

# نيوكت لاثمب AnyConnect VPN فتاه لاصتا Cisco IOS هجوم

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [مخطط الشبكة](#)
- [تكوين خادم SSL VPN](#)
- [خطوات التكوين الشائعة](#)
- [التكوين باستخدام مصادقة AAA](#)
- [التكوين باستخدام شهادة LSC الهامة محليا لهاتف IP لمصادقة العميل](#)
- [تكوين مدير المكالمات](#)
- [تصدير شهادة الهوية أو التوقيع الذاتي من الموجه إلى CUCM](#)
- [تكوين بوابة VPN والمجموعة وتوصيف البيانات في CUCM](#)
- [تطبيق المجموعة والتوصيف على هاتف IP باستخدام ملف تعريف الهاتف الشائع](#)
- [تطبيق ملف تعريف الهاتف الشائع على هاتف IP](#)
- [تثبيت الشهادات المهمة محليا \(LSC\) على هواتف بروتوكول الإنترنت \(IP\) من Cisco](#)
- [تسجيل الهاتف للاتصال بمدير مرة أخرى لتنزيل التكوين الجديد](#)
- [التحقق من الصحة](#)
- [التحقق من الموجه](#)
- [التحقق من CUCM](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [تصحيح الأخطاء على خادم SSL VPN](#)
- [تصحيح الأخطاء من الهاتف](#)
- [الأخطاء ذات الصلة](#)

## المقدمة

يصف هذا المستند كيفية تكوين أجهزة موجه Cisco IOS® و Call Manager حتى يمكن لهواتف Cisco IP إنشاء اتصالات VPN بموجه Cisco IOS. يلزم وجود اتصالات VPN هذه لتأمين الاتصال بأي من طريقتي مصادقة العميل هاتين:

- خادم المصادقة والتفويض والمحاسبة (AAA) أو قاعدة البيانات المحلية
- شهادة الهاتف

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- Cisco IOS 15.1(2)T أو إصدار أحدث
- مجموعة الميزات/الترخيص: شامل (البيانات والأمان والاتصالات الموحدة) لموجه الخدمة المدمجة (ISR)-G2 من Cisco IOS
- مجموعة الميزات/الترخيص: الأمان المتقدم ل Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM)، الإصدار 4-8.0.1.10000 أو إصدار أحدث
- هاتف IP الإصدار SR1S(2)9.0 - بروتوكول Skinny للتحكم في المكالمات (SCCP) أو الإصدارات الأحدث للحصول على قائمة كاملة من الهواتف المدعومة في إصدار CUCM، أكمل الخطوات التالية:

1. افتح عنوان الربط هذا: <https://<CUCM Server IP address>:8443/cucreports/systemReports.do>
2. أختَر قائمة ميزات هاتف Unified CM < إنشاء تقرير جديد > ميزة: الشبكة الخاصة الظاهرية. تتضمن الإصدارات المستخدمة في مثال التكوين هذا:

- موجه IOS الإصدار M4(4)15.1 من Cisco
- مدير المكالمات الإصدار 26-8.5.1.1000
- هاتف IP الإصدار SR1S(1)9.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

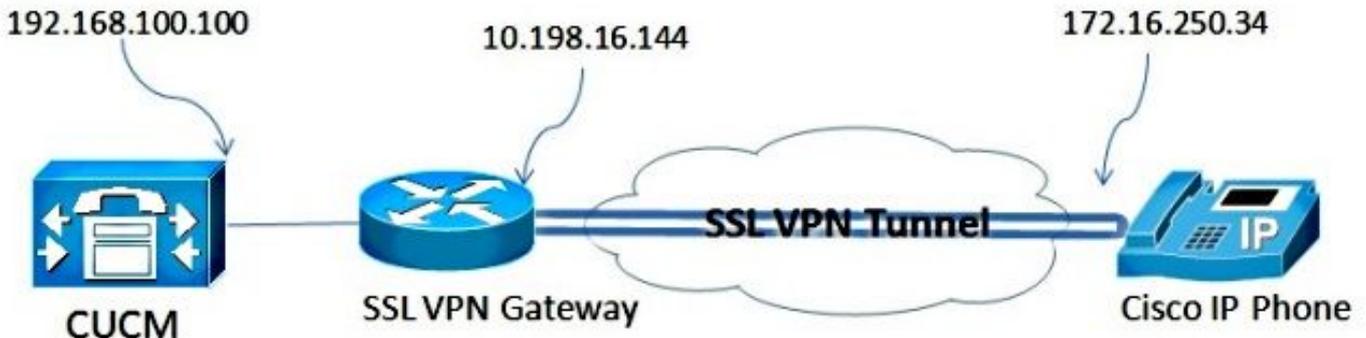
## التكوين

يغطي هذا القسم المعلومات اللازمة لتكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

## مخطط الشبكة

تتضمن الطبولوجيا المستخدمة في هذا المستند هاتف Cisco IP واحدا، وموجه Cisco IOS كبوابة VPN لطبقة مأخذ التوصيل الآمنة (SSL)، و CUCM كبوابة الصوت.



## تكوين خادم SSL VPN

يصف هذا القسم كيفية تكوين واجهة برمجة تطبيقات Cisco IOS للسماح باتصالات SSL VPN الواردة.

### خطوات التكوين الشائعة

1. قم بإنشاء مفتاح (RSA) (Rivest-Shamir-Adleman) بطول 1024 بايت:

```
Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
```

2. قم بإنشاء نقطة الثقة للشهادة الموقعة ذاتيا، وأرفق مفتاح SSL RSA:

```
Router(config)#crypto pki trustpoint server-certificate
enrollment selfsigned
usage ssl-server
serial-number
subject-name CN=10.198.16.144
revocation-check none
rsa keypair SSL
```

3. ما إن شكلت ال trustPoint يكون، سجل الشهادة ذاتية التوقيع مع هذا أمر:

```
Router(config)#crypto pki enroll server-certificate
Include an IP address in the subject name? [no]: no %
Generate Self Signed Router Certificate? [yes/no]: yes
```

```
Router Self Signed Certificate successfully created
```

4. قم بتمكين حزمة AnyConnect الصحيحة على الطرف الرئيسي. الهاتف نفسه لا يقوم بتنزيل هذه الحزمة. ولكن في غياب الحزمة، لا يؤسس نفق الشبكة الخاصة الظاهرية (VPN). يوصى باستخدام أحدث إصدار من برنامج العميل المتوفر على Cisco.com. يستخدم هذا المثال الإصدار 3.1.3103.

في إصدارات Cisco IOS القديمة، هذا هو الأمر لتمكين الحزمة:

```
Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

ومع ذلك، في أحدث إصدار من Cisco IOS، هذا هو الأمر:

```
-Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win
3.1.03103-k9.pkg sequence 1
```

5. قم بتكوين بوابة VPN. يتم استخدام عبارة WebVPN لإنهاء اتصال SSL من المستخدم.

```
webvpn gateway SSL
ip address 10.198.16.144 port 443
ssl encryption 3des-sha1 aes-sha1
http-redirect port 80
ssl trustpoint server-certificate
inservice
```

ملاحظة: إما أن يكون عنوان IP المستخدم هنا موجودا على الشبكة الفرعية نفسها الخاصة بالواجهة التي تتصل بها الهواتف، أو أن البوابة بحاجة إلى أن يتم الحصول عليها مباشرة من واجهة على الموجه. كما يتم استخدام البوابة لتحديد الشهادة التي يتم استخدامها من قبل الموجه للتحقق من صحة نفسها للعميل. 6. قم بتحديد التجمع المحلي الذي يتم استخدامه لتعيين عناوين IP إلى العملاء عند إتصالهم:

```
ip local pool ap_phonevpn 192.168.100.1 192.168.100.254
```

## التكوين باستخدام مصادقة AAA

يصف هذا القسم الأوامر التي تحتاجها لتكوين خادم AAA أو قاعدة البيانات المحلية لمصادقة هواتفك. إذا كنت تخطط لاستخدام مصادقة الشهادة فقط للهواتف، تابع إلى القسم التالي.

### تكوين قاعدة بيانات المستخدم

يمكن استخدام قاعدة البيانات المحلية للموجه أو خادم AAA خارجي للمصادقة:

• دخلت in order to شكلت المعطيات محلي،:

```
aaa new-model
aaa authentication login SSL local
username phones password 0 phones
```

• دخلت in order to شكلت بعيد AAA RADIUS نادل للمصادقة،:

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

### تكوين السياق الظاهري ونهج المجموعة

يتم استخدام السياق الظاهري لتحديد السمات التي تحكم اتصال VPN، مثل:

- عنوان URL الذي سيتم استخدامه عند الاتصال
- التجمع الذي سيتم استخدامه لتعيين عناوين العميل
- أسلوب المصادقة الذي سيتم استخدامه

هذه الأوامر هي مثال على سياق يستخدم مصادقة AAA للعميل:

```
webvpn context SSL
aaa authenticate list SSL
gateway SSL domain SSLPhones
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonevpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

### التكوين باستخدام شهادة LSC الهامة محليا لهاتف IP لمصادقة العميل

يصف هذا القسم الأوامر التي تحتاجها لتكوين مصادقة العميل المستندة إلى شهادة للهواتف. ومع ذلك، فمن أجل القيام بذلك، يلزم معرفة الأنواع المختلفة لشهادات الهاتف:

- الشهادة المثبتة من الشركة المصنعة (MIC) - يتم تضمين أجهزة MIC في جميع هواتف Cisco IP طراز 7941 و 7961. إن MICs هي 2,048-بت شهادة مفتاح أن يكون وقعت من قبل ال cisco شهادة المرجع المصدق (CA). من أجل أن يثق CUCM بشهادة MIC، فإنه يستخدم شهادات CA المثبتة مسبقا -CAP، CAP-RTP-001،

RTP-002، و Cisco\_MANUFACTURING\_CA في مخزن الشهادات الموثوق به. لا يوصى باستخدام هذه الشهادة لمصادقة العميل، نظرا لأن هذه الشهادة مقدمة من المصنع نفسه، كما هو موضح في الاسم.

- **LSC** - يؤمن ال LSC الاتصال بين CUCM والهاتف بعد أن يشكل أنت الجهاز أمن أسلوب للمصادقة أو تشفير. يحتوي LSC على المفتاح العام لهاتف Cisco IP، والذي تم توقيعه من قبل المفتاح الخاص لوظيفة وكيل شهادة (CAPF) (CUCM). هذه هي الطريقة الأكثر أمانا (مقارنة باستخدام أجهزة MICs).

**تحذير:** نظرا لزيادة مخاطر الأمان، توصي Cisco باستخدام أجهزة MIC فقط لتثبيت LSC وليس للاستخدام المستمر. العملاء الذين يقومون بتكوين هواتف Cisco IP لاستخدام بطاقات MICs لمصادقة أمان طبقة النقل (TLS)، أو لأي غرض آخر، يقومون بذلك على مسؤوليتهم الخاصة.

في مثال التكوين هذا، يتم استخدام LSC لمصادقة الهواتف.

**تلميح:** الطريقة الأكثر أمانا لتوصيل هاتفك هي استخدام المصادقة المزدوجة، والتي تجمع بين الشهادة ومصادقة AAA. يمكنك تكوين هذا إذا قمت بدمج الأوامر المستخدمة لكل واحد ضمن سياق ظاهري واحد.

### تكوين TrustPoint للتحقق من صحة شهادة العميل

يجب أن يحتوي الموجه على شهادة CAPF مثبتة للتحقق من صحة LSC من هاتف IP. للحصول على هذه الشهادة وتثبيتها على الموجه، أكمل الخطوات التالية:

1. انتقل إلى صفحة الويب الخاصة بإدارة نظام تشغيل (OS) (CUCM).
2. اختر التأمين < إدارة الترخيص.
3. ملاحظة: قد يتغير هذا الموقع استنادا إلى إصدار CUCM.
4. ابحث عن الشهادة المسماة CAPF، وقم بتنزيل ملف pem. احفظه على هيئة ملف txt.

بمجرد استخراج الترخيص، قم بإنشاء نقطة ثقة جديدة على الموجه، وصدق نقطة الثقة باستخدام CAPF، كما هو موضح هنا. عندما يطلب منك لشهادة المرجع المصدق بترميز base-64، حدد وصق النص في ملف pem. الذي تم تنزيله مع أسطر BEGIN و END.

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
#(Router(config)
```

quit

**امور يجب ملاحظتها:**

- أسلوب التسجيل هو terminal لأنه يجب تثبيت الشهادة يدويا على الموجه.
- يلزم الأمر **authorization username** لإعلام الموجه بما يجب استخدامه كاسم مستخدم عندما يقوم العميل بإجراء الاتصال. في هذه الحالة، يستعمل الإسم الشائع (CN).
- يجب تعطيل التحقق من الإبطال لأن شهادات الهاتف لا تحتوي على قائمة إبطال الشهادات (CRL) معرفة. لذلك، ما لم يكن معاق، يفشل التوصيل ويؤدي تصحيح أخطاء المفتاح العام (PKI) هذا إنتاج:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
.query CRL
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilities request 0
```

```
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

## تكوين السياق الظاهري ونهج المجموعة

هذا جزء من التكوين مماثل للتكوين المستخدم سابقا، باستثناء نقطتين:

- أسلوب المصادقة
  - يستخدم السياق TrustPoint للمصادقة على الهواتف
- يتم عرض الأوامر هنا:

```
webvpn context SSL
gateway SSL domain SSLPhones
authentication certificate
ca trustpoint CAPF
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonevpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

## تكوين مدير المكالمات

يصف هذا القسم خطوات تكوين مدير الاتصال.

## تصدير شهادة الهوية أو التوقيع الذاتي من الموجه إلى CUCM

لتصدير الشهادة من الموجه واستيراد الشهادة إلى "إدارة المكالمات" كشهادة Phone-VPN-Trust، أكمل الخطوات التالية:

1. تحقق من الشهادة المستخدمة ل SSL.

```
Router#show webvpn gateway SSL
SSL Trustpoint: server-certificate
```

2. تصدير الشهادة.

```
Router(config)#crypto pki export server-certificate pem terminal
:The Privacy Enhanced Mail (PEM) encoded identity certificate follows
-----BEGIN CERTIFICATE-----
<output removed>
-----END CERTIFICATE-----
```

3. انسخ النص من الوحدة الطرفية واحفظه على هيئة ملف pem.
4. قم بتسجيل الدخول للاتصال بمدير، واختر إدارة نظام التشغيل الموحد < الأمان > إدارة الشهادات < تحميل الشهادة > تحديد ثقة الهاتف VPN لتحميل ملف الشهادة المحفوظ في الخطوة السابقة.

تكوين بوابة VPN والمجموعة وتوصيف البيانات في CUCM

1. انتقل إلى إدارة CM الموحدة من Cisco.
2. من شريط القوائم، اختر ميزات متقدمة < VPN > بوابة الشبكة الخاصة الظاهرية (VPN).

3. في نافذة تكوين عبارة VPN، أكمل الخطوات التالية:

في حقل اسم عبارة VPN، أدخل اسما. يمكن أن يكون هذا أي اسم. في حقل وصف عبارة VPN، أدخل وصفا (إختياري). في حقل URL لعبارة VPN، أدخل عنوان URL الخاص بالمجموعة المعرف على الوجه. في شهادات الشبكة الخاصة الظاهرية (VPN) في حقل الموقع هذا، اختر الشهادة التي تم تحميلها إلى "إدارة المكالمات" مسبقا لنقلها من مخزن الثقة إلى هذا الموقع.

**VPN Gateway Information**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

---

**VPN Gateway Certificates**

VPN Certificates in your Truststore

SUBJECT: CN=10.198.16.136,unstructuredName=10.198.16.136 ISSUER: CN=10.198.16.136,unstructuredName=...  
SUBJECT: unstructuredName=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com ISSUER: DC=com,DC=crtac,DC=...  
SUBJECT: C=CR,O=Cisco,OU=VPN,CN=ASA5520-C.cisco.com,unstructuredName=ASA5520-C.cisco.com ISSUER: ...  
SUBJECT: CN=10.198.16.140:8443 ISSUER: CN=10.198.16.140:8443 S/N: e7:e2:72:4f  
SUBJECT: CN=ASA5510-F-IP-PHONE,unstructuredName=ASA5510-F.cisco.com ISSUER: CN=ASA5510-F-IP-PHON...

VPN Certificates in this Location\*

SUBJECT: CN=10.198.16.144,SERIALNUMBER=FTX1309A406+unstructuredName=R2811.vpn.cisco-tac.com ISSU...

4. من شريط القوائم، اختر ميزات متقدمة < VPN > مجموعة VPN.

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Admin

### VPN Gateway Configuration

Save Delete Copy Add

**Status**  
 Status: Ready

**VPN Gateway Information**

VPN Gateway Name\* IOS\_SSL\_Phones  
 VPN Gateway Description  
 VPN Gateway URL\* https://10.198.16.144/SSLPhones

Advanced Features Menu:  
 Voice Mail  
 SAF  
 EMCC  
 Intercompany Media Services  
 Fallback  
 VPN

VPN Sub-menu:  
 VPN Profile  
 VPN Group  
 VPN Gateway  
 VPN Feature Configuration

5. في حقل جميع بوابات الشبكات الخاصة الظاهرية (VPN) المتاحة، أختار عبارة الشبكة الخاصة الظاهرية (VPN) التي تم تعريفها مسبقا. انقر فوق السهم لأسفل لنقل البوابة المحددة إلى بوابات الشبكة الخاصة الظاهرية (VPN) المحددة في حقل مجموعة الشبكات الخاصة الظاهرية (VPN) هذا.

### VPN Group Configuration

Save Delete Copy Add New

**Status**  
 Status: Ready

**VPN Group Information**

VPN Group Name\* IOS\_SSL\_Phones  
 VPN Group Description

**VPN Gateway Information**

All Available VPN Gateways

Selected VPN Gateways in this VPN Group\* IOS\_SSL\_Phones

Save Delete Copy Add New

6. من شريط القوائم، أختار ميزات متقدمة < VPN > ملف تخصيص VPN.

System ▾ Call Routing ▾ Media Resources ▾ **Advanced Features ▾** Device ▾ Application ▾ User Management ▾ Bulk Admin

**VPN Group Configuration**

Save  Delete  Copy  Add

**Status**

 Status: Ready

**VPN Group Information**

VPN Group Name\*

VPN Group Description

Voice Mail ▸  
SAF ▸  
EMCC ▸  
Intercompany Media Services ▸  
Fallback ▸  
**VPN ▸**  
VPN Profile  
VPN Group  
VPN Gateway  
VPN Feature Configuration

7. أتمت in order to شكلت ملف تعريف VPN، كل الحقول أن يكون علمت بنجمة (\*).

**VPN Profile Configuration**

Save  Delete  Copy  Add New

**Status**

 Status: Ready

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check

**Client Authentication**

Client Authentication Method\*

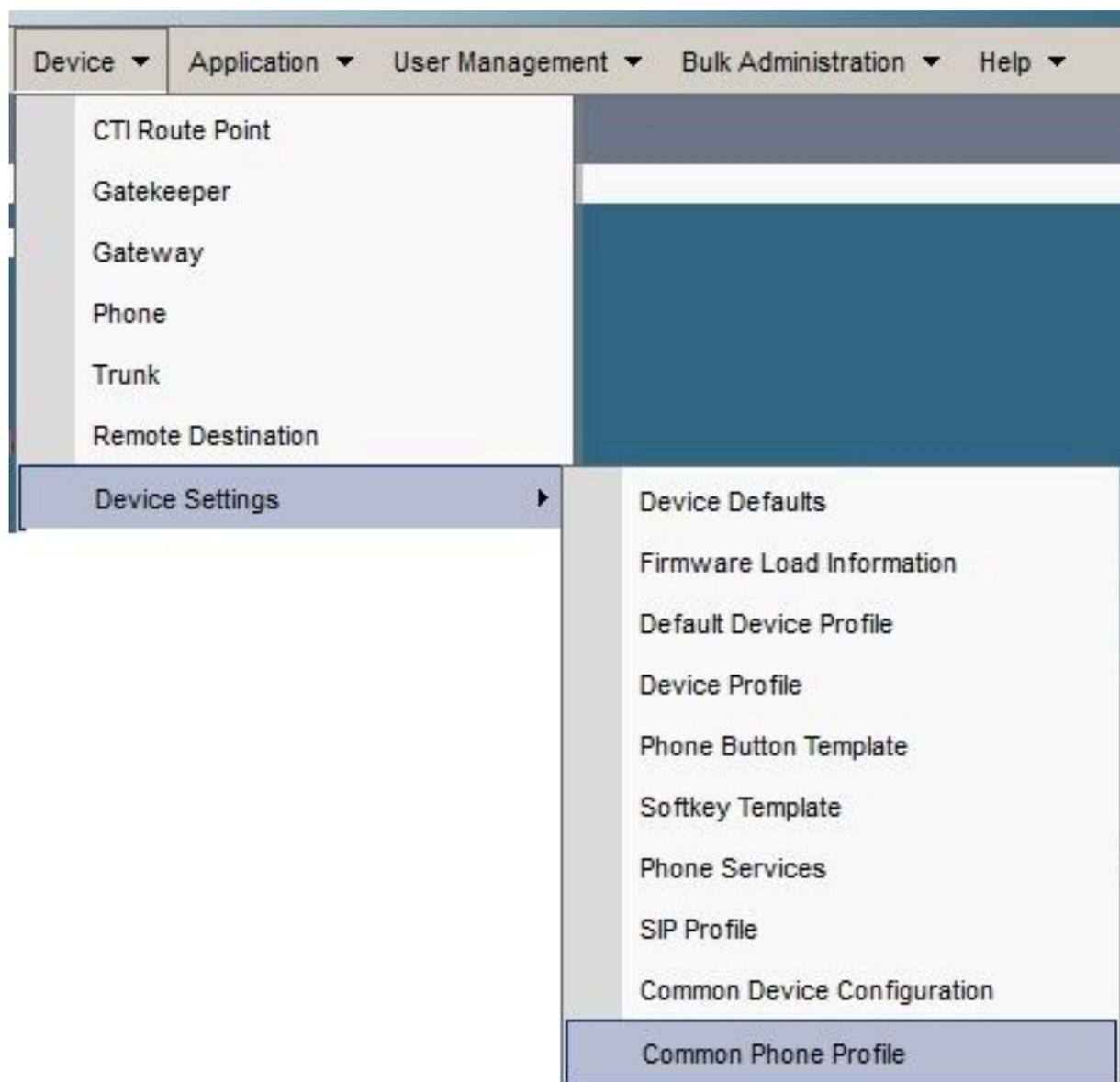
Enable Password Persistence

Save Delete Copy Add New

تمكين الكشف التلقائي عن الشبكة: إذا تم تمكين ذلك، تجبر هواتف VPN خادم TFTP. في حالة عدم تلقي أية استجابة، يقوم تلقائياً ببدء اتصال VPN. تمكين التحقق من معرف المضيف: إذا تم تمكين هذا الخيار، يقوم هاتف شبكة VPN بمقارنة اسم المجال المؤهل بالكامل (FQDN) لعنوان URL لبوابة شبكة VPN مقابل شبكة منطقة التخزين (SAN) الخاصة بالشهادة. يفشل العميل في الاتصال إذا لم تتطابق هذه العناصر أو إذا تم استخدام شهادة حرف بدل مع علامة نجمية (\*). قم بتمكين إستمرارية كلمة المرور: يسمح هذا لهاتف VPN بذاكرة التخزين المؤقت لاسم المستخدم وكلمة المرور للمحاولة التالية لشبكة VPN.

## تطبيق المجموعة والتوصيف على هاتف IP باستخدام ملف تعريف الهاتف الشائع

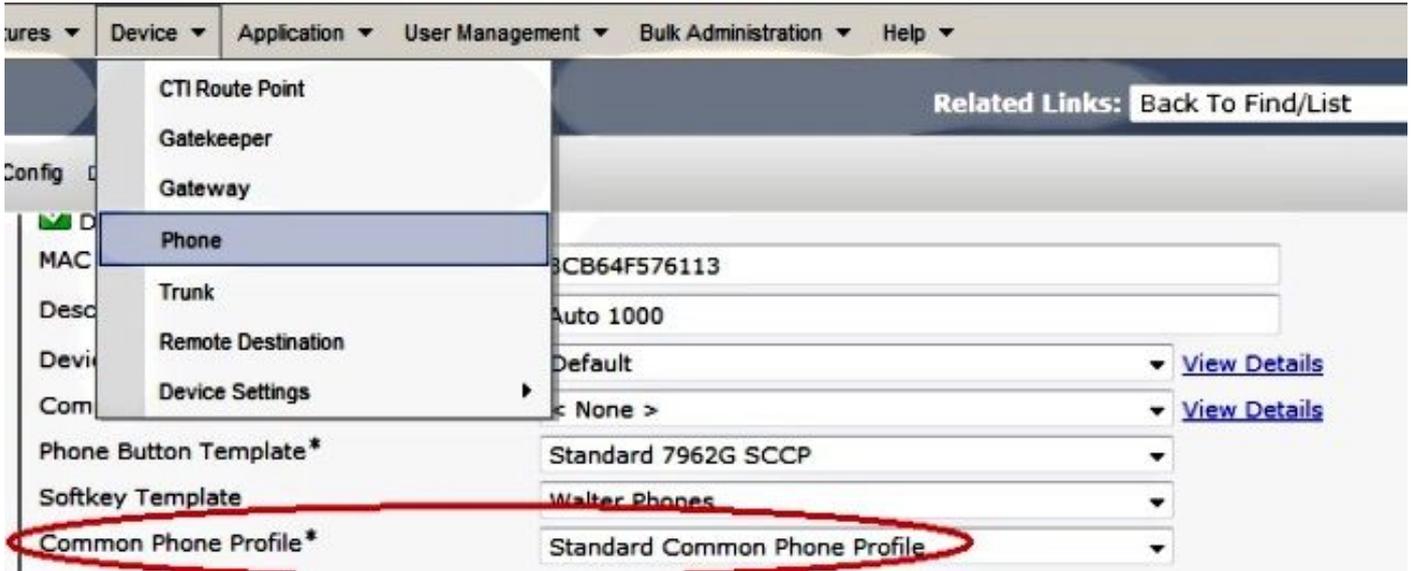
في نافذة تكوين ملف تعريف الهاتف الشائع، انقر فوق **تطبيق التكوين** لتطبيق تكوين VPN الجديد. يمكنك استخدام **توصيف الهاتف العام القياسي** أو إنشاء توصيف جديد.



## تطبيق ملف تعريف الهاتف الشائع على هاتف IP

إذا قمت بإنشاء ملف تعريف جديد لهواتف/مستخدمين معينين، فانتقل إلى نافذة **تكوين الهاتف**. في حقل ملف تعريف

الهاتف الشائع، أختار ملف تعريف الهاتف الشائع القياسي.



تثبيت الشهادات المهمة محليا (LSC) على هواتف بروتوكول الإنترنت (IP) من Cisco

يمكن استخدام الدليل التالي لتثبيت الشهادات المهمة محليا على هواتف Cisco IP. تكون هذه الخطوة مطلوبة فقط في حالة استخدام المصادقة باستخدام LSC. لا تتطلب المصادقة التي تستخدم الشهادة المثبتة (MIC) الخاصة بالمصمم أو اسم المستخدم وكلمة المرور تثبيت LSC.

[قم بتثبيت LSC على هاتف مع تعيين وضع أمان نظام مجموعة CUCM على غير آمن.](#)

تسجيل الهاتف للاتصال بمدير مرة أخرى لتنزيل التكوين الجديد

هذه هي الخطوة الأخيرة في عملية التكوين.

## التحقق من الصحة

### التحقق من الموجه

in order to فحصت الاحصائيات من ال VPN جلسة في المسحاج تخديد، أنت يستطيع استعملت هذا أمر، وفحصت الفروق بين المخرج (مبرز) ل username ومصادقة الشهادة:

لمصادقة اسم المستخدم/كلمة المرور:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
(Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0

Username : phones                               Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
: Rekey Time : 3600 Rekey Method
```

```

Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
: Msie-Exception
Client Ports : 51534
DTLS Port : 52768
#Router

```

Router#show webvpn session context all

```

WebVPN context name: SSL
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
phones 172.16.250.34 1 00:30:38 00:00:20

```

لمصادقة الشهادة:

Router#show webvpn session user SEP8CB64F578B2C context all

```

Session Type : Full Tunnel
(Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0

```

```

Username : SEP8CB64F578B2C Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint : CAPF
: Context : SSL Policy Group
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
: Rekey Time : 3600 Rekey Method
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
: Msie-Exception
Client Ports : 50122
DTLS Port : 52932

```

Router#show webvpn session context all

```

WebVPN context name: SSL
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
SEP8CB64F578B2C 172.16.250.34 1 3d04h 00:00:16

```

التحقق من CUCM

تأكد من تسجيل هاتف IP مع "إدارة المكالمات" بالعنوان المعين الذي يقدمه الموجه إلى اتصال SSL.

Phone (1 - 4 of 4)							
Find Phone where		Device Name	begins with	Find	Clear Filter		
Select item or enter search text							
<input type="checkbox"/>		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
<input type="checkbox"/>		SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F576113	Auto 1000	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

استكشاف الأخطاء وإصلاحها

## تصحيح الأخطاء على خادم SSL VPN

```
Router#show debug
```

```
:WebVPN Subsystem
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on
```

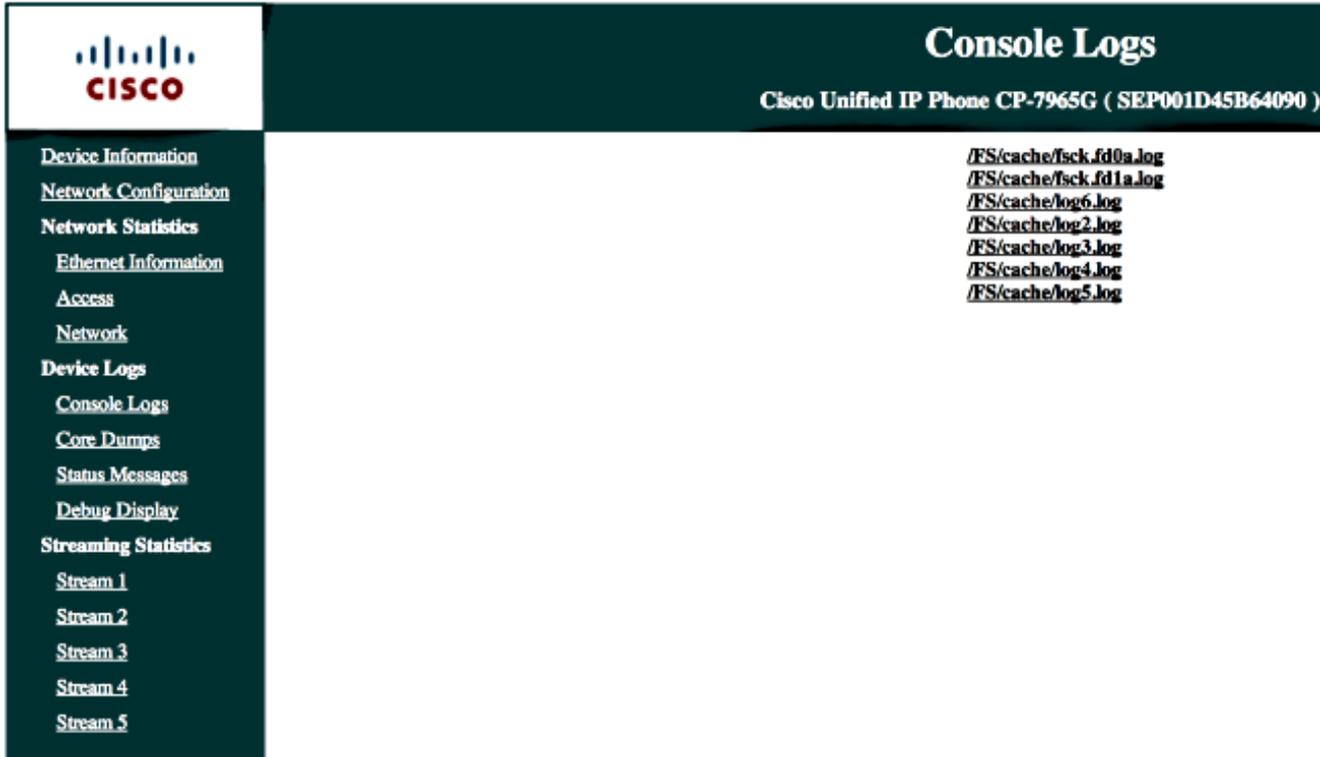
```
:PKI
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

### تصحيح الأخطاء من الهاتف

1. انتقل إلى الجهاز < الهاتف من CUCM.
2. في صفحة تكوين الجهاز، قم بتعيين Web Access إلى Enabled.
3. انقر فوق حفظ، ثم انقر فوق تطبيق التكوين.

Web Access\* Enabled

4. من متصفح، أدخل عنوان IP الخاص بالهاتف، واختر سجلات وحدة التحكم من القائمة الموجودة على اليسار.



The screenshot shows the Cisco Unified IP Phone Web Access interface. The top bar is dark green with the Cisco logo on the left and the text 'Console Logs' and 'Cisco Unified IP Phone CP-7965G ( SEP001D45B64090 )' on the right. Below the bar is a navigation menu on the left with the following items: Device Information, Network Configuration, Network Statistics, Ethernet Information, Access, Network, Device Logs, Console Logs, Core Dumps, Status Messages, Debug Display, Streaming Statistics, Stream 1, Stream 2, Stream 3, Stream 4, and Stream 5. The main content area on the right displays a list of log files: /FS/cache/fsck.fd0a.log, /FS/cache/fsck.fd1a.log, /FS/cache/log6.log, /FS/cache/log2.log, /FS/cache/log3.log, /FS/cache/log4.log, and /FS/cache/log5.log.

5. قم بتنزيل كافة ملفات /FS/cache/log\*.log. تحتوي ملفات سجل وحدة التحكم على معلومات حول سبب فشل الهاتف في الاتصال بشبكة VPN.

### الأخطاء ذات الصلة

معرف تصحيح الأخطاء من IOS SSLVPN، Cisco [CSCty46387](https://www.cisco.com/cisco/web/errata/CSCty46387): التحسين لإنشاء سياق يكون افتراضيا

معرفة تصحيح الأخطاء من IOS SSLVPN، Cisco [CSCty46436](#): تحسين سلوك التحقق من صحة شهادة العميل

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل