

# ةق داصم عم AnyConnect VPN فتاه نيوكت ASA ىلع ةداهشلا

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [أنواع شهادات الهاتف](#)
- [التكوين](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند نموذجاً لتكوين جهاز الأمان القابل للتكيف (ASA) وأجهزة CallManager لتوفير مصادقة الشهادة لعملاء AnyConnect الذين يعملون على هواتف بروتوكول الإنترنت (IP) من Cisco. بعد اكتمال هذا التكوين، يمكن لهواتف Cisco IP إنشاء إتصالات VPN إلى ASA التي تستخدم الشهادات لتأمين الاتصال.

## المتطلبات الأساسية

### المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- ترخيص AnyConnect Premium SSL
- ترخيص هاتف AnyConnect لـ Cisco VPN
- استناداً إلى إصدار ASA، ستري إما "AnyConnect for Linksys Phone" لـ ASA الإصدار x.8.0 أو "AnyConnect" لهاتف "Cisco VPN" لـ ASA الإصدار x.8.2 أو إصدار أحدث.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA - الإصدار 8.0(4) أو إصدار أحدث

- طرز هاتف بروتوكول الإنترنت 7975 / 7965 / 7945 / 7962 / 7942 - IP
  - الهواتف - الإصدار 9971/9951/8961 مع الإصدار 9.1(1) من البرامج الثابتة
  - الهاتف - الإصدار SR1S(2)9.0 - بروتوكول Skinny للتحكم في المكالمات (SCCP) أو الإصدارات الأحدث
  - CUCM (Cisco Unified Communications Manager) - الإصدار 4-8.0.1.10000 أو إصدار أحدث
- تتضمن الإصدارات المستخدمة في مثال التكوين هذا:

- ASA - الإصدار 9.1(1)
  - CallManager - الإصدار 26-8.5.1.1000
- للحصول على قائمة كاملة من الهواتف المدعومة في إصدار CUCM، أكمل الخطوات التالية:

1. افتح عنوان URL هذا: <https://<CUCM Server IP address>:8443/cucreports/systemReports.do>
  2. أختَر قائمة ميزات هاتف Unified CM < إنشاء تقرير جديد > ميزة: الشبكة الخاصة الظاهرية.
- 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.

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## أنواع شهادات الهاتف

تستخدم Cisco أنواع الشهادات التالية في الهواتف:

- الشهادة المثبتة (MIC) من قبل الشركة المصنعة - يتم تضمين أجهزة MIC في جميع هواتف Cisco IP طراز 7941 و 7961 والطراز الأحدث. إن MICs هي شهادات مفاتيح 2048-بت التي يتم توقيعها من قبل مرجع شهادة Cisco (CA). عند وجود ميكروفون، ليس من الضروري تثبيت شهادة هام محليا (LSC). من أجل أن يثق CUCM في شهادة MIC، فإنه يستخدم شهادات CA المثبتة مسبقا CAP-RTP-001، CAP-RTP-002، و Cisco\_MANUFACTURING\_CA في مخزن الشهادات الموثوق به.
- 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 توقيعها من قبل المفتاح الخاص لوظيفة وكيل شهادة (CAPF) CUCM. هذه هي الطريقة المفضلة (مقارنة باستخدام أجهزة MIC) لأنه يسمح فقط لهواتف IP من Cisco التي يتم توفيرها يدويا بواسطة المسؤول بتنزيل ملف CTL والتحقق منه. **ملاحظة:** نظرا لتزايد مخاطر الأمان، توصي Cisco باستخدام أجهزة MIC فقط لتثبيت LSC وليس للاستخدام المستمر. يقوم العملاء الذين يقومون بتكوين هواتف بروتوكول الإنترنت (IP) من Cisco باستخدام بطاقات MIC لمصادقة أمان طبقة النقل (TLS) أو لأي غرض آخر بذلك على مسؤوليتهم الخاصة.

## التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

## التكوينات

يصف هذا المستند التكوينات التالية:

- تكوين ASA
  - تكوين CallManager
  - تكوين VPN على CallManager
  - تثبيت الشهادة على هواتف بروتوكول الإنترنت (IP)
- تكوين ASA**

يكاد يكون تكوين ASA هو نفسه عند توصيل جهاز كمبيوتر عميل AnyConnect بـ ASA. ومع ذلك، تنطبق هذه القيود:

- يجب أن يكون لمجموعة النفق عنوان URL للمجموعة. سيتم تكوين عنوان URL هذا في CM تحت عنوان URL لعبارة VPN.
  - يجب ألا يحتوي نهج المجموعة على نفق تقسيم.
- يستخدم هذا التكوين شهادة ASA (موقعة ذاتيا أو من جهة خارجية) تم تكوينها وتثبيتها مسبقا في Secure Socket Layer (SSL) TrustPoint لجهاز ASA. لمزيد من المعلومات، ارجع إلى هذه المستندات:

- [تهيئة الشهادات الرقمية](#)
  - [ASA 8.x يركب يدويا شهادات مورد الطرف الثالث للاستخدام مع مثال تكوين WebVPN](#)
  - [ASA 8.x: وصول VPN مع عميل AnyConnect VPN باستخدام مثال تكوين شهادة موقعة ذاتيا](#)
- التكوين ذو الصلة لـ ASA هو:

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

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

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

ssl trust-point SSL outside
```

### تكوين CallManager

لتصدير الشهادة من ASA واستيراد الشهادة إلى CallManager كشهادة Phone-VPN-Trust، أكمل الخطوات التالية:

1. تسجيل الشهادة التي تم إنشاؤها باستخدام CUCM.

2. تحقق من الشهادة المستخدمة لـ SSL.

```
ASA(config)#show run ssl
ssl trust-point SSL outside
```

3. تصدير الشهادة.

```
ASA(config)#crypto ca export SSL identity-certificate
```

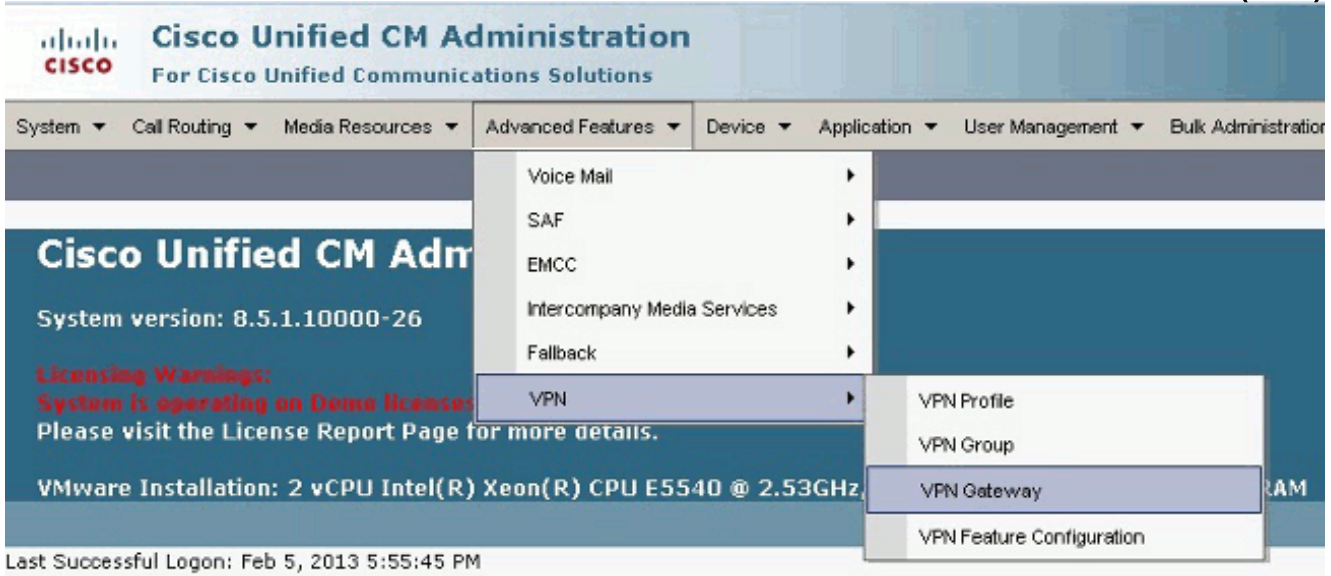
وفيما يلي شهادة الهوية المشفرة للبريد المحسن للخصوصية (PEM):

```
BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWWhcNMjMw-----
```

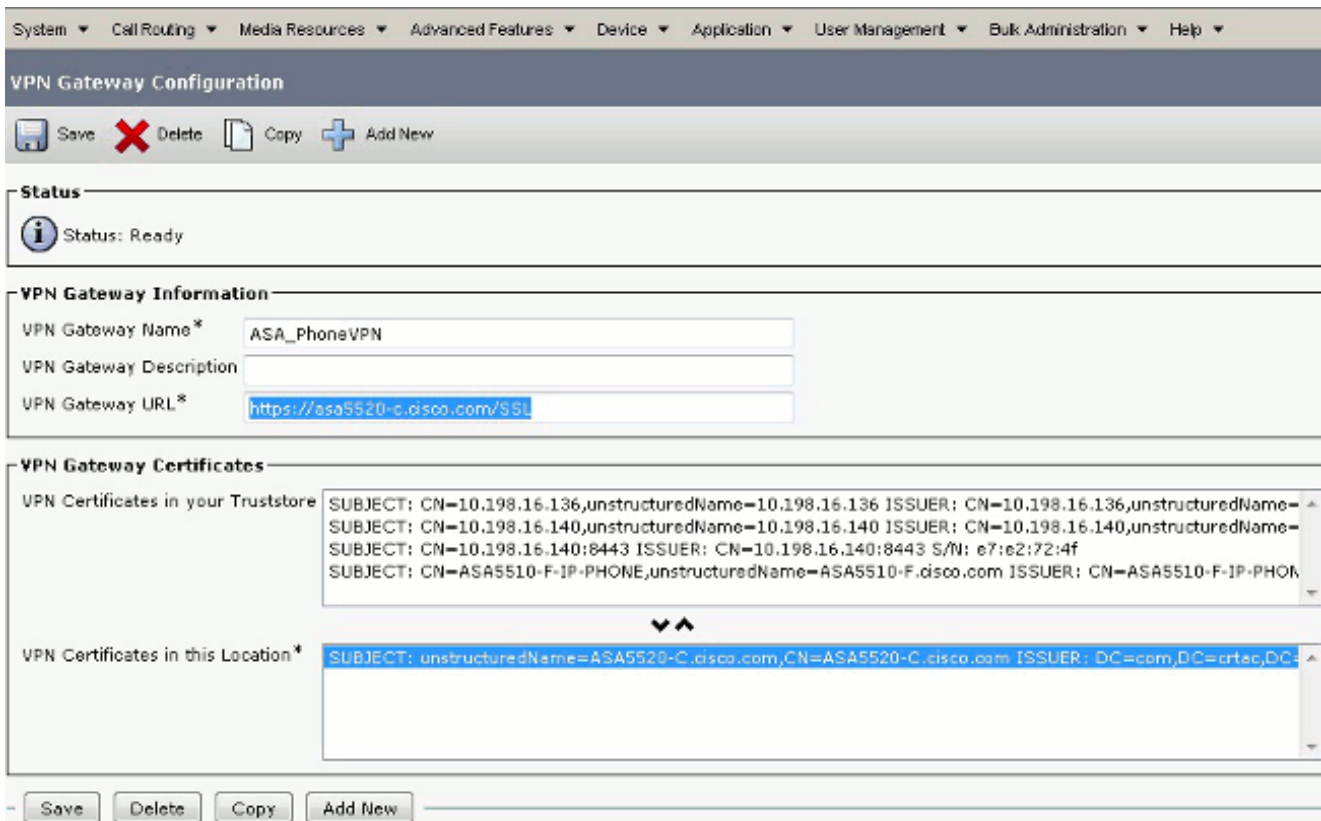
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxZjAUBGkqhkiG9w0BCQIWB0FTQTU1  
NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMycrys jZ+MawKBx8Zk69SW4AR  
FSpV6FPcUL7xssovhw6hsJE/2VDgd3pkawc5jc15vkcpTkjbf2xC4C1q6ZQwpahde22sdf1  
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1  
-----END CERTIFICATE-----

4. انسخ النص من الوحدة الطرفية واحفظه على هيئة ملف pem.
5. قم بتسجيل الدخول إلى CallManager واختر إدارة نظام التشغيل الموحدة < الأمان > إدارة الشهادات < تحميل الشهادة > تحديد ثقة الهاتف VPN لتحميل ملف الشهادة المحفوظ في الخطوة السابقة.  
تكوين VPN على CallManager

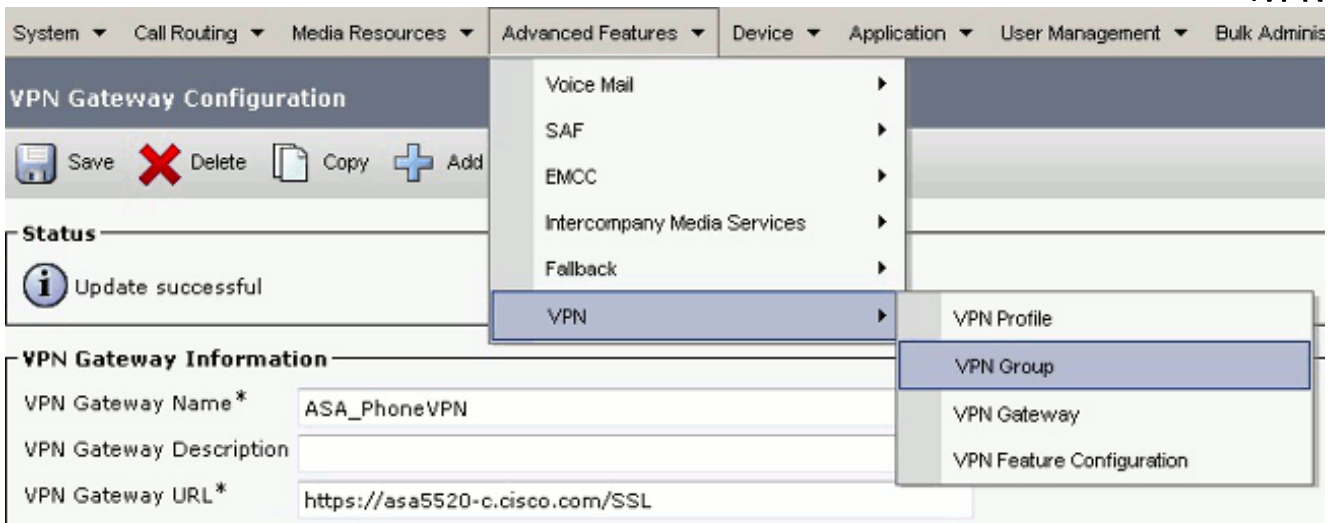
1. انتقل إلى إدارة Cisco Unified CM.
2. من شريط القوائم، اختر ميزات متقدمة < VPN > بوابة الشبكة الخاصة الظاهرية (VPN).



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 عنوان URL لعبارة VPN، أدخل عنوان URL الخاص بالمجموعة المعرف على ASA. في "شهادات الشبكة الخاصة الظاهرية (VPN)" في حقل "الموقع" هذا، حدد الشهادة التي تم تحميلها إلى CallManager مسبقا لنقلها من TrustStore إلى هذا الموقع.



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



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

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manag

## VPN Group Configuration

Save Delete Copy Add New

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

**VPN Gateway Information**

All Available VPN Gateways

Selected VPN Gateways in this VPN Group\*

ASA\_PhoneVPN

**Move the Gateway down**

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

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

## VPN Group Configuration

Save Delete Copy Add

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

VPN Profile

VPN Group

VPN Gateway


VPN Feature Configuration

7. أنمت 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

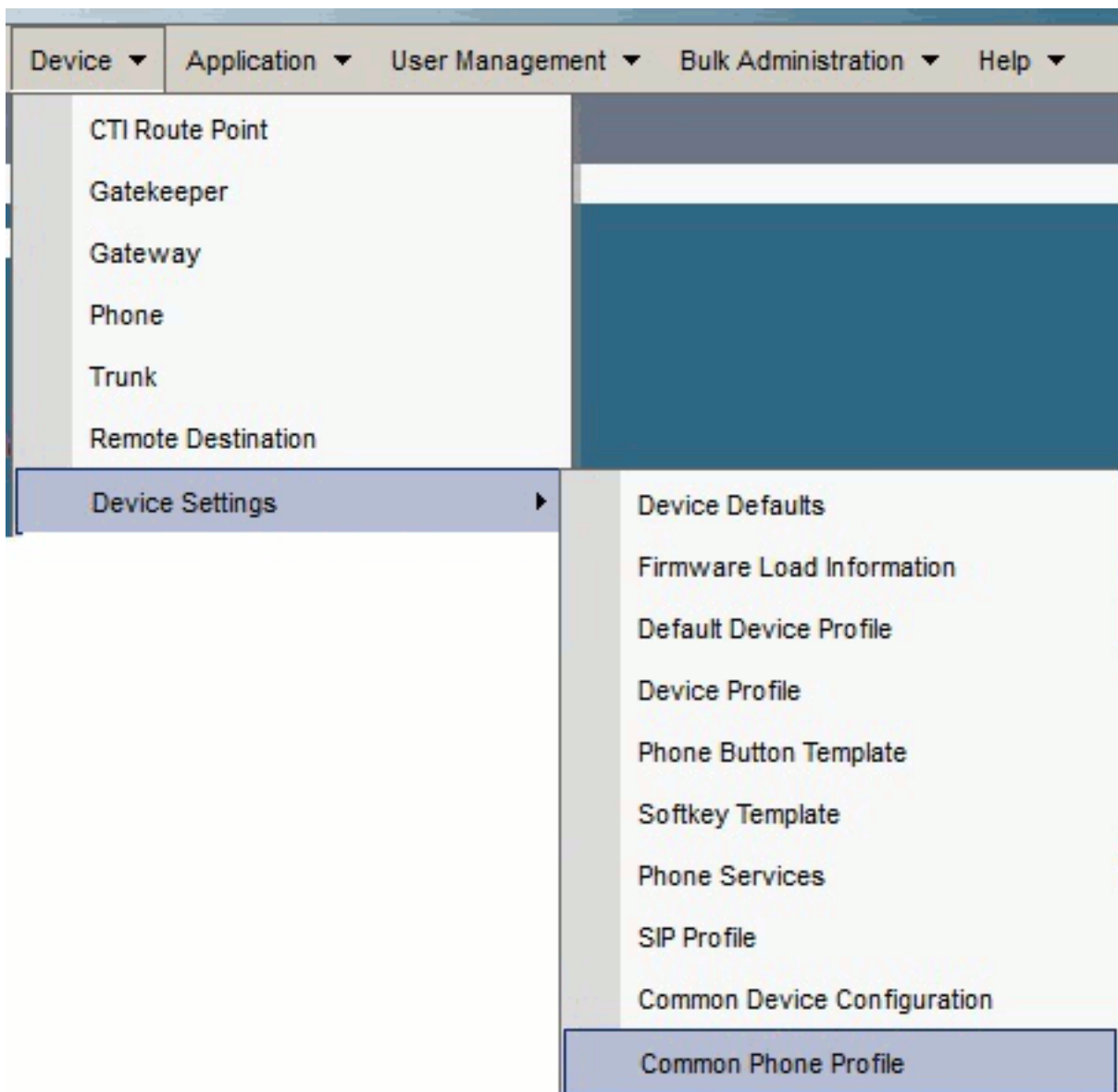
## Client Authentication

Client Authentication Method\*

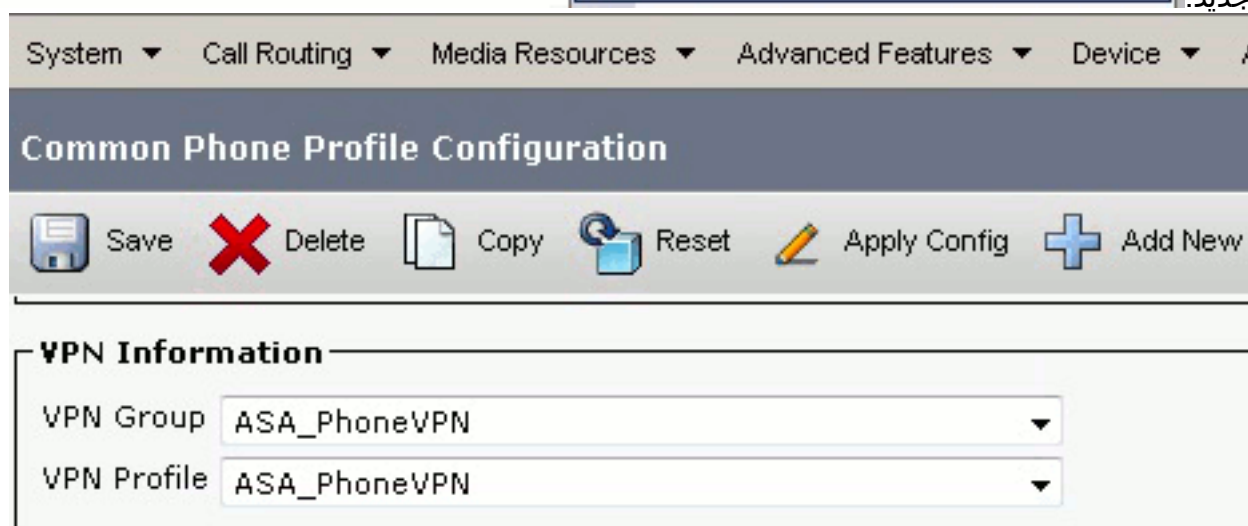
Enable Password Persistence

تمكين الكشف التلقائي عن الشبكة: إذا تم تمكين هذا الخيار، يقوم هاتف VPN بتعطيل خادم TFTP وإذا لم يتم تلقي أية إستجابة، فإنه يقوم تلقائياً ببدء اتصال VPN. تمكين التحقق من معرف المضيف: إذا تم تمكين هذا الخيار، يقوم هاتف شبكة VPN بمقارنة FQDN الخاص بعنوان URL لبوابة VPN مع CN/SAN الخاص بالشهادة. يفشل العميل في الاتصال إذا لم يتطابق أو إذا تم إستخدام 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.

8. في نافذة تكوين ملف تعريف الهاتف الشائع، انقر فوق تطبيق التكوين لتطبيق تكوين VPN الجديد. يمكنك إستخدام "توصيف الهاتف القياسي المشترك" أو إنشاء توصيف

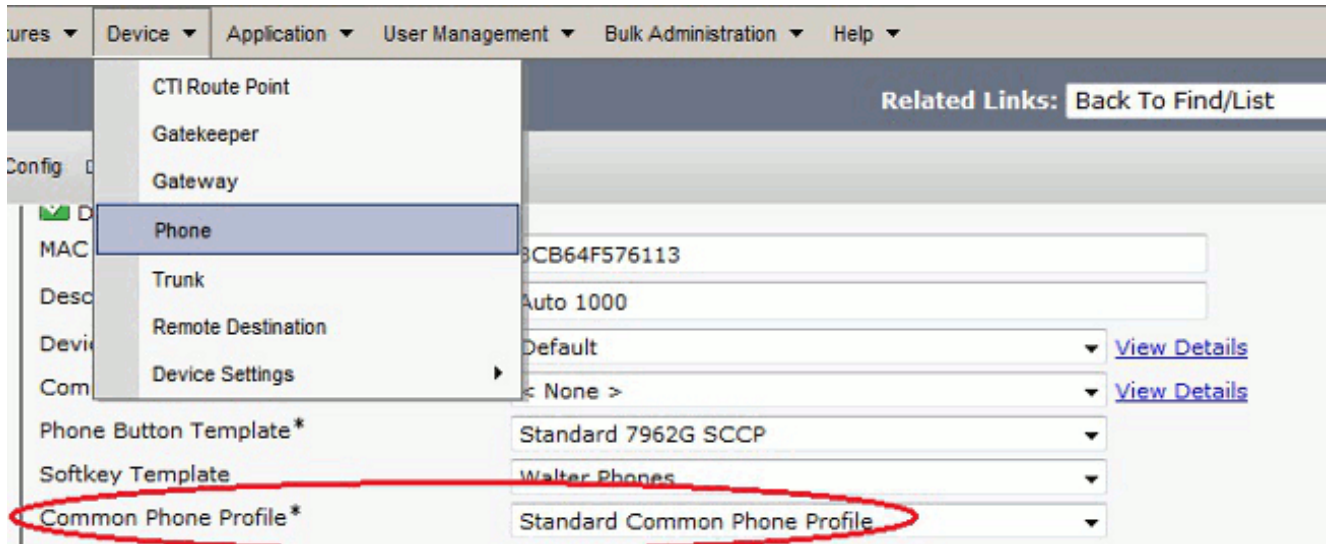


جديد.



9. إذا قمت بإنشاء ملف تعريف جديد لهواتف/مستخدمين معينين، فانتقل إلى نافذة تكوين الهاتف. في حقل ملف تعريف الهاتف الشائع، اختر ملف تعريف الهاتف الشائع القياسي.









10. سجل الهاتف إلى CallManager مرة أخرى لتنزيل التكوين الجديد.  
تكوين مصادقة الشهادة

لتكوين مصادقة الشهادة، أكمل الخطوات التالية في CallManager و ASA:

1. من شريط القوائم، اختر **ميزات متقدمة > VPN > ملف تخصيص VPN**.
2. تأكيد تعيين حقل أسلوب مصادقة العميل على **الشهادة**.


System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## 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

3. سجل الدخول إلى CallManager من شريط القوائم، أختار إدارة نظام التشغيل الموحد < التأمين > إدارة الترخيص < بحث.

4. تصدير الشهادة (الشهادات) الصحيحة لأسلوب مصادقة الشهادة المحدد::MICs Cisco\_MANUFACTURING\_CA - مصادقة هواتف IP باستخدام MIC

Find Certificate List where File Name ▾ begins with ▾

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>

(LSCs: Cisco Certificate Authority Proxy Function (CAPF) - مصادقة هواتف IP باستخدام LSC

Certificate Name	Certificate Type	.PEM File	
tomcat	certs	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>
psec	certs	<a href="#">losec.pem</a>	<a href="#">losec.der</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
psec-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
CallManager	certs	<a href="#">CallManager.pem</a>	<a href="#">CallManager.der</a>
CAPF	certs	<a href="#">CAPF.pem</a>	<a href="#">CAPF.der</a>
TVS	certs	<a href="#">TVS.pem</a>	<a href="#">TVS.der</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>	

5. ابحث عن الشهادة، إما Cisco\_MANUFACTURING\_CA أو CAPF. قم بتنزيل ملف pem. وحفظه كملف txt.

6. قم بإنشاء نقطة ثقة جديدة على ASA وصادق على TrustPoint الشهادة المحفوظة السابقة. عندما يطلب منك لشهادة CA المرمزة للأساس 64، حدد والصق النص في ملف pem. الذي تم تنزيله مع أسطر BEGIN و END. يتم عرض مثال:

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

<base-64 encoded CA certificate>

quit

7. تأكيد تعيين المصادقة في مجموعة النفق على مصادقة الشهادة.

```
tunnel-group SSL webvpn-attributes
authentication certificate
```

```
group-url https://asa5520-c.cisco.com/SSL enable
```

**تثبيت الشهادة على هواتف بروتوكول الإنترنت (IP)**

يمكن أن تعمل هواتف IP باستخدام بطاقات MIC أو LSCs، ولكن عملية التكوين مختلفة لكل شهادة.

### تثبيت MIC

وبشكل افتراضي، يتم تحميل جميع الهواتف التي تدعم VPN مسبقا بميكروفونات. هواتف 7960 و 7940 لا تأتي مع ميكروفون، وتتطلب إجراءات تركيب خاصة ليسجل LSC بأمان.

**ملاحظة:** توصي Cisco باستخدام أجهزة MICs لتثبيت LSC فقط. تدعم Cisco قوائم التحكم في الوصول (LSCs) لمصادقة اتصال TLS باستخدام CUCM. نظرا لإمكانية اختراق شهادات جذر الميكروفون، يقوم العملاء الذين يقومون بتكوين الهواتف لاستخدام ميكروفون لمصادقة TLS أو لأي غرض آخر بذلك على مسؤوليتهم الخاصة. لا تتحمل Cisco أي مسؤولية في حالة اختراق بطاقات MIC.

### تثبيت LSC

1. تمكين خدمة CAPF على CUCM.

2. بعد تنشيط خدمة CAPF، قم بتعيين إرشادات الهاتف لإنشاء LSC في CUCM. سجل الدخول إلى إدارة Cisco Unified CM واختار الجهاز < الهاتف. حدد الهاتف الذي قمت بتكوينه.

3. في قسم معلومات وظيفية وكيل المرجع المصدق (CAPF)، تأكد من صحة كافة الإعدادات ومن تعيين العملية على تاريخ مستقبلي.

## Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
Authentication String	123456
<input type="button" value="Generate String"/>	
Key Size (Bits)*	2048
Operation Completes By	2013 3 10 12 (YYYY:MM:DD:HH)
Certificate Operation Status: None	
Note: Security Profile Contains Addition CAPF Settings.	

4. في حالة تعيين وضع المصادقة إلى سلسلة خالية أو شهادة موجودة، لا يتطلب الأمر أي إجراء إضافي.
5. إذا كان وضع المصادقة مضبوطاً على سلسلة، فحدد يدوياً الإعدادات < تكوين التأمين < #\*\* < LSC < تحديث في وحدة تحكم الهاتف.

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

### التحقق من ASA

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

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

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

:AnyConnect-Parent
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
```

Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
(Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0  
Bytes Tx : 1759 Bytes Rx : 799  
Pkts Tx : 2 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

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

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

## التحقق من CUCM

Device Name	Description	Device Pool	Device Protocol	Status	IP Address
SEPXXXXXXXXXXXX	Auto 1001	Default	SCCP	Unknown	Unknown
SEPXXXXXXXXXXXX	Auto 1000	Default	SCCP	Registered with: 192.168.100.1	10.10.10.2

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

### الأخطاء ذات الصلة

- معرف تصحيح الأخطاء من Cisco [CSCtf09529](#)، إضافة دعم لميزة VPN في CUCM لالهواتف 8961، 9951، 9971
- معرف تصحيح الأخطاء من Cisco [CSCuc71462](#)، تستغرق عملية تجاوز فشل هاتف 8 VPN IP دقائق
- معرف تصحيح الأخطاء من Cisco [CSCtz42052](#)، دعم VPN لهاتف IP SSL لأرقام المنافذ غير الافتراضية

- cisco بق [CSCth96551](#) id، ليس كل ASCII رمز مدعوم أثناء هاتف VPN مستعمل + كلمة تسجيل الدخول.
- معرف تصحيح الأخطاء من [CSCuj71475](#) Cisco، الإدخال اليدوي TFTP المطلوب ل IP Phone VPN
- معرف تصحيح الأخطاء من [CSCum10683](#) Cisco، هواتف IP التي لا تسجل المكالمات الفاتكة أو الموزعة أو المستلمة

## معلومات ذات صلة

- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل م عد ي و ت ح م م ي د ق ت ل ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ي ل أ ة مچرت ل ض ف أ ن أ ة ظ ح ال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا