمدير الاتصالات الموحدة (CUCM) من Cisco الذي يتم استخدامه كخادم صوت.

للحصول على أمثلة تكوين من AnyConnect بهواتف VPN، ارجع إلى هذه المستندات:

• [SSLVPN مع مثال تكوين هواتف IP](#)

• [هاتف AnyConnect VPN مع مثال تكوين مصادقة الشهادة](#)

## معلومات أساسية

قبل نشر شبكة VPN الخاصة بـ SSL مع هواتف IP، تأكد من استيفاء المتطلبات الأولية لتراخيص AnyConnect لـ ASA وإصدار التصدير المقيد للولايات المتحدة من CUCM.

## تأكيد ترخيص هاتف VPN على ASA

يتيح ترخيص هاتف شبكة VPN الميزة في ASA. لتأكيد عدد المستخدمين الذين يمكنهم الاتصال بـ AnyConnect (سواء كان هاتف IP أم لا)، تحقق من ترخيص AnyConnect Premium SSL. ارجع إلى [ما هو ترخيص ASA المطلوب لاتصالات IP Phone و VPN المحمولة؟](#) للحصول على مزيد من التفاصيل.

على ASA، أستخدم الأمر `show version` للتحقق من تمكين الميزة. يختلف اسم الترخيص مع إصدار ASA:

• ASA الإصدار x.8.0: اسم الترخيص هو AnyConnect for Linksys Phone.

• ASA الإصدار x.8.2 والإصدارات الأحدث: اسم الترخيص هو AnyConnect لهاتف Cisco VPN.

هنا مثال لـ ASA إطلاق x.8.0:

```
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
```

وفيما يلي مثال على إصدارات ASA 8.2.x والإصدارات الأحدث:

```
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
```

## تصدير CUCM غير المقيد وتصديره

يجب نشر إصدار U.S مقيد للتصدير من CUCM لميزة هاتف VPN.

إذا كنت تستخدم إصدارا غير مقيد من CUCM من إنتاج الولايات المتحدة، فلاحظ ما يلي:

يتم تعديل تكوينات أمان هاتف IP من أجل تعطيل إرسال الإشارات وتشغيل الوسائط، وهذا يتضمن التشفير الذي توفره ميزة هاتف شبكة VPN.

- لا يمكنك تصدير تفاصيل شبكة VPN من خلال الاستيراد/التصدير.
- لا يتم عرض خانة الاختيار الخاصة بتكوين ملف تعريف VPN وبوابة VPN ومجموعة VPN وميزة VPN.

**ملاحظة:** بمجرد الترقية إلى الإصدار غير المقيد من CUCM الخاص بتصدير الولايات المتحدة، لا يمكنك الترقية لاحقا إلى هذا البرنامج أو إجراء تثبيت جديد له، أو إصدار التصدير المقيد الخاص بالولايات المتحدة من هذا البرنامج.

# القضايا المشتركة في هيئة المعايير المالية

ملاحظة: يمكنك استخدام [Cisco CLI Analyzer](#) (محلل واجهة سطر الأوامر من Cisco) (العملاء المسجلون فقط) لعرض تحليل مخرج الأمر `show`. يجب عليك أيضا الرجوع إلى [المعلومات المهمة حول أوامر التصحيح من مستند Cisco](#) قبل استخدام أوامر `debug`.

## شهادات الاستخدام في ASA

على ASA، يمكنك استخدام شهادات SSL ذاتية التوقيع، وشهادات SSL من جهات خارجية، وشهادات حرف بدل، ويضمن أي من هذه الاتصال بين هاتف IP و ASA.

يمكن استخدام شهادة هوية واحدة فقط لأنه يمكن تعيين شهادة واحدة فقط لكل واجهة.

بالنسبة لشهادات SSL الخاصة بجهة خارجية، قم بتثبيت السلسلة الكاملة في ASA، وقم بتضمين أي شهادات متوسطة أو شهادات جذر.

## TrustPoint/Certificate لتصدير ASA واستيراد CUCM

يجب تصدير الشهادة التي يقدمها ASA إلى هاتف IP أثناء تفاوض SSL من ASA واستيرادها إلى CUCM. تحقق من نقطة الثقة المعينة للواجهة التي تتصل بها هواتف IP لمعرفة الشهادة التي سيتم تصديرها من ASA.

أستخدم الأمر `show run ssl` للتحقق من TrustPoint (الشهادة) التي سيتم تصديرها. راجع [هاتف AnyConnect VPN مع مثال تكوين مصادقة الشهادة](#) للحصول على مزيد من المعلومات.

ملاحظة: إذا كنت قد قمت بنشر شهادة من جهة خارجية إلى واحد أو أكثر من ASA، فأنت بحاجة إلى تصدير كل شهادة هوية من كل ASA ثم استيرادها إلى CUCM كتنقة بالهاتف VPN.

يقدم ASA شهادة ECDSA موقعة ذاتيا بدلا من شهادة RSA التي تم تكوينها

عند حدوث هذه المشكلة، يتعذر على الهواتف النموذجية الأحدث الاتصال، بينما لا تواجه الهواتف النموذجية الأقدم أي مشاكل. هنا السجلات على الهاتف عند حدوث هذه المشكلة:

```
(VPNC: -protocol_handler: SSL dpd 30 sec from SG (enabled
VPNC: -protocol_handler: connect: do_dtls_connect
VPNC: -do_dtls_connect: udp_connect
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: binding sock to eth0 IP 63.85.30.39
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: connecting to 63.85.30.34:443
VPNC: -udp_connect: connected to 63.85.30.34:443
VPNC: -do_dtls_connect: create_dtls_connection
VPNC: -create_dtls_connection: cipher list: AES256-SHA
VPNC: -create_dtls_connection: calling SSL_connect in non-block mode
VPNC: -dtls_state_cb: DTLS: SSL_connect: before/connect initialization
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: DTLS1 read hello verify request A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 flush data
VPNC: -dtls_state_cb: DTLS: write: alert: fatal:illegal parameter
VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
(VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1
:VPNC: -DTLS: SSL_connect: error:140920C5:SSL routines:SSL3_GET_SERVER_HELLO
old session cipher not returned VPNC: -create_dtls_connection: DTLS setup failure, cleanup VPNC:
-do_dtls_connect: create_dtls_connection failed VPNC: -protocol_handler: connect:
do_dtls_connect failed VPNC: -protocol_handler: connect : err: SSL success DTLS fail
```

في الإصدارات 9.4.1 والإصدارات الأحدث، يتم دعم تشفير المنحنى البيضاوي ل SSL/TLS. عندما يتصل عميل SSL VPN قابل للمنحنى الاهليلجي مثل نموذج هاتف جديد ب ASA، يتم التفاوض على مجموعة تشفير المنحنى البيضاوي، ويقدم ASA عميل SSL VPN مع شهادة منحني بيضاوي، حتى عند تكوين الواجهة التي تتطابق مع نقطة ثقة تستند إلى RSA. لمنع ASA من تقديم شهادة SSL موقعة ذاتيا، يجب على المسؤول إزالة مجموعات التشفير التي تتوافق عبر أمر تشفير SSL. على سبيل المثال، لواجهة تم تكوينها باستخدام نقطة اتصال RSA، يمكن للمسؤول تنفيذ هذا الأمر حتى يتم التفاوض حول الشفرة المستندة إلى RSA فقط:

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

مع التنفيذ من CISCO بق [CSCuu02848](#) id، تعطى الأولوية إلى التشكيل. يتم استخدام الشهادات التي تم تكوينها بشكل صريح دائما. تستخدم الشهادات الموقعة ذاتيا فقط في غياب شهادة تم تكوينها.

شفرة العميل المقترحة	شهادة RSA فقط	شهادة RSA فقط	شهادة RSA فقط	شهادة RSA فقط
شفرة RSA فقط	يستخدم شهادة RSA	يستخدم شهادة RSA الموقعة ذاتيا	يستخدم تشفير RSA	يستخدم تشفير RSA
شهادة RSA فقط	يستخدم شهادة RSA	يستخدم شهادة RSA الموقعة ذاتيا	يستخدم تشفير RSA	يستخدم تشفير RSA
شهادة RSA فقط	يستخدم شهادة RSA	يستخدم شهادة RSA الموقعة ذاتيا	يستخدم تشفير RSA	يستخدم تشفير RSA
شهادة RSA فقط	يستخدم شهادة RSA	يستخدم شهادة RSA الموقعة ذاتيا	يستخدم تشفير RSA	يستخدم تشفير RSA

يستخدم شهادة EC	يستخدم شهادة EC	يستخدم شهادة EC	فشل الاتصال	شفرات EC فقط (نادرة)
يستخدم شفرات EC ذاتية التوقيع	يستخدم شفرات EC	يستخدم شفرات EC		
يستخدم شفرات EC	يستخدم شهادة EC	يستخدم شهادة EC	يستخدم شهادة RSA	كلا الشفرين فقط
يستخدم شفرات EC ذاتية التوقيع	يستخدم شفرات EC	يستخدم شفرات EC	يستخدم تشفير RSA	

## قاعدة بيانات خارجية لمصادقة مستخدمى هاتف IP

يمكنك استخدام قاعدة بيانات خارجية لمصادقة مستخدمى هاتف IP. يمكن استخدام بروتوكولات مثل البروتوكول الخفيف للوصول إلى الدليل (LDAP) أو طلب المصادقة عن بعد في خدمة المستخدم (RADIUS) لمصادقة مستخدمى هاتف شبكة VPN.

## تطابقات الشهادة بين شهادة ASA وقائمة ثقة هاتف VPN

تذكر أنه يجب عليك تنزيل الشهادة المعينة لواجهة ASA SSL وتحميلها كشهادة ثقة هاتف VPN في CUCM. قد تتسبب الظروف المختلفة في عدم تطابق تجزئة هذه الشهادة المقدمة من قبل ASA مع التجزئة التي يقوم خادم CUCM بتوليدها ودفعها إلى هاتف VPN من خلال ملف التكوين.

بمجرد اكتمال التكوين، اختبر اتصال VPN بين هاتف IP و ASA. إذا استمر فشل الاتصال، فتتحقق مما إذا كانت تجزئة شهادة ASA تطابق التجزئة التي يتوقعها هاتف IP:

1. تحقق من تجزئة خوارزمية التجزئة الآمنة 1 (SHA1) التي يقدمها ASA.
2. استخدم TFTP لتنزيل ملف تكوين هاتف IP من CUCM.
3. فك ترميز التجزئة من النظام السداسي العشري إلى القاعدة 64 أو من القاعدة 64 إلى النظام السداسي العشري.

## فحص تجزئة SHA1

يعرض ASA الشهادة المطبقة باستخدام الأمر `ssl trustPoint` على الواجهة التي يتصل بها هاتف IP. للتحقق من هذه الشهادة، افتح المستعرض (في هذا المثال، Firefox)، وأدخل عنوان `URL (group-url)` الذي يجب أن تتصل به الهواتف:

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**

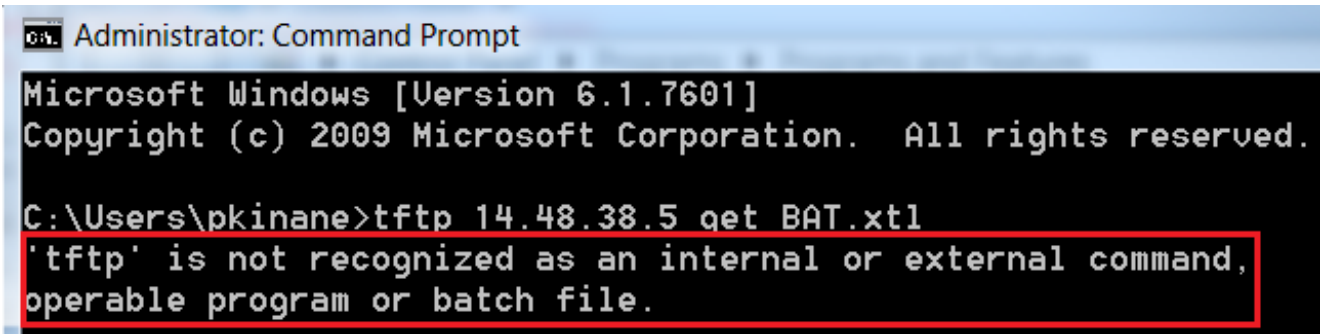
3 SHA1 Fingerprint E5:7E:81:EA:99:54:C1:44:97:66:78:D0:E2:41:8C:DF:79:A9:31:76

MD5 Fingerprint D7:10:78:FB:61:A2:F6:C2:01:07:6C:03:DE:17:EF:F9

تنزيل ملف تكوين هاتف IP

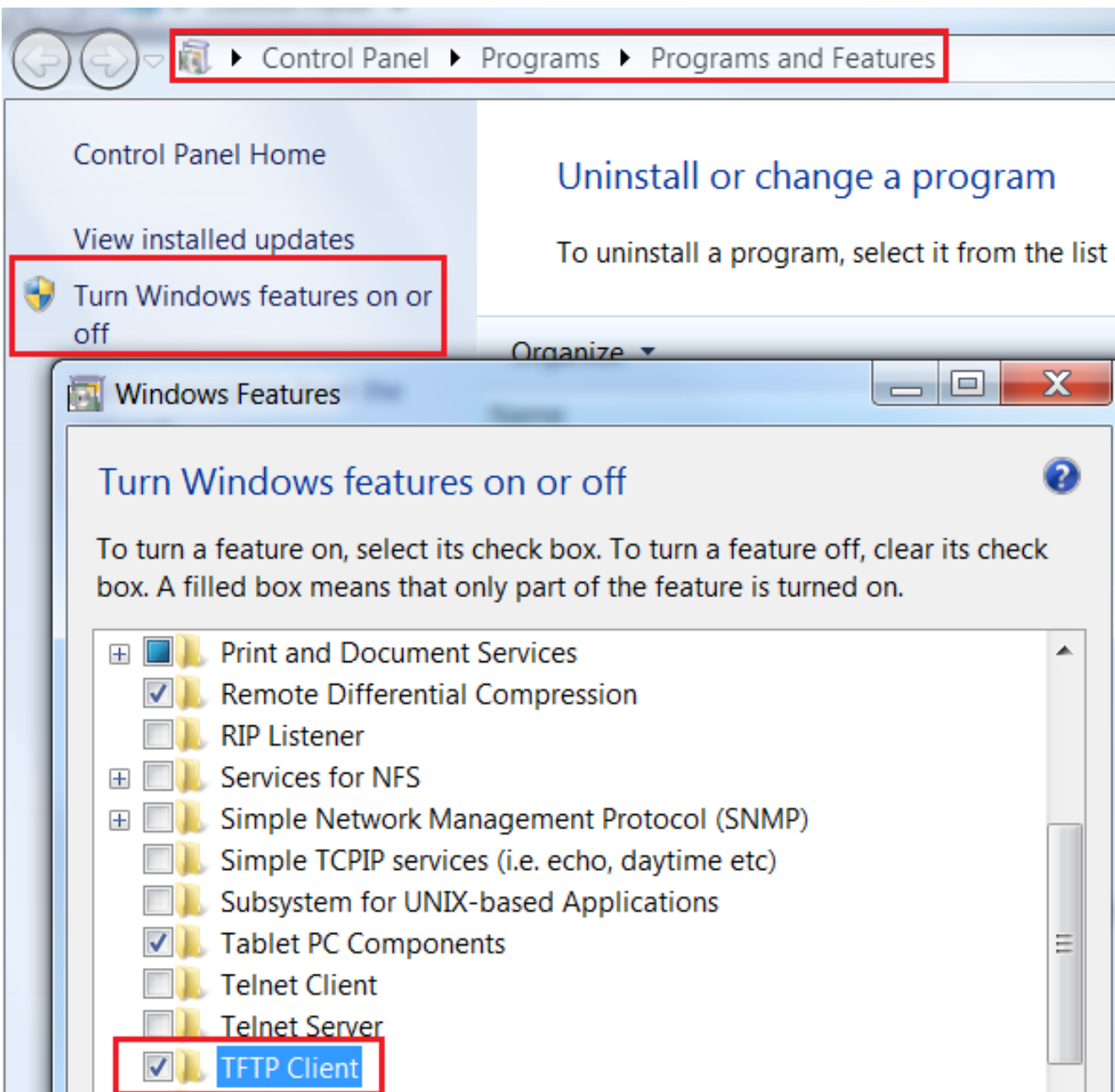
من كمبيوتر به وصول مباشر إلى CUCM، قم بتنزيل ملف تكوين TFTP للهاتف الذي به مشاكل في الاتصال. طريقتان للتنزيل هما:

1. افتح جلسة CLI في Windows، واستخدم الـ `TFTP -i` نادل <Phone Mac> يحصل `SEP` `>.cnf.xml` أمر.  
ملاحظة: إذا تلقيت خطأ مماثلاً للخطأ أدناه، فيجب عليك تأكيد تمكين ميزة عميل TFTP.



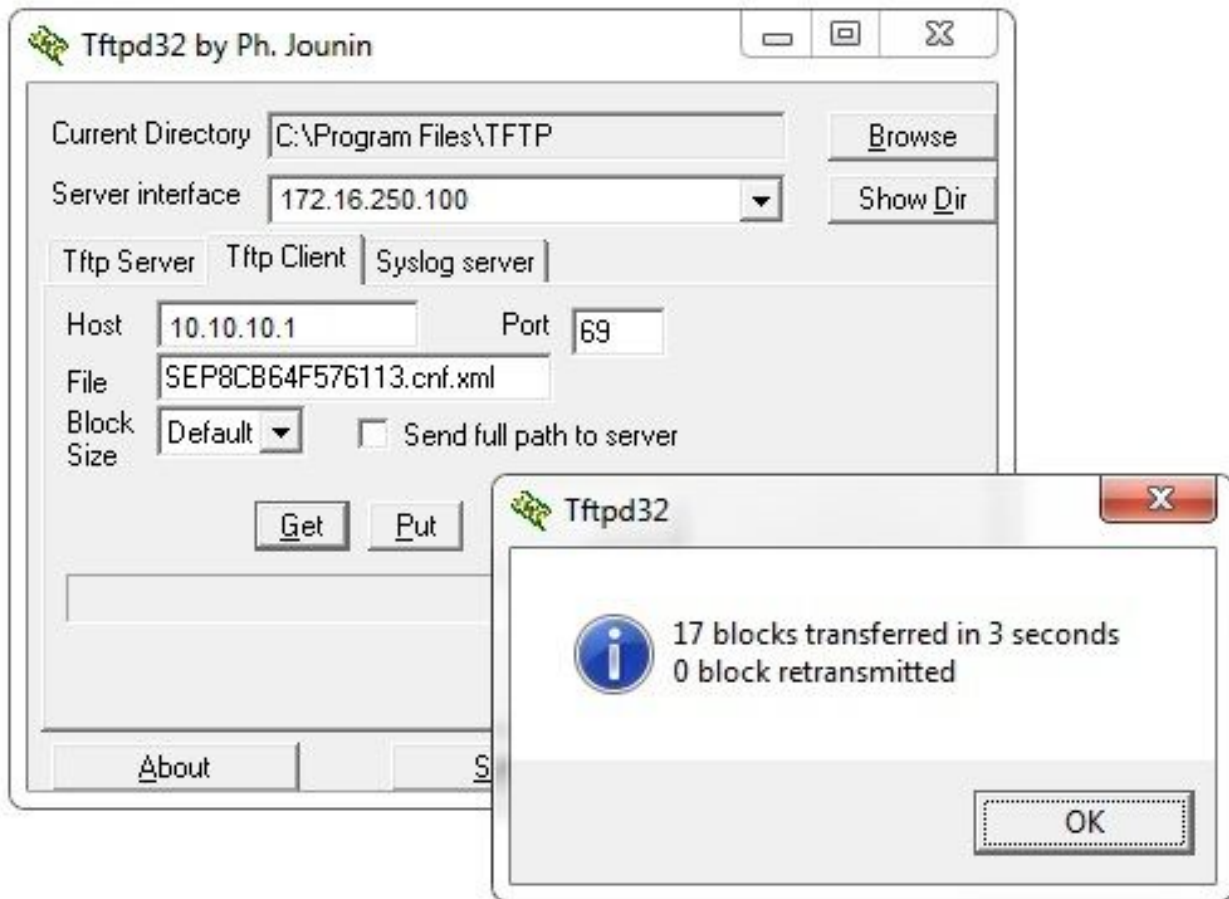
```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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. استخدم تطبيقاً مثل [TFTPD32](#) لتنزيل الملف:





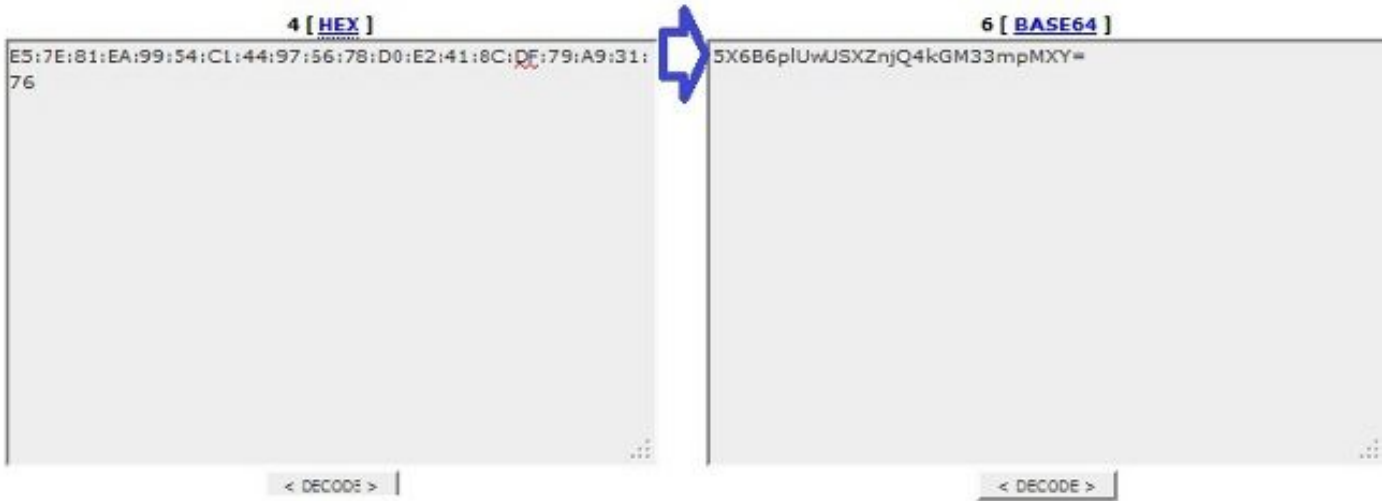
3. بمجرد تنزيل الملف، افتح XML وحدد تكوين *vpnGroup*. يوضح هذا المثال المقطع و *certHash* المراد التحقق منهما:

```

        <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>
        </vpnGroup/>
    
```

فك ترميز التجزئة

تأكد من تطابق قيمتي التجزئة. يعرض المستعرض التجزئة بتنسيق سداسي عشر، بينما يستخدم ملف XML التنسيق base 64، لذا قم بتحويل أحد التنسيقات إلى الآخر لتأكيد المطابقة. هناك العديد من المترجمين المتاحين ، وأحد الأمثلة هو المترجم ، ثنائي .



ملاحظة: إذا لم تتطابق قيمة التجزئة السابقة، لا يثق هاتف VPN في الاتصال الذي يتم التفاوض بشأنه مع ASA، ويفشل الاتصال.

## موازنة حمل شبكة VPN وهواتف بروتوكول الإنترنت (IP)

لا يتم دعم SSL VPN المتوازن للتحميل لهواتف VPN. لا تقوم هواتف VPN بالتحقق من صحة الشهادة الحقيقية ولكن بدلا من ذلك تستخدم التجزئة التي تم دفعها لأسفل من قبل CUCM للتحقق من الخوادم. لأن موازنة حمل VPN هي إعادة توجيه HTTP بشكل أساسي، فإنها تتطلب أن تقوم الهواتف بالتحقق من صحة شهادات متعددة، مما يؤدي إلى الفشل. تتضمن أعراض فشل موازنة حمل الشبكة الخاصة الظاهرية (VPN) ما يلي:

- ينتقل الهاتف بين الخوادم ويستغرق وقتا طويلا بشكل إستثنائي للاتصال أو في نهاية المطاف يفشل.

• تحتوي سجلات الهاتف على رسائل مثل:

```
NOT 20:59:50.051721 VPNC: do_login: got login response :909
NOT 20:59:50.052581 VPNC: process_login: HTTP/1.0 302 Temporary moved :910
(NOT 20:59:50.053221 VPNC: process_login: login code: 302 (redirected :911
NOT 20:59:50.053823 VPNC: process_login: redirection indicated :912
: 'NOT 20:59:50.054441 VPNC: process_login: new 'Location :913
webvpn+/index.html+/
NOT 20:59:50.055141 VPNC: set_redirect_url: new URL :914
<https://xyz1.abc.com:443/+webvpn+/index.html>
```

## هواتف CSD و IP

حاليا، لا تدعم هواتف بروتوكول الإنترنت (IP) سطح المكتب الآمن من Cisco (CSD) ولا تتصل عند تمكين CSD لمجموعة النفق أو بشكل عام في ASA.

أولا، تأكد ما إذا كان ASA قد تم تمكين CSD. دخلت العرض شوط webVPN أمر في ال 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
```

للتحقق من مشاكل CSD أثناء اتصال هاتف IP، راجع السجلات أو تصحيح الأخطاء في ASA.

## ASA LOG

```
ASA-4-724002: Group <VPNPhone> User <Phone> IP <172.6.250.9> WebVPN session not%
.terminated. Cisco Secure Desktop was not running on the client's workstation
```

## تصحيح أخطاء 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>
```

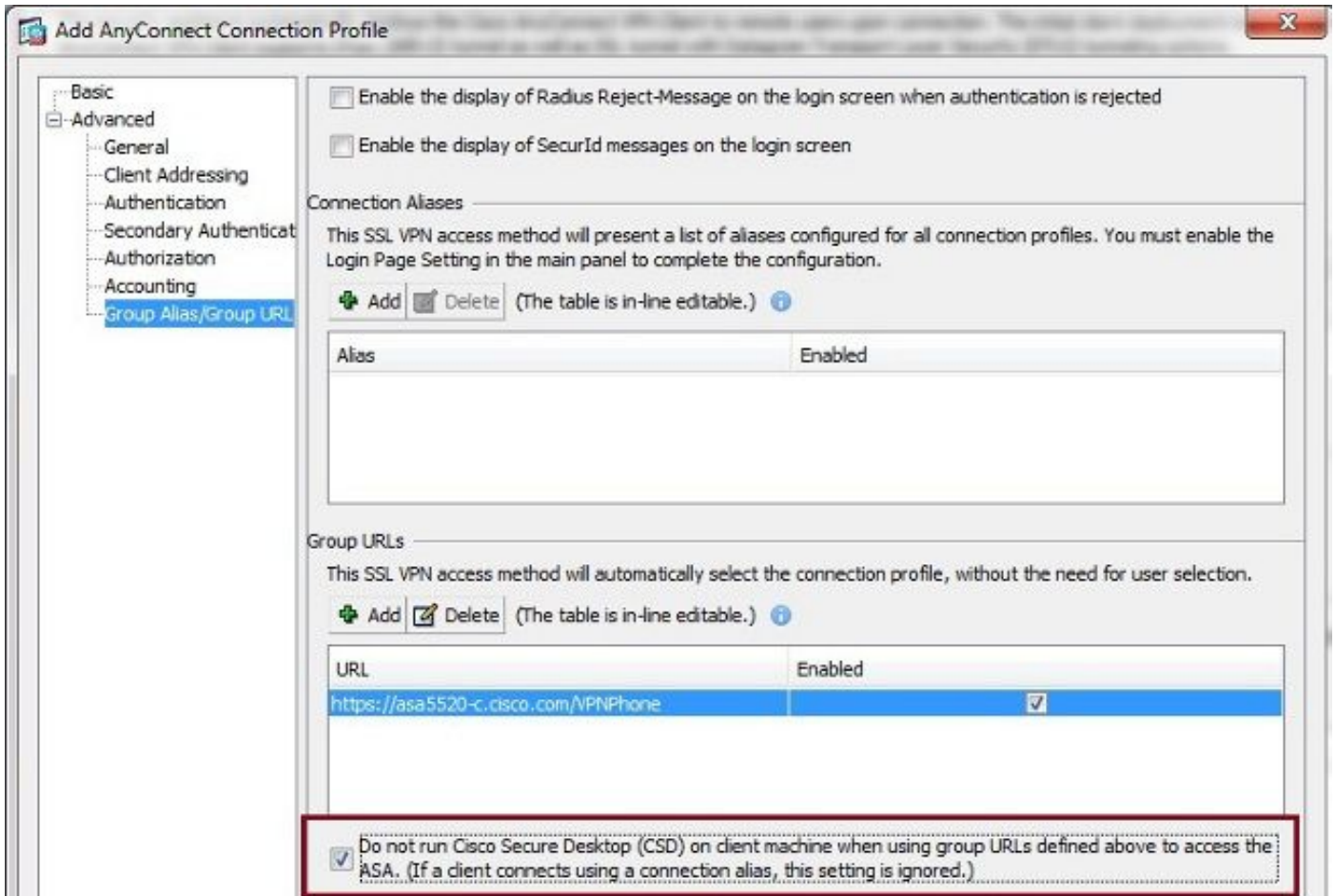
ملاحظة: في عملية نشر كبيرة مع حمل مرتفع من مستخدمي AnyConnect، توصي Cisco بعدم تمكين تصحيح أخطاء WebVPN AnyConnect. لا يمكن تصفية مخرجاته بواسطة عنوان IP، لذلك قد يتم إنشاء كمية كبيرة من المعلومات.

في ASA الإصدارات 8.2 والإصدارات الأحدث، يجب عليك تطبيق الأمر **without-csd** أسفل سمات WebVPN الخاصة بمجموعة النفق:

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

في الإصدارات السابقة من ASA، لم يكن هذا ممكناً، لذلك كان الحل البديل الوحيد هو تعطيل CSD بشكل عام.

في مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco، يمكنك تعطيل CSD لتوصيف توصيل معين كما هو موضح في هذا المثال:



ملاحظة: أستخدم عنوان URL للمجموعة لإيقاف تشغيل ميزة CSD.

لا تقوم معظم عمليات النشر بتوصيل هواتف IP بالجهاز ASA فحسب، بل تقوم أيضا بتوصيل أنواع مختلفة من الأجهزة (Microsoft و Linux و Mac OS) والأجهزة المحمولة (Android و iOS). ولهذا السبب، من الطبيعي العثور على تكوين موجود لقواعد سياسة الوصول الديناميكي (DAP)، حيث يكون الإجراء الافتراضي في معظم الوقت ضمن DfltAccessPolicy هو إنهاء الاتصال.

إذا كان هذا هو الحال، قم بإنشاء قاعدة DAP منفصلة لهواتف VPN. أستخدم معلمة معينة، مثل ملف تعريف الاتصال، و قم بتعيين الإجراء إلى متابعة:

The screenshot shows the 'Add Dynamic Access Policy' configuration window. The 'Policy Name' field is set to 'VPNPhone'. Below it, the 'Description' field is empty, and the 'ACL Priority' is set to 0. The 'Selection Criteria' section is expanded, showing a dropdown menu set to 'User has ANY of the following AAA Attributes values...'. Below this, there are two empty tables for 'AAA Attribute' and 'Endpoint ID'. The 'Advanced' section is also expanded, showing the 'Access/Authorization Policy Action' section. The 'Action' is set to 'Continue'. The 'Add AAA Attribute' dialog box is open, showing the 'AAA Attribute Type' set to 'Cisco'. The 'Connection Profile' is set to 'VPNPhone', and the 'Action' is set to 'Continue'. The 'Group Policy' is set to 'GroupPolicy\_VPNPhone'. The 'Assigned IPv4 Address', 'Assigned IPv6 Address', 'Username', 'Username2', and 'SCEP Required' fields are also visible.

إذا لم تقم بإنشاء سياسة DAP معينة لهواتف IP، فإن ASA يظهر رسالة تعريف تحت DfltAccessPolicy واتصال

فاشل:

```
ASA-6-716038: Group <DfltGrpPolicy> User <CP-7962G-SEP8CB64F576113> IP%
.Authentication: successful, Session Type: WebVPN <172.16.250.9>
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
```

بمجرد إنشاء سياسة DAP معينة لهواتف IP مع تعيين الإجراء على متابعة، يمكنك الاتصال:

```
- 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%
Address <10.10.10.10> assigned to session <172.16.250.9>
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
```

## القيم الموروثة من DfltGrpPolicy أو مجموعات أخرى

في العديد من الحالات، يتم إعداد DfltGrpPolicy بعدة خيارات. وبشكل افتراضي، يتم توريث هذه الإعدادات لجلسة عمل هاتف IP ما لم يتم تحديدها يدويا في نهج المجموعة الذي يجب أن يستخدمه هاتف IP.

بعض المعلمات التي قد تؤثر على الاتصال إذا كانت موروثة من DfltGrpPolicy هي:

- قفل جماعي
- بروتوكول VPN-tunnel
- عمليات تسجيل الدخول المتزامنة الخاصة بالشبكة الخاصة الظاهرية (VPN)
- عامل تصفية VPN

بافتراض أن لديك مثال التكوين هذا في DfltGrpPolicy و GroupPolicy\_VPNPone:

```
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
```

يرث الاتصال المعلومات من DfltGrpPolicy التي لم يتم تحديدها بشكل صريح ضمن GroupPolicy\_VPNPhone وبدفع جميع المعلومات إلى هاتف IP أثناء الاتصال.

لتجنب هذا، قم بتعيين القيمة (القيم) التي تحتاج إليها مباشرة في المجموعة يدويا:

```
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
```

للتحقق من القيم الافتراضية ل DfltGrpPolicy، أستخدم الأمر `show run all group-policy`؛ يوضح هذا المثال الفرق بين المخرجات:

```
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

```

فيما يلي إخراج سمات وراثية نهج المجموعة من خلال ASDM:

Name: DNIGrpPolicy

Banner: [Empty]

SCEP forwarding URL: [Empty]

Address Pools: [Empty]

IPv6 Address Pools: [Empty]

More Options

Tunneling Protocols:  Clientless SSL VPN  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:  Unlimited [ ] minutes

Idle Timeout:  None [ 30 ] minutes

On smart card removal:  Disconnect  Keep the connection

Name: VPNPhone

Banner:  Inherit [Empty]

SCEP forwarding URL:  Inherit [Empty]

Address Pools:  Inherit [Empty]

IPv6 Address Pools:  Inherit [Empty]

More Options

Tunneling Protocols:  Inherit  Clientless SSL VPN  SSL VPN Client

Filter:  Inherit [Empty]

NAC Policy:  Inherit [Empty]

Access Hours:  Inherit [Empty]

Simultaneous Logins:  Inherit [Empty]

Restrict access to VLAN:  Inherit [Empty]

Connection Profile (Tunnel Group) Lock:  Inherit [Empty]

Maximum Connect Time:  Inherit  Unlimited [ ] minutes

Idle Timeout:  Inherit  None [ ] minutes

On smart card removal:  Inherit  Disconnect  Keep the connection

## شفرات التشفير المدعومة

يدعم هاتف AnyConnect VPN الذي تم إختباره مع هاتف بروتوكول الإنترنت طراز IP 7962G والبرنامج الثابت، الإصدار 9.1.1، شفرين فقط، وكلاهما معيار التشفير المتقدم (AES256-SHA): AES128-SHA و AES). إذا لم يتم تحديد التشفير الصحيح في ASA، سيتم رفض الاتصال، كما هو موضح في سجل 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
.(cipher(s 2
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

```



لتأكيد ما إذا كان ASA لديه التشفير الصحيح الذي تم تمكينه، أدخل الأمر `show ssl` و `show run all 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

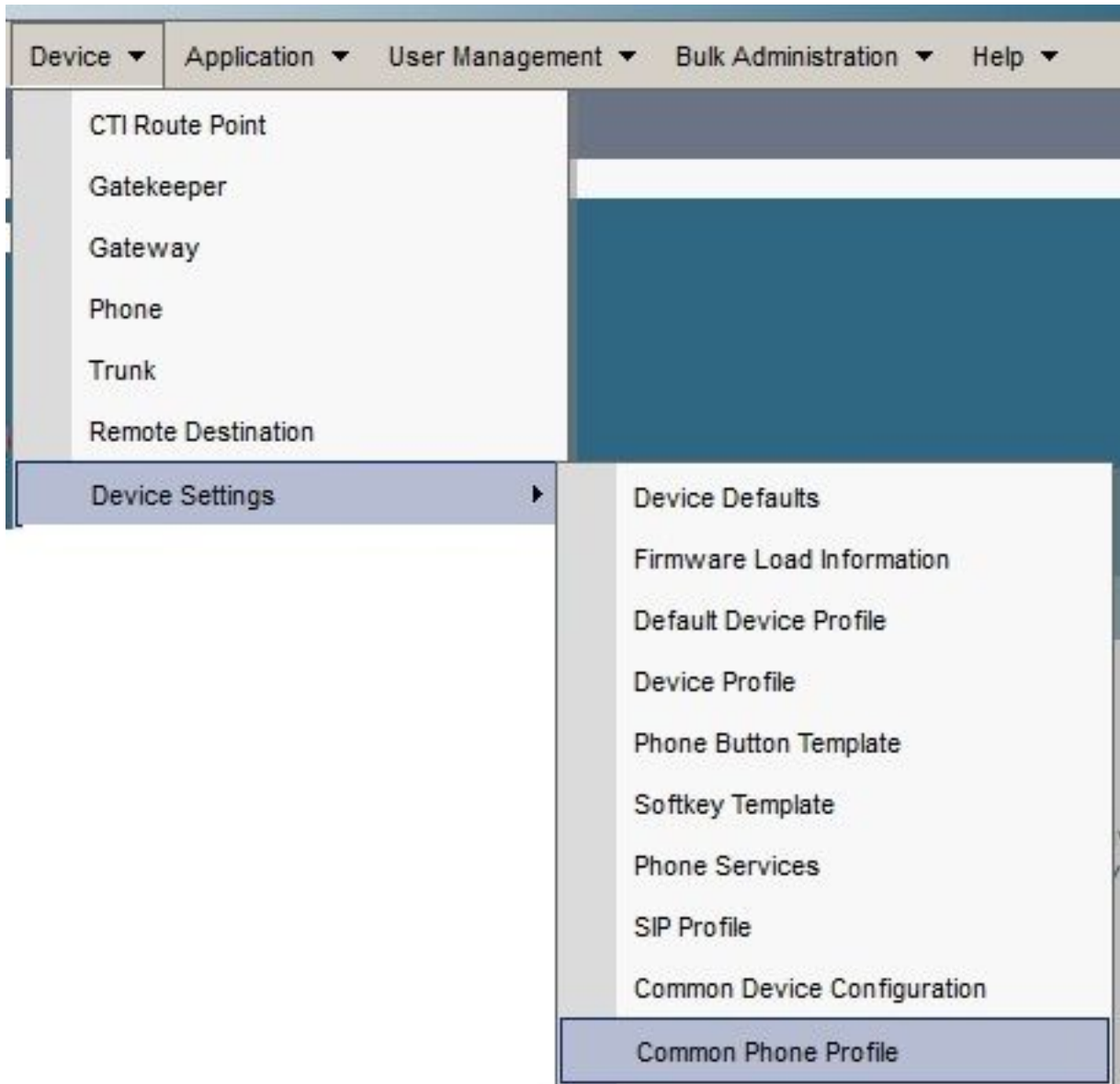
ASA5510-F# show ssl
Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
Enabled cipher order: rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 dhe-aes128-sha1 dhe-aes256-sha1 null-sha1
:SSL trust-points
outside interface: SSL
Certificate authentication is not enabled
#ASA5510-F
```

## القضايا المشتركة في إتفاقية حفظ السلام في القرن الأفريقي

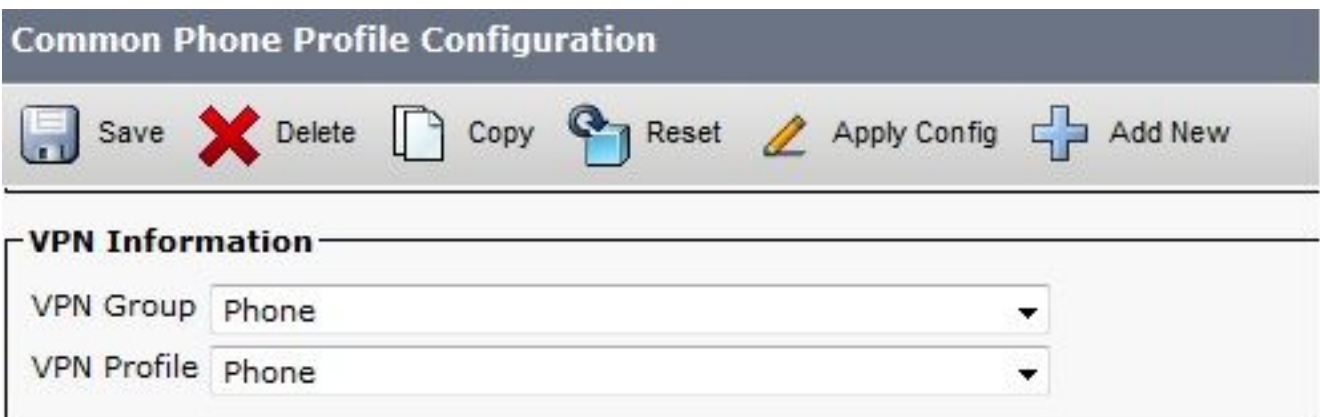
### إعدادات VPN غير مطبقة على هاتف IP

ما إن خلقت التشكيل على ال CUCM (مدخل، مجموعة، وتوصيف)، طبقت ال VPN عملية إعداد في ال مشترك هاتف التوصيف:

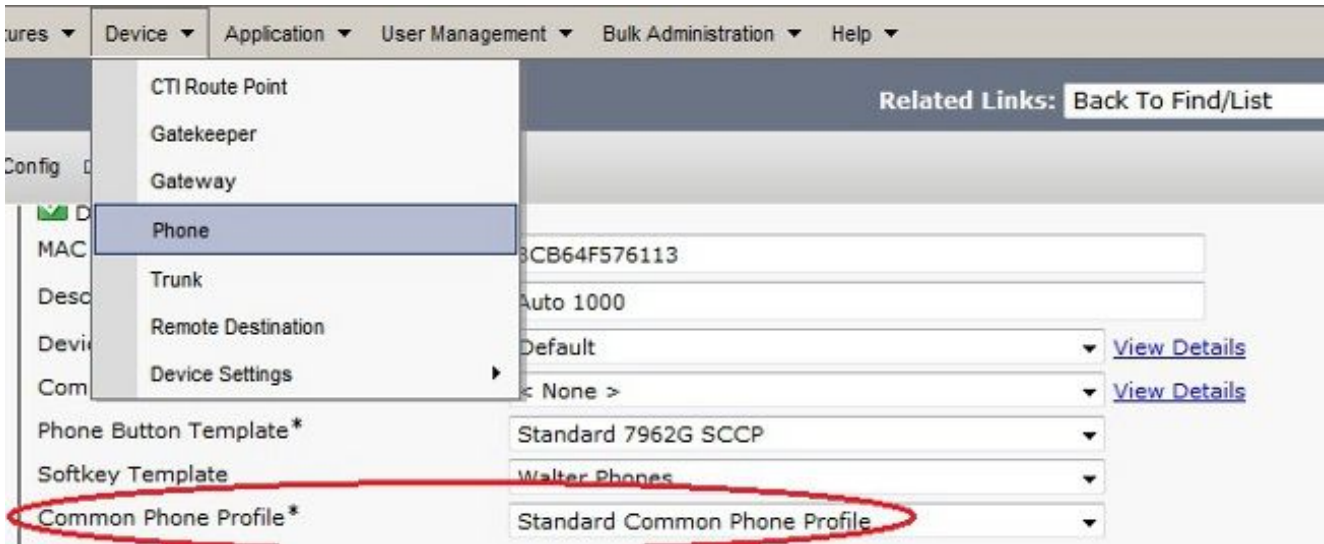
1. انتقل إلى الجهاز < إعدادات الجهاز > ملف تعريف الهاتف الشائع.



2. دخلت ال VPN معلومة:



3. انتقل إلى الجهاز < الهاتف وتأكد من تعيين ملف التعريف هذا لتكوين الهاتف:



## أسلوب مصادقة الشهادة

هناك طريقتان لتكوين مصادقة الشهادة لهواتف IP: الشهادة المثبتة من قبل الشركة المصنعة (MIC) والشهادة ذات الأهمية المحلية (LSC). ارجع إلى [هاتف AnyConnect VPN مع مثال تكوين مصادقة الشهادة](#) لاختيار الخيار الأفضل لوضعك.

عند تكوين مصادقة الشهادة، قم بتصدير الشهادة (الشهادات) (المرجع المصدق الجذر) من خادم CUCM واستيرادها إلى ASA:

1. سجل الدخول إلى CUCM.
2. انتقل إلى إدارة نظام التشغيل الموحدة < الأمان > إدارة الشهادات.
3. ابحث عن وظيفة وكيل المرجع المصدق (CAPF) أو Cisco\_MANUFACTURING\_CA؛ يعتمد نوع الشهادة على ما إذا كنت تستخدم مصادقة شهادة MIC أو LSC.
4. قم بتنزيل الملف إلى الكمبيوتر المحلي.

بمجرد تنزيل الملفات، قم بتسجيل الدخول إلى ASA من خلال CLI (واجهة سطر الأوامر) أو ASDM وقم باستيراد الشهادة كشهادة CA.

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

وبشكل افتراضي، يتم تحميل جميع الهواتف التي تدعم VPN مسبقا بميكروفونات. والهواتف النموذجية 7960 و 7940 لا تأتي بميكروفون وتتطلب إجراء تثبيت خاصا لكي تسجل LSC بشكل آمن.

تتضمن أحدث هواتف (8851، 8841، 8811، Cisco IP)، و (8861) شهادات MIC التي يتم توقيعها بواسطة الجهة المصنعة الجديدة SHA2 CA:

- يتضمن الإصدار 10.5(1) من CUCM الشهادات الجديدة SHA2 ويثق بها.
- إذا قمت بتشغيل إصدار CUCM سابق، فقد يطلب منك تنزيل شهادة CA للتصنيع الجديدة و:  
قم بتحميله إلى ثقة CAPF حتى يمكن أن تتم مصادقة الهواتف باستخدام CAPF للحصول على LSC.  
قم بتحميله إلى ثقة CallManager إذا كنت تريد السماح للهواتف بالمصادقة مع ميكروفون ل SIP 5061.

**تلميح:** انقر فوق [هذا الارتباط](#) للحصول على المرجع المصدق SHA2 إذا كان CUCM يشغل حاليا إصدارا سابقا.

**تحذير:** توصي Cisco باستخدام أجهزة MICs لتثبيت LSC فقط. تدعم Cisco LSCs لمصادقة اتصال TLS مع CUCM. نظرا لإمكانية اختراق شهادات جذر الميكروفون، يقوم العملاء الذين يقومون بتكوين الهواتف لاستخدام ميكروفونات TLS لمصادقة TLS أو لأي غرض آخر بذلك على مسؤوليتهم الخاصة. لا تحمل Cisco أي مسؤولية في حالة اختراق بطاقات MIC.

بشكل افتراضي، إذا كانت هناك LSC في الهاتف، فإن المصادقة تستخدم LSC، بغض النظر عما إذا كان هناك ميكروفون في الهاتف. إذا كان هناك MIC و LSC في الهاتف، فإن المصادقة تستخدم LSC. إذا لم يوجد LSC في

الهاتف، ولكن يوجد MIC، فإن المصادقة تستخدم MIC.

ملاحظة: تذكر أنه بالنسبة لمصادقة الشهادة، يجب تصدير شهادة SSL من ASA واستيرادها إلى CUCM.

## التحقق من معرف المضيف

إذا لم يتطابق الاسم الشائع (CN) في موضوع الشهادة مع (group-url URL) الذي تستخدمه الهواتف للاتصال ب ASA من خلال VPN، فقم بتعطيل التحقق من معرف المضيف على CUCM أو استخدم شهادة في ASA تطابق URL على ASA.

ويكون هذا ضروريا عندما تكون شهادة SSL من ASA شهادة حرف بدل، أو عندما تحتوي شهادة SSL على شبكة SAN مختلفة (اسم موضوع بديل)، أو عندما يكون عنوان URL قد تم إنشاؤه باستخدام عنوان IP بدلا من اسم المجال المؤهل بالكامل (FQDN).

هذا مثال لسجل هاتف IP عندما لا يتطابق CN للشهادة مع URL الذي يحاول الهاتف الوصول إليه.

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

لإيقاف إتاحة التحقق من معرف المضيف في CUCM، انتقل إلى **ميزات متقدمة < VPN < ملف تعريف VPN**:

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

# أستكشاف الأخطاء وإصلاحها بشكل إضافي

## السجلات وتصحيح الأخطاء لاستخدامها في ASA

على ال ASA، أنت يستطيع مكنت هذا يضبط وسجل ل يتحرى:

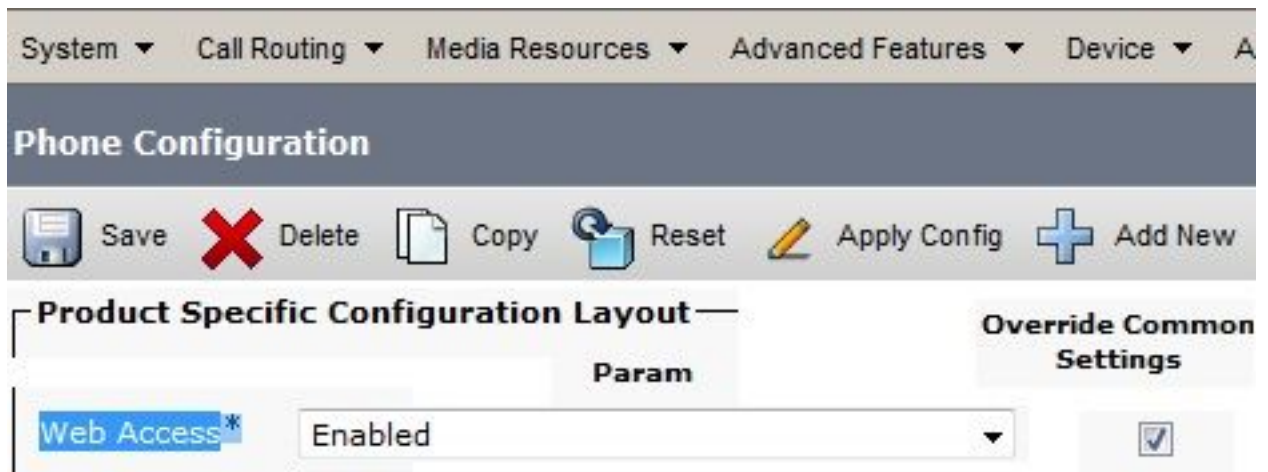
```
logging enable
logging buffer-size 1048576
logging buffered debugging

debug webvpn anyconnect 255
```

ملاحظة: في عملية نشر كبيرة مع حمل مرتفع من مستخدمي AnyConnect، توصي Cisco بعدم تمكين تصحيح أخطاء WebVPNH AnyConnect. لا يمكن تصفية مخرجاته بواسطة عنوان IP، لذلك قد يتم إنشاء كمية كبيرة من المعلومات.

## سجلات هاتف IP

للوصول إلى سجلات الهاتف، قم بتمكين ميزة الوصول إلى الويب. قم بتسجيل الدخول إلى CUCM، وانتقل إلى الجهاز < الهاتف > تكوين الهاتف. ابحث عن هاتف IP الذي تريد تمكين هذه الميزة عليه، وابحث عن المقطع ل Web Access. تطبيق تغييرات التكوين على هاتف IP:



بمجرد تمكين الخدمة وإعادة ضبط الهاتف لإدخال هذه الميزة الجديدة، يمكنك الوصول إلى سجلات هاتف IP في المستعرض، واستخدام عنوان IP الخاص بالهاتف من جهاز كمبيوتر لديه حق الوصول إلى هذه الشبكة الفرعية. انتقل إلى سجلات وحدة التحكم وفحص ملفات السجل الخمسة. لأن الهاتف يستبدل الملفات الخمسة، يجب أن تتحقق من كل هذه الملفات لتجد المعلومات التي تبحث عنها.

10.10.10.10/C 1

CISCO

## Console Logs

Cisco Unified IP Phone CP-7962G ( SEP8CB64F576113 )

- Device Information
- Network Configuration
- Network Statistics
- Ethernet Information
- Access
- Network
- Device Logs
- Console Logs 2

- /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

## المشاكل المرتبطة بين سجلات ASA وسجلات هاتف IP

هذا مثال على كيفية ربط السجلات من ASA وهاتف IP. في هذا المثال، لا تتطابق تجزئة الشهادة الموجودة على ASA مع تجزئة الشهادة الموجودة على ملف تكوين الهاتف لأنه تم إستبدال الشهادة الموجودة على ASA بشهادة مختلفة.

## ASA LOG

```
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%
```

## سجلات الهاتف

```

NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect :902
                                initialization
NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state :903
NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A :904
                                :NOT 10:19:27.364687 VPNC: cert_vfy_cb: depth:1 of 1, subject :905
                                <CN=10.198.16.140/unstructuredName=10.198.16.140/>
(NOT 10:19:27.365344 VPNC: cert_vfy_cb: depth:1 of 1, pre_err: 18 (self signed certificate :906
                                NOT 10:19:27.368304 VPNC: cert_vfy_cb: peer cert saved: /tmp/leaf.crt :907
NOT 10:19:27.375718 SECD: Leaf cert hash = 1289B8A7AA9FFD84865E38939F3466A61B5608FC :908
<ERR 10:19:27.376752 SECD: EROR:secLoadFile: file not found </tmp/issuer.crt :909
                                ERR 10:19:27.377361 SECD: Unable to open file /tmp/issuer.crt :910
ERR 10:19:27.420205 VPNC: VPN cert chain verification failed, issuer certificate not found :911
                                and leaf not trusted
                                :ERR 10:19:27.421467 VPNC: ssl_state_cb: TLSv1: write: alert: fatal :912
                                unknown CA
ERR 10:19:27.422295 VPNC: alert_err: SSL write alert: code 48, unknown CA :913
ERR 10:19:27.423201 VPNC: create_ssl_connection: SSL_connect ret -1 error 1 :914
                                (ERR 10:19:27.423820 VPNC: SSL: SSL_connect: SSL_ERROR_SSL (error 1 :915
ERR 10:19:27.424541 VPNC: SSL: SSL_connect: error:14090086:SSL :916
                                routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
ERR 10:19:27.425156 VPNC: create_ssl_connection: SSL setup failure :917
ERR 10:19:27.426473 VPNC: do_login: create_ssl_connection failed :918
                                NOT 10:19:27.427334 VPNC: vpn_stop: de-activating vpn :919
                                NOT 10:19:27.428156 VPNC: vpn_set_auto: auto -> auto :920
                                NOT 10:19:27.428653 VPNC: vpn_set_active: activated -> de-activated :921
(NOT 10:19:27.429187 VPNC: set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED :922
                                NOT 10:19:27.429716 VPNC: set_login_state: VPNC : 1 (LoggingIn) --> 3 :923
                                (LoginFailed)
[NOT 10:19:27.430297 VPNC: vpnc_send_notify: notify type: 1 [LoginFailed] :924
                                NOT 10:19:27.430812 VPNC: vpnc_send_notify: notify code: 37 :925
                                [SslAlertSrvrCert]
NOT 10:19:27.431331 VPNC: vpnc_send_notify: notify desc: [alert: Unknown :926
                                [(CA (server cert
NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to :927
                                pid 14
ERR 10:19:27.432467 VPNC: protocol_handler: login failed :928

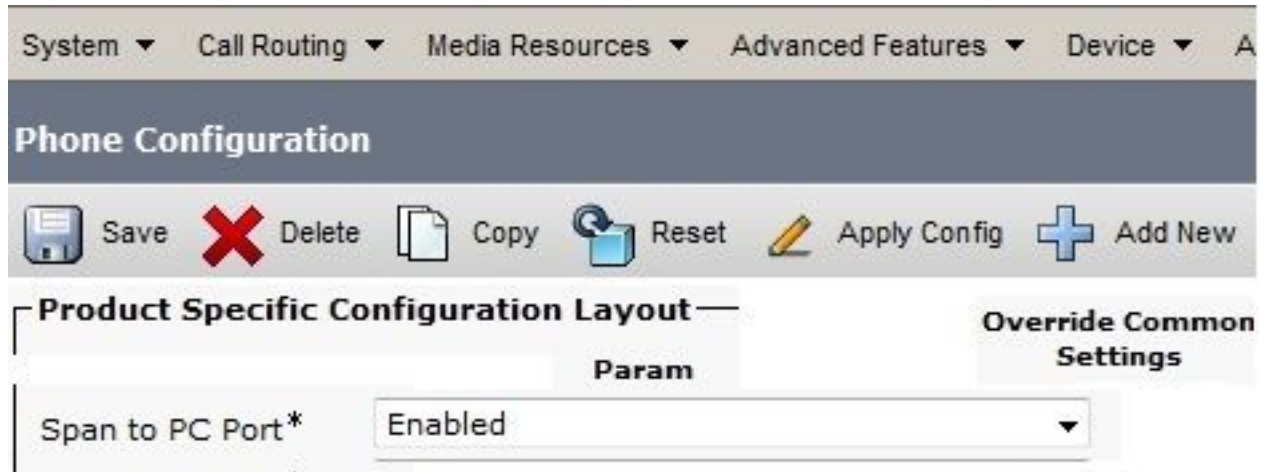
```

## فسحة بين دعامتین إلى PC ميناء سمة

يمكنك توصيل جهاز كمبيوتر بهاتف مباشرة. يحتوي الهاتف على منفذ محول في اللوحة الخلفية.

شكلت الهاتف بما أن أنت عملت سابقا، مكنت الفسحة بين دعامتین إلى PC ميناء على ال CUCM، وطبقت التشكيل. يبدأ الهاتف بإرسال نسخة من كل إطار إلى الكمبيوتر الشخصي. أستخدم Wireshark في الوضع المختلط من أجل التقاط حركة مرور البيانات للتحليل.





## تغييرات تكوين هاتف IP أثناء الاتصال بشبكة VPN

السؤال الشائع هو ما إذا يمكنك تعديل تكوين VPN أثناء توصيل هاتف IP خارج الشبكة بواسطة AnyConnect. الجواب هو نعم، ولكن يجب عليك تأكيد بعض إعدادات التكوين.

قم بإجراء التغييرات اللازمة في CUCM، ثم قم بتطبيق التغييرات على الهاتف. هناك ثلاثة خيارات (تطبيق التكوين، إعادة الضبط، إعادة التشغيل) لدفع التكوين الجديد إلى الهاتف. على الرغم من أن الخيارات الثلاثة تؤدي إلى فصل شبكة VPN من الهاتف و ASA، يمكنك إعادة الاتصال تلقائياً إذا كنت تستخدم مصادقة الشهادة، وإذا كنت تستخدم المصادقة والتحويل والمحاسبة (AAA)، يوعز إليك بإدخال بيانات الاعتماد الخاصة بك مرة أخرى.



**ملاحظة:** عندما يكون هاتف IP في الجانب البعيد، فإنه يستلم عادة عنوان IP من خادم DHCP خارجي. لهاتف IP لاستلام التكوين الجديد من CUCM، يجب أن يتصل بخادم TFTP في المكتب الرئيسي. عادة ما يكون CUCM هو نفس خادم TFTP.

لاستلام ملفات التكوين مع التغييرات، تأكد من إعداد عنوان IP لخادم TFTP بشكل صحيح في إعدادات الشبكة في الهاتف؛ وللتأكد، استخدم الخيار 150 من خادم DHCP أو قم بتعيين TFTP يدويا على الهاتف. يمكن الوصول إلى خادم TFTP هذا من خلال جلسة عمل AnyConnect.

إذا كان هاتف IP يستقبل خادم TFTP من خادم DHCP محلي ولكن هذا العنوان غير صحيح، فيمكنك استخدام خيار خادم TFTP البديل لتجاوز عنوان IP الخاص بخادم TFTP الذي يقدمه خادم DHCP. يوضح هذا الإجراء كيفية تطبيق خادم TFTP البديل:

1. انتقل إلى الإعدادات < تكوين الشبكة < تكوين IPv4.
2. قم بالتمرير إلى خيار TFTP البديل.
3. اضغط على المفتاح التفتي "نعم" للهاتف لاستخدام خادم TFTP بديل؛ وإلا، اضغط على المفتاح "لا برنامج". إذا كان الخيار مؤمنا، اضغط \* \* # لإلغاء تأمينه.
4. اضغط على برنامج حفظ.
5. تطبيق خادم TFTP البديل ضمن الخيار 1 TFTP Server.

راجع رسائل الحالة في مستعرض الويب أو في قوائم الهاتف مباشرة للتأكد من أن الهاتف يتلقى المعلومات الصحيحة. إذا تم إعداد الاتصال بشكل صحيح، ستري رسائل مثل:



The screenshot shows the Cisco Status Messages 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 circle), and Debug Display. The main content area displays a list of status messages for a 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

إذا تعذر على الهاتف إسترداد المعلومات من خادم TFTP، فأنت تتلقى رسائل خطأ 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

### تجديد شهادة ASA SSL

إذا كان لديك إعداد هاتف AnyConnect VPN فعال ولكن شهادة ASA SSL على وشك الانتهاء، فلن تكون بحاجة إلى إحضار جميع هواتف IP إلى الموقع الرئيسي لإدخال شهادات SSL الجديدة إلى الهاتف؛ يمكنك إضافة الشهادات الجديدة أثناء توصيل شبكة VPN.

إذا كنت قد قمت بتصدير أو إستيراد شهادة المرجع المصدق الجذر الخاصة بـ ASA بدلا من شهادة الهوية، وإذا كنت تريد الاستمرار في إستخدام نفس المورد (CA) أثناء هذا التجديد، فليس من الضروري تغيير الشهادة في CUCM لأنها تظل هي نفسها. ولكن، إذا كنت تستخدم شهادة الهوية، فإن هذا الإجراء ضروري؛ وإلا، فإن قيمة التجزئة بين ASA وهاتف IP لا تتطابق، والتوصيل غير موثوق به بواسطة الهاتف.

1. تجديد الشهادة في ASA.

ملاحظة: للحصول على تفاصيل، ارجع إلى [ASA 8.x: تجديد وتثبيت شهادة SSL مع ASDM](#). قم بإنشاء TrustPoint منفصلة ولا تقم بتطبيق هذه الشهادة الجديدة باستخدام الأمر `ssl trustPoint <name>` الموجود خارج النظام حتى تقوم بتطبيق الشهادة على جميع هواتف IP الخاصة بالشبكة الخاصة الظاهرية (VPN). تصدير الشهادة الجديدة.

2.

3. إستيراد الشهادة الجديدة إلى CUCM كشهادة ثقة هاتف VPN.

ملاحظة: كن على علم بأن تحميل [CSCuh19734](#) باستخدام CN نفسه سيقوم باستبدال الشهادة القديمة في Phone-VPN-Trust

4. انتقل إلى تكوين بوابة VPN في CUCM، وطبق الشهادة الجديدة. لديك الآن كلا الشهادتين: الشهادة التي توشك على الانتهاء والشهادة الجديدة التي لم يتم تطبيقها على ASA بعد.

5. تطبيق هذا التكوين الجديد على هاتف IP. انتقل إلى **تطبيق التكوين > إعادة ضبط > إعادة التشغيل** لإدخال تغييرات التكوين الجديدة إلى هاتف IP من خلال نفق VPN. تأكد من أن جميع هواتف IP متصلة من خلال الشبكة الخاصة الظاهرية (VPN) ومن أنها يمكن أن تصل إلى خادم TFTP من خلال النفق.

6. أستخدم TFTP للتحقق من رسائل الحالة وملف التكوين للتأكد من أن هاتف IP استلم ملف التكوين مع التغييرات.

7. تطبيق TrustPoint ل SSL الجديد في ASA، واستبدال الشهادة القديمة.

ملاحظة: إذا كانت شهادة ASA SSL منتهية الصلاحية بالفعل وإذا كانت هواتف IP غير قادرة على الاتصال من خلال AnyConnect، فيمكنك دفع التغييرات (مثل تجزئة شهادة ASA الجديدة) إلى هاتف IP. قم بتعيين TFTP يدويا في هاتف IP إلى عنوان IP عام حتى يمكن لهاتف IP إسترداد المعلومات من هناك. أستخدم خادم TFTP عام لاستضافة ملف التكوين؛ وأحد الأمثلة هو إنشاء إعادة توجيه منفذ على ASA وإعادة توجيه حركة مرور البيانات إلى خادم TFTP الداخلي.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل