وأ Windows 7 ءالمع عم ASA IKEv2 RA VPN ةداهشلا ةقداصم نيوكتو Android VPN

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco الإصدار 9.7.1 والإصدارات الأحدث للسماح لعملاء Windows 7 و Android الأصليين (الشبكة الخاصة الظاهرية) VPN بإنشاء اتصال RA VPN (الوصول عن بعد) باستخدام بروتوكول تبادل مفتاح الإنترنت (IKEv2) والشهادات كطريقة مصادقة.

تمت المساهمة من قبل ديفيد ريفيرا و سيزار لوبيز زاماريبا، مهندسي TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جهة منح الشهادة (CA)
- البنية الأساسية للمفتاح العام (PKI)
- RA VPN مع IKEv2 على ASA
- عميل شبكة VPN مدمج يعمل بنظام التشغيل Windows 7
- عميل VPN الأصلي من Android

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- Cisco 1921/K9 - 15.5(3)M4a as IOS CA Server
- ASA5506X - 9.7(1) كنقطة الاستقبال والبث VPN
- نظام التشغيل Windows 7 كجهاز عميل
- Galaxy J5 - نظام التشغيل Android 6.0.1 كعميل جهاز محمول

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

التكوين

نظرة عامة

هذه هي الخطوات اللازمة لتكوين عملاء VPN الأصليين لنظام التشغيل Windows 7 و Android للاتصال بمنفذ ASA:

تكوين مرجع الشهادة

يسمح CA بتضمين إستخدام المفتاح الموسع (EKU) المطلوب في الشهادة. بالنسبة لمحطة الاستقبال والبث الخاصة ب ASA، يلزم مصادقة خادم الشهادة EKU، بينما تحتاج شهادة العميل إلى وحدة الاستقبال والبث الخاصة بالعميل.

يمكن إستخدام مجموعة متنوعة من خوادم CA مثل:

- خادم IOS CA من Cisco
- خادم OpenSSL CA
- خادم Microsoft CA
- 3سطح إئتمان الأطراف

يتم إستخدام خادم IOS CA لمثال التكوين هذا.

يلخص هذا قسم التشكيل أساسي أن يجعل Cisco1921/K9 مع صيغة 15.5(3)M4a يعمل كخادم CA.

الخطوة 1. تأكد من أن الجهاز والإصدار يدعمان أمر eku.

```
IOS-CA# show run | section crypto pki
<crypto pki server <CA_Server
<issuer-name <cn=calo_root,ou=TAC,o=cisco
grant auto
eku server-auth client-auth
```

الخطوة 2. قم بتمكين خادم HTTP على الموجه.

```
IOS-CA(config)#ip http server
```

الخطوة 3. قم بإنشاء زوج مفاتيح RSA قابل للتصدير.

```
IOS-CA(config)# crypto key generate rsa modulus 2048 label <HeadEnd> exportable
The name for the keys will be: HeadEnd
The key modulus size is 2048 bits %
...Generating 2048 bit RSA keys, keys will be exportable %
(OK] (elapsed time was 5 seconds]
```

الخطوة 4. تكوين TrustPoint.

```
<IOS-CA(config)# crypto pki trustpoint <HeadEnd
IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
<IOS-CA(ca-trustpoint)#subject-name <cn=HeadEnd.david.com
IOS-CA(ca-trustpoint)#revocation-check none
<IOS-CA(ca-trustpoint)#rsakeypair <HeadEnd
```

ملاحظة: عنوان IP لأمر التسجيل هو أحد عناوين IP التي تم تكوينها للواجهة القابلة للوصول الخاصة بالموجه.

الخطوة 5. مصادقة TrustPoint (الحصول على شهادة CA).

```
<IOS-CA(config)#crypto pki authenticate <HeadEnd
:Certificate has the following attributes
Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
Do you accept this certificate? [yes/no]: yes %
.Trustpoint CA certificate accepted
```

الخطوة 6. قم بتسجيل TrustPoint (الحصول على شهادة الهوية).

```
<IOS-CA(config)#crypto pki enroll <HeadEnd
%
.. Start certificate enrollment %
Create a challenge password. You will need to verbally provide this %
.password to the CA Administrator in order to revoke your certificate
.For security reasons your password will not be saved in the configuration
.Please make a note of it
Password: cisco123
Re-enter password: cisco123
The subject name in the certificate will include: cn=HeadEnd.david.com %
The subject name in the certificate will include: Connected_2_INET-B %
Include the router serial number in the subject name? [yes/no]: no %
Include an IP address in the subject name? [no]: no %
Request certificate from CA? [yes/no]: yes
Certificate request sent to Certificate Authority %
.The 'show crypto pki certificate verbose HeadEnd' command will show the fingerprint %
Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 0017C310 9F6084E8*
63053228 B449794F
Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: CFE22C7A B2855C4D*
B4B2412B 57FC7106 1C5E7791
Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority*
```

الخطوة 7. تحقق من الشهادات.

```
<IOS-CA#show crypto pki certificates verbose <HeadEnd
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 05
  Certificate Usage: General Purpose
  :Issuer
    cn=calo_root
  :Subject
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
    cn=HeadEnd.david.com
  :Validity Date
    start date: 16:56:14 UTC Jul 16 2017
    end   date: 16:56:14 UTC Jul 16 2018
  :Subject Key Info
```

```
                                  Public Key Algorithm: rsaEncryption
                                           (RSA Public Key: (2048 bit
                          Signature Algorithm: SHA1 with RSA Encryption
                   Fingerprint MD5: 0017C310 9F6084E8 63053228 B449794F
         Fingerprint SHA1: CFE22C7A B2855C4D B4B2412B 57FC7106 1C5E7791
                                                     :X509v3 extensions
                                           X509v3 Key Usage: A0000000
                                                  Digital Signature
                                                   Key Encipherment
  X509v3 Subject Key ID: E9B3A080 779A76E7 8BE44F38 C3E4DEDF 18E75009
X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
                                                :Authority Info Access
                                                  :Extended Key Usage
                                                      Client Auth
                                                      Server Auth
                                        Associated Trustpoints: HeadEnd
                                                     Key Label: HeadEnd

                                                           CA Certificate
                                                      Status: Available
                                                             Version: 3
                                    Certificate Serial Number (hex): 01
                                           Certificate Usage: Signature
                                                                :Issuer
                                                         cn=calo_root
                                                               :Subject
                                                         cn=calo_root
                                                         :Validity Date
                                 start date: 13:24:35 UTC Jul 13 2017
                                 end   date: 13:24:35 UTC Jul 12 2020
                                                      :Subject Key Info
                                  Public Key Algorithm: rsaEncryption
                                           (RSA Public Key: (1024 bit
                           Signature Algorithm: MD5 with RSA Encryption
                   Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
         Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
                                                     :X509v3 extensions
                                           X509v3 Key Usage: 86000000
                                                  Digital Signature
                                                      Key Cert Sign
                                                      CRL Signature
  X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
                                            :X509v3 Basic Constraints
                                                         CA: TRUE
X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
                                               :Authority Info Access
                         Associated Trustpoints: test HeadEnd CA_Server
```

الخطوة 8. قم بتصدير HeadEnd TrustPoint إلى الوحدة الطرفية بتنسيق PKCS12 للحصول على شهادة الهوية. تتم إضافة شهادة CA والمفتاح الخاص في ملف واحد مفرد.

```
                                IOS-CA(config)#crypto pki export



                                             <cisco123>
                                        :Exported pkcs12 follows
MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH
BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz
Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB
3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj
v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV
```

```
ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu
niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3
vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz
+EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y
Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2
bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F
bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam
RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b
eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg
VbYsR+51XfQEH5xu88E5EUPWZ86YdUSlbD8ky6WOn0M1O4K6rNDLkgwXcxw3CaZ8
zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8
C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc
OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN+
Ua0MbDEa8T5Le4dCigaA+t1QxQOPGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O
lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw
9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h
9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC
77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2
zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7LOlCeUcVDM8aQfy
HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X
2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE
RE6m7O8RiPSD2RjjamCmmmnH5dK5wxF7YlIeK/+ZVrfwLecEPRl+eVw0isM/JN/a
WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs
yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR
4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhGO88voq8MMGXEe/q+DIjaVE1htYu
k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWXlXfgrfLEH0utwHTyr3J2vQk5CD37
ZAfsF6zxEvtU2t41J0e9OjWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y
BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg
ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm9OBsqd12lHurCCmHy7kM5pqf0MMlhH7
oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR
QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX1l
BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte
ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt
xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w
+S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d
ik6bmxcnO0qdcHtt2HTbI+kYpken3YrFOh9Jnm9ZKT63gQSqQWL800ZVd4dAZceg
FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd
XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn
ISSzQjrkxoNwwOfn87O5fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy
/FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N
Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ
jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9
TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp
3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn
cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir
pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX
AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp
kuauRzQ8/pwszaZuPh/5rE77z8zMut3+OE5CslB9npzNi0b0itaaRl13bBBml1xn
r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG
ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR
B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id
zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr
ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv
cJRb68aOyZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSFlM89Sn4
GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo
5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z
LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F
I8Ii8TA9MCEwCQYFKw4DAhoFAAQUjO/On/REYODupznP9SwYnFX92BYEFESx1MSa
==ho3Cv1cZYM0TzZEzlsKdAgIEAA
```

```
End - This line not part of the pkcs12------

.CRYPTO_PKI: Exported PKCS12 file successfully
.Jul 17 15:46:49.706: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported*
```

الخطوة 9. قم بإنشاء نقطة ثقة فارغة على ASA.

```
<ASA(config)# crypto ca trustpoint <HeadEnd
DRIVERAP(config-ca-trustpoint)# exit
```

الخطوة 10. قم باستيراد ملف PKCS12.

```
<ASA(config)#crypto ca import <HeadEnd> pkcs12 <cisco123
.Enter the base 64 encoded pkcs12
:End with the word "quit" on a line by itself
```

```
MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH
BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz
Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB
3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj
v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV
ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu
niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3
vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz
+EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y
Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2
bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F
bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam
RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b
eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg
VbYsR+51XfQEH5xu88E5EUPWZ86YdUSlbD8ky6WOn0M1O4K6rNDLkgwXcxw3CaZ8
zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8
C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc
OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN+
Ua0MbDEa8T5Le4dCigaA+t1QxQOPGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O
lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw
9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h
9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC
77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2
zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7LOlCeUcVDM8aQfy
HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X
2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE
RE6m7O8RiPSD2RjjamCmmmnH5dK5wxF7YlIeK/+ZVrfwLecEPRl+eVw0isM/JN/a
WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs
yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR
4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhGO88voq8MMGXEe/q+DIjaVE1htYu
k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWXlXfgrfLEH0utwHTyr3J2vQk5CD37
ZAfsF6zxEvtU2t41J0e9OjWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y
BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg
ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm9OBsqd12lHurCCmHy7kM5pqf0MMlhH7
oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR
QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX1l
BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte
ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt
xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w
+S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d
ik6bmxcnO0qdcHtt2HTbI+kYpken3YrFOh9Jnm9ZKT63gQSqQWL800ZVd4dAZceg
FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd
XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn
ISSzQjrkxoNwwOfn87O5fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy
/FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N
Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ
jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9
TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp
3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn
cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir
pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX
```

```
AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp
kuauRzQ8/pwszaZuPh/5rE77z8zMut3+OE5CslB9npzNi0b0itaaRl13bBBml1xn
r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG
ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR
B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id
zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr
ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv
cJRb68aOyZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSFlM89Sn4
GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo
5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z
LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F
I8Ii8TA9MCEwCQYFKw4DAhoFAAQUjO/On/REYODupznP9SwYnFX92BYEFESx1MSa
                                    ==ho3Cv1cZYM0TzZEzlsKdAgIEAA
                                                            quit
            INFO: Import PKCS12 operation completed successfully
```

الخطوة 11. تحقق من معلومات الشهادة.

```
<ASA(config)#show crypto ca certificates <HeadEnd
                                   CA Certificate
                              Status: Available
                  Certificate Serial Number: 01
                   Certificate Usage: Signature
               (Public Key Type: RSA (1024 bits
   Signature Algorithm: MD5 with RSA Encryption
                                   :Issuer Name
                                 cn=calo_root
                                  :Subject Name
                                 cn=calo_root
                                 :Validity Date
         start date: 13:24:35 UTC Jul 13 2017
         end   date: 13:24:35 UTC Jul 12 2020
                                Storage: config
           Associated Trustpoints: test HeadEnd
                                      Certificate
                              Status: Available
                  Certificate Serial Number: 05
             Certificate Usage: General Purpose
               (Public Key Type: RSA (2048 bits
  Signature Algorithm: SHA1 with RSA Encryption
                                   :Issuer Name
                                 cn=calo_root
                                  :Subject Name
                  hostname=Connected_2_INET-B
                         cn=HeadEnd.david.com
                                 :Validity Date
         start date: 16:56:14 UTC Jul 16 2017
         end   date: 16:56:14 UTC Jul 16 2018
                                Storage: config
                Associated Trustpoints: HeadEnd
```

إنشاء شهادة عميل

الخطوة 1. قم بإنشاء زوج مفاتيح RSA قابل للتصدير.

```
IOS-CA(config)# crypto key generate rsa modulus 2048 label <Win7_PC> exportable
                                         The name for the keys will be: Win7_PC
                                            The key modulus size is 2048 bits %
                     ...Generating 2048 bit RSA keys, keys will be exportable %
                                               OK] (elapsed time was 5 seconds]
```

الخطوة 2. تكوين TrustPoint.

```
<IOS-CA(config)# crypto pki trustpoint <Win7_PC
IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
<IOS-CA(ca-trustpoint)#subject-name <cn=Win7_PC.david.com
IOS-CA(ca-trustpoint)#revocation-check none
<IOS-CA(ca-trustpoint)#rsakeypair <Win7_PC
```

الخطوة 3. مصادقة TrustPoint التي تم تكوينها (الحصول على شهادة CA).

```
<IOS-CA(config)#crypto pki authenticate <Win7_PC
:Certificate has the following attributes
Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
Do you accept this certificate? [yes/no]: yes %
.Trustpoint CA certificate accepted
```

الخطوة 4. تسجيل TrustPoint التي تمت مصادقتها (الحصول على شهادة الهوية).

```
<IOS-CA(config)#crypto pki enroll <Win7_PC
%
.. Start certificate enrollment %
Create a challenge password. You will need to verbally provide this %
.password to the CA Administrator in order to revoke your certificate
.For security reasons your password will not be saved in the configuration
.Please make a note of it
Password: cisco123
Re-enter password: cisco123
The subject name in the certificate will include: cn=Win7_PC.david.com %
The subject name in the certificate will include: Connected_2_INET-B %
Include the router serial number in the subject name? [yes/no]: no %
Include an IP address in the subject name? [no]: no %
Request certificate from CA? [yes/no]: yes
Certificate request sent to Certificate Authority %
.The 'show crypto pki certificate verbose Win7_PC' command will show the fingerprint %
Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 9153E537 11C16FAE*
B03F7A38 775DBB92
Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 3BC4AC98 91067707*
BB6BBBFB ABD97796 F7FB3DD1
Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority*
```

الخطوة 5. تحقق من معلومات الشهادات.

```
<IOS-CA#show crypto pki certificates verbose <Win7_PC
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
:Issuer
cn=calo_root
:Subject
Name: Connected_2_INET-B
hostname=Connected_2_INET-B
cn=Win7_PC.david.com
:Validity Date
start date: 13:29:51 UTC Jul 13 2017
end   date: 13:29:51 UTC Jul 13 2018
:Subject Key Info
Public Key Algorithm: rsaEncryption
(RSA Public Key: (2048 bit
Signature Algorithm: SHA1 with RSA Encryption
```

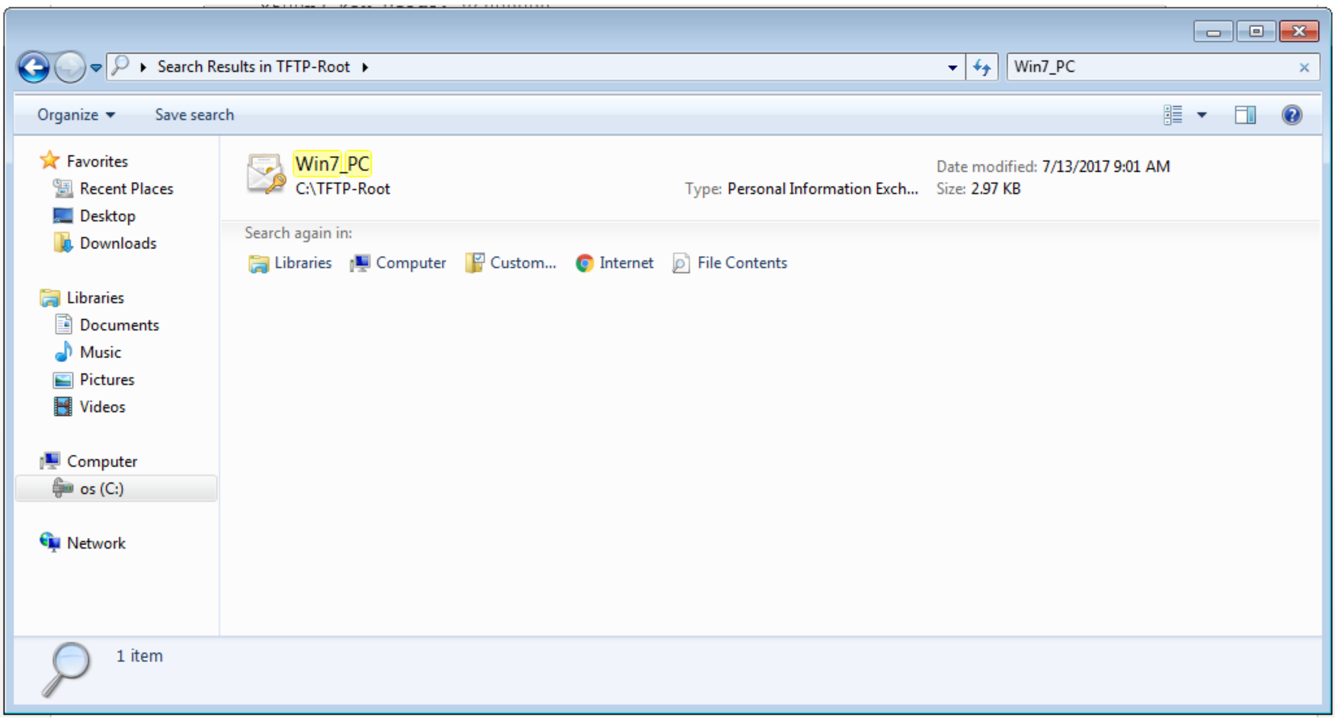
```
Fingerprint MD5: 9153E537 11C16FAE B03F7A38 775DBB92
Fingerprint SHA1: 3BC4AC98 91067707 BB6BBBFB ABD97796 F7FB3DD1
:X509v3 extensions
X509v3 Key Usage: A0000000
Digital Signature
Key Encipherment
X509v3 Subject Key ID: F37266AE 61F64BD9 3E9FA80C 77455F21 5BEB870D
X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
:Authority Info Access
:Extended Key Usage
Client Auth
Server Auth
Associated Trustpoints: Win7_PC
Key Label: Win7_PC
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 01
Certificate Usage: Signature
:Issuer
cn=calo_root
:Subject
cn=calo_root
:Validity Date
start date: 13:24:35 UTC Jul 13 2017
end   date: 13:24:35 UTC Jul 12 2020
:Subject Key Info
Public Key Algorithm: rsaEncryption
(RSA Public Key: (1024 bit
Signature Algorithm: MD5 with RSA Encryption
Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
:X509v3 extensions
X509v3 Key Usage: 86000000
Digital Signature
Key Cert Sign
CRL Signature
X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
:X509v3 Basic Constraints
CA: TRUE
X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
:Authority Info Access
Associated Trustpoints: test HeadEnd Win7_PC CA_Server
```

تثبيت شهادة الهوية على جهاز عميل Windows 7

الخطوة 1. قم بتصدير Win7_PC TrustPoint المسمى إلى خادم FTP/TFTP (المثبت على جهاز Windows 7) بتنسيق PKCS12 (.p12) للحصول على شهادة الهوية وشهادة CA والمفتاح الخاص في ملف واحد.

```
IOS-CA(config)#crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password
<<cisco123
?[Address or name of remote host [10.152.206.175
?[Destination filename [Win7_PC.p12
Writing pkcs12 file to tftp://10.152.206.175/Win7_PC.p12!
!
.CRYPTO_PKI: Exported PKCS12 file successfully
.Jul 17 16:29:20.310: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported*
```

هذه هي الطريقة التي يبدو بها الملف المصدر على جهاز عميل.



Win7_PC

Win7_PC

C:\TFTP-Root

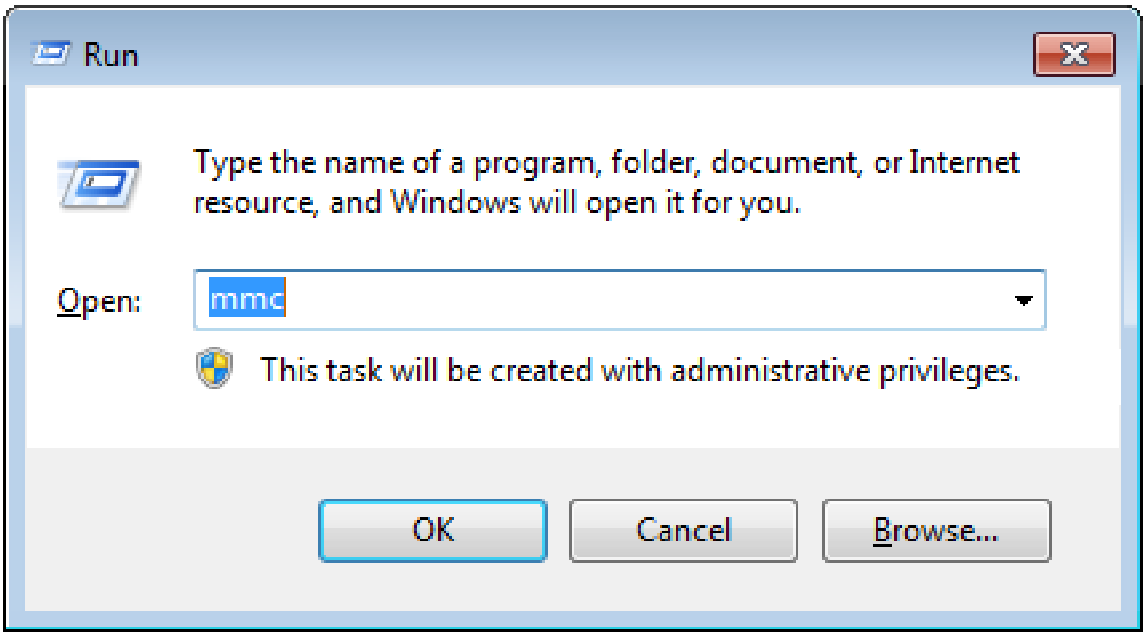
Type: Personal Information Exch...

Date modified: 7/13/2017 9:01 AM

Size: 2.97 KB

1 item

الخطوة 2. اضغط على **Ctrl + R** واكتب **MMC** لفتح وحدة تحكم الإدارة (MMC) من Microsoft.

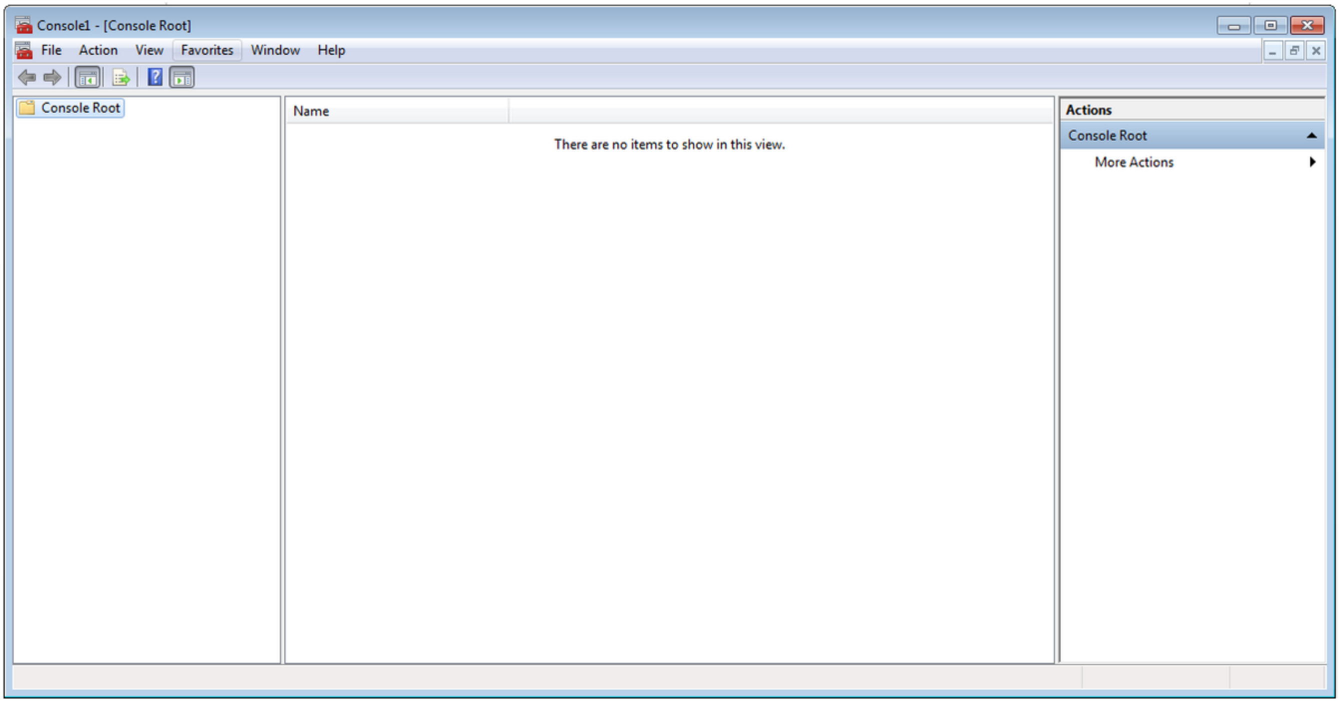

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

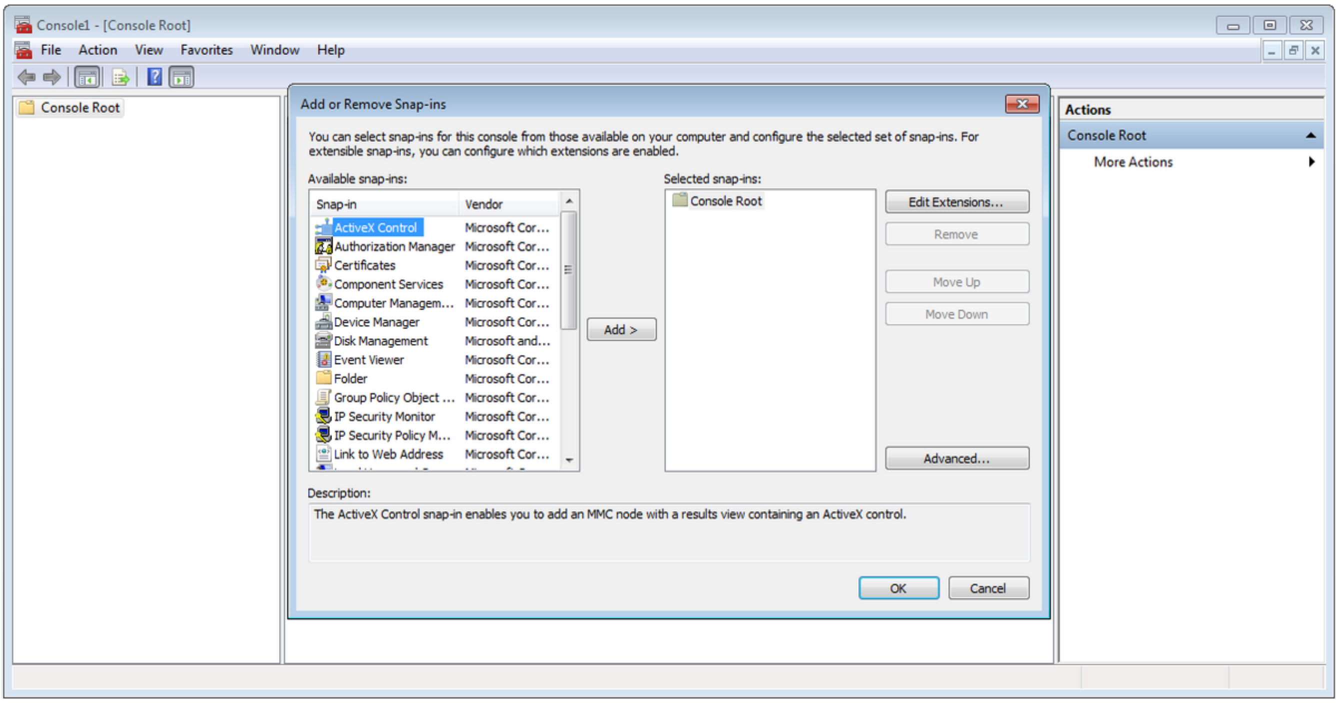
This task will be created with administrative privileges.

الخطوة 3. حدد **OK**.



There are no items to show in this view.

الخطوة 4. انتقل إلى **ملف>إضافة/إزالة الأداة الإضافية**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

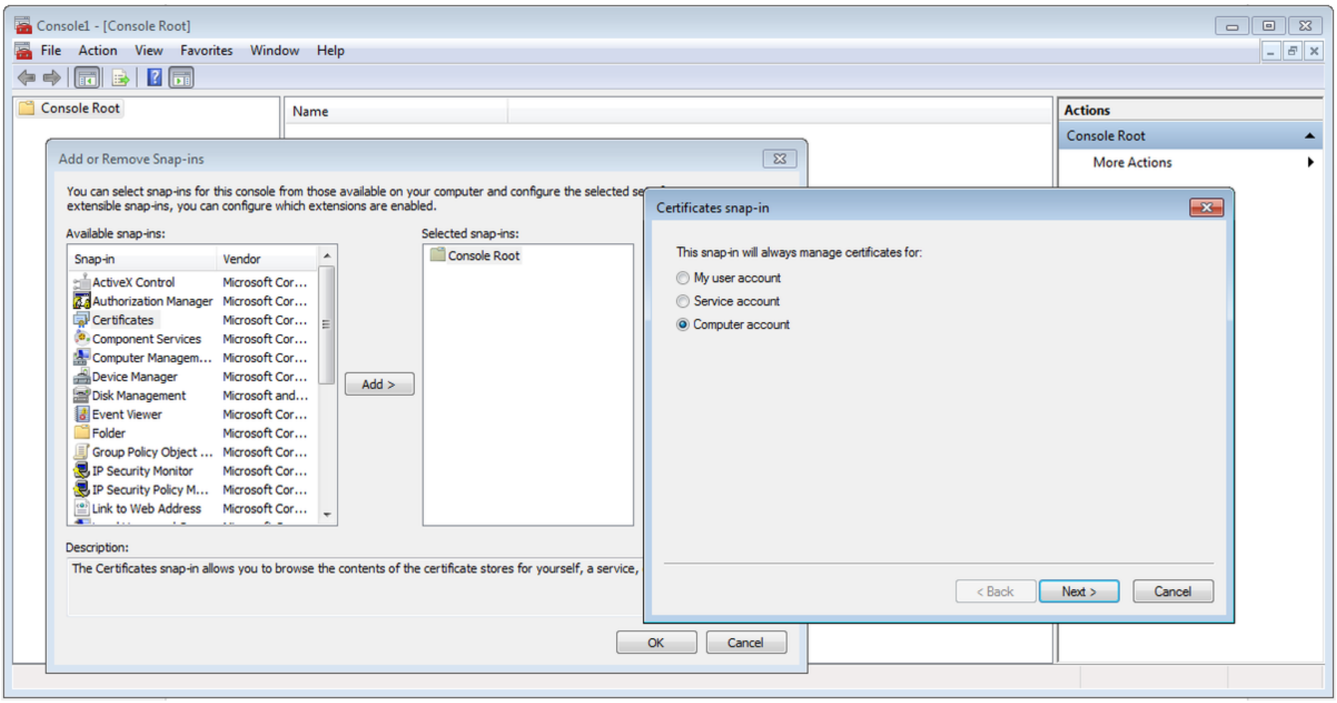
Selected snap-ins:

Console Root

Description:

The ActiveX Control snap-in enables you to add an MMC node with a results view containing an ActiveX control.

الخطوة 5. حدد **شهادات > إضافة > حساب الكمبيوتر**.



You can select snap-ins for this console from those available on your computer and configure the selected se… extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor…
Authorization Manager	Microsoft Cor…
Certificates	Microsoft Cor…
Component Services	Microsoft Cor…
Computer Managem…	Microsoft Cor…
Device Manager	Microsoft Cor…
Disk Management	Microsoft and…
Event Viewer	Microsoft Cor…
Folder	Microsoft Cor…
Group Policy Object …	Microsoft Cor…
IP Security Monitor	Microsoft Cor…
IP Security Policy M…	Microsoft Cor…
Link to Web Address	Microsoft Cor…

Selected snap-ins: Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service,

Certificates snap-in

This snap-in will always manage certificates for:

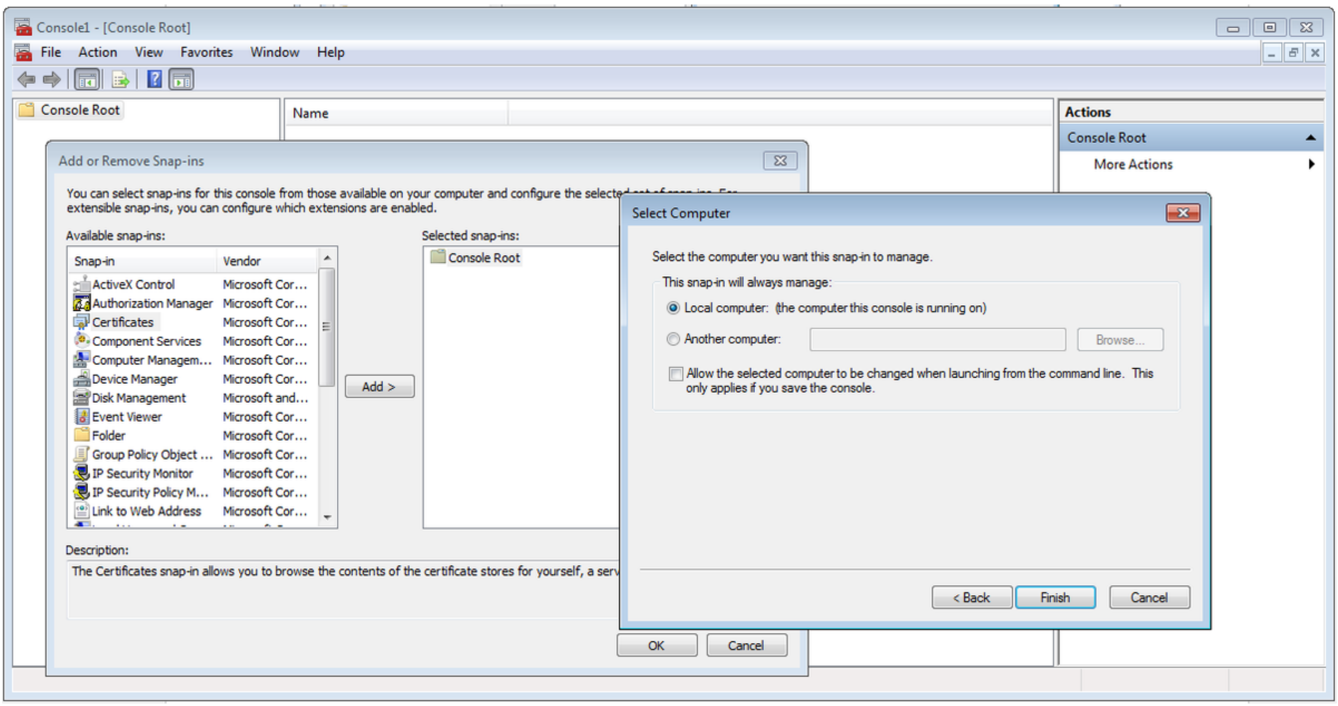
○ My user account

○ Service account

● Computer account

< Back | Next > | Cancel

الخطوة 6. حدد **التالي**،



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor…
Authorization Manager	Microsoft Cor…
Certificates	Microsoft Cor…
Component Services	Microsoft Cor…
Computer Managem…	Microsoft Cor…
Device Manager	Microsoft Cor…
Disk Management	Microsoft and…
Event Viewer	Microsoft Cor…
Folder	Microsoft Cor…
Group Policy Object …	Microsoft Cor…
IP Security Monitor	Microsoft Cor…
IP Security Policy M…	Microsoft Cor…
Link to Web Address	Microsoft Cor…

Selected snap-ins: Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a serv

Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

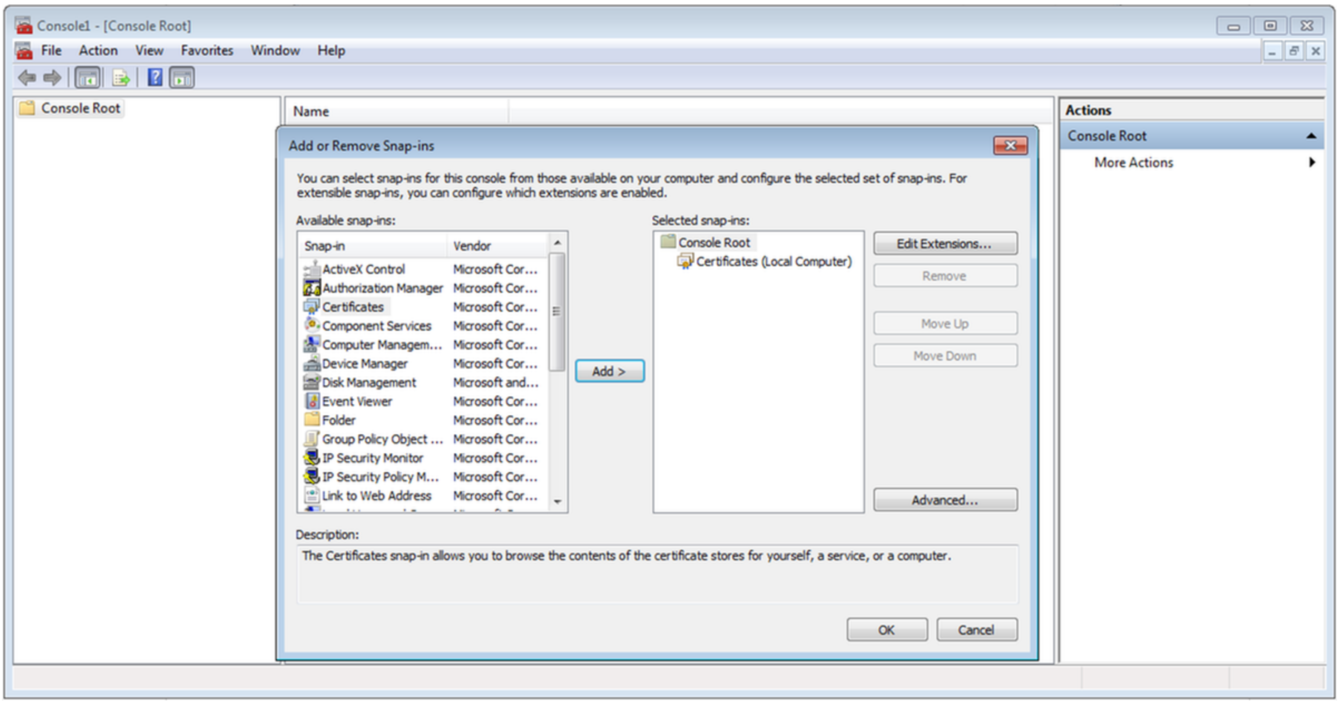
● Local computer: (the computer this console is running on)

○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

< Back | Finish | Cancel

الخطوة 7. **إنهاء**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

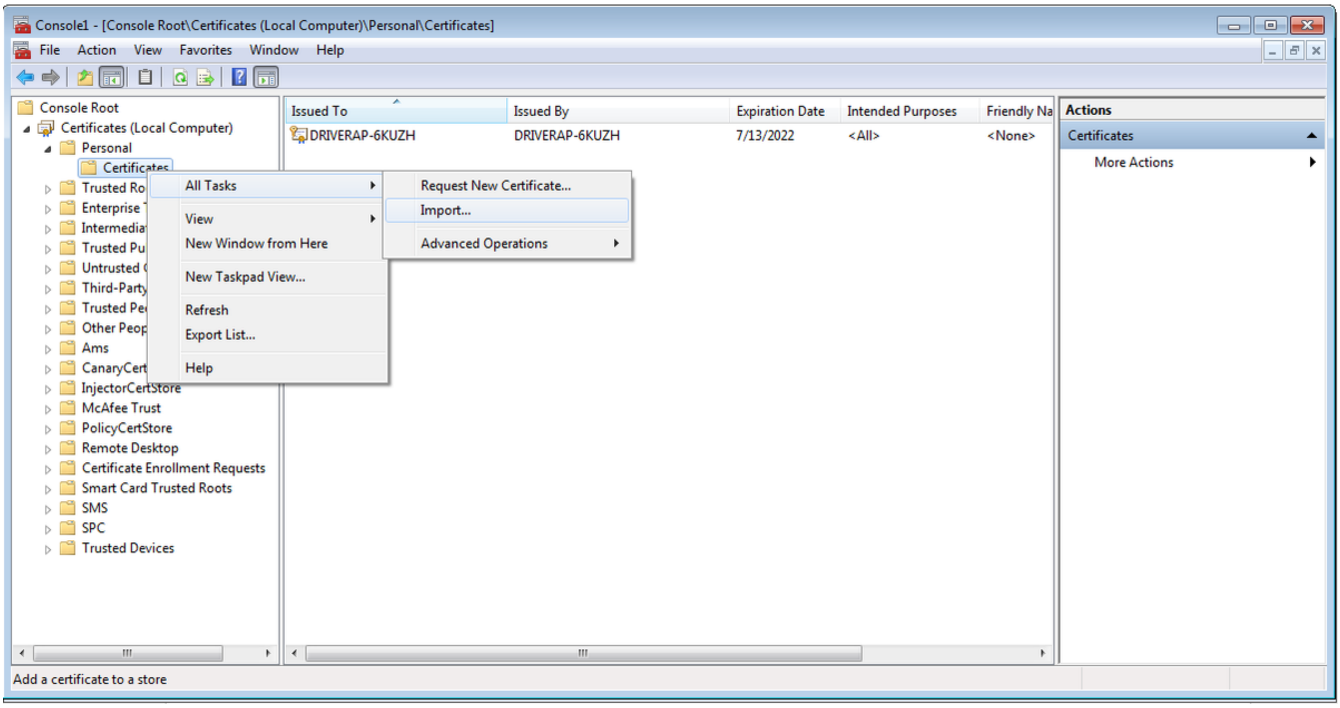
Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

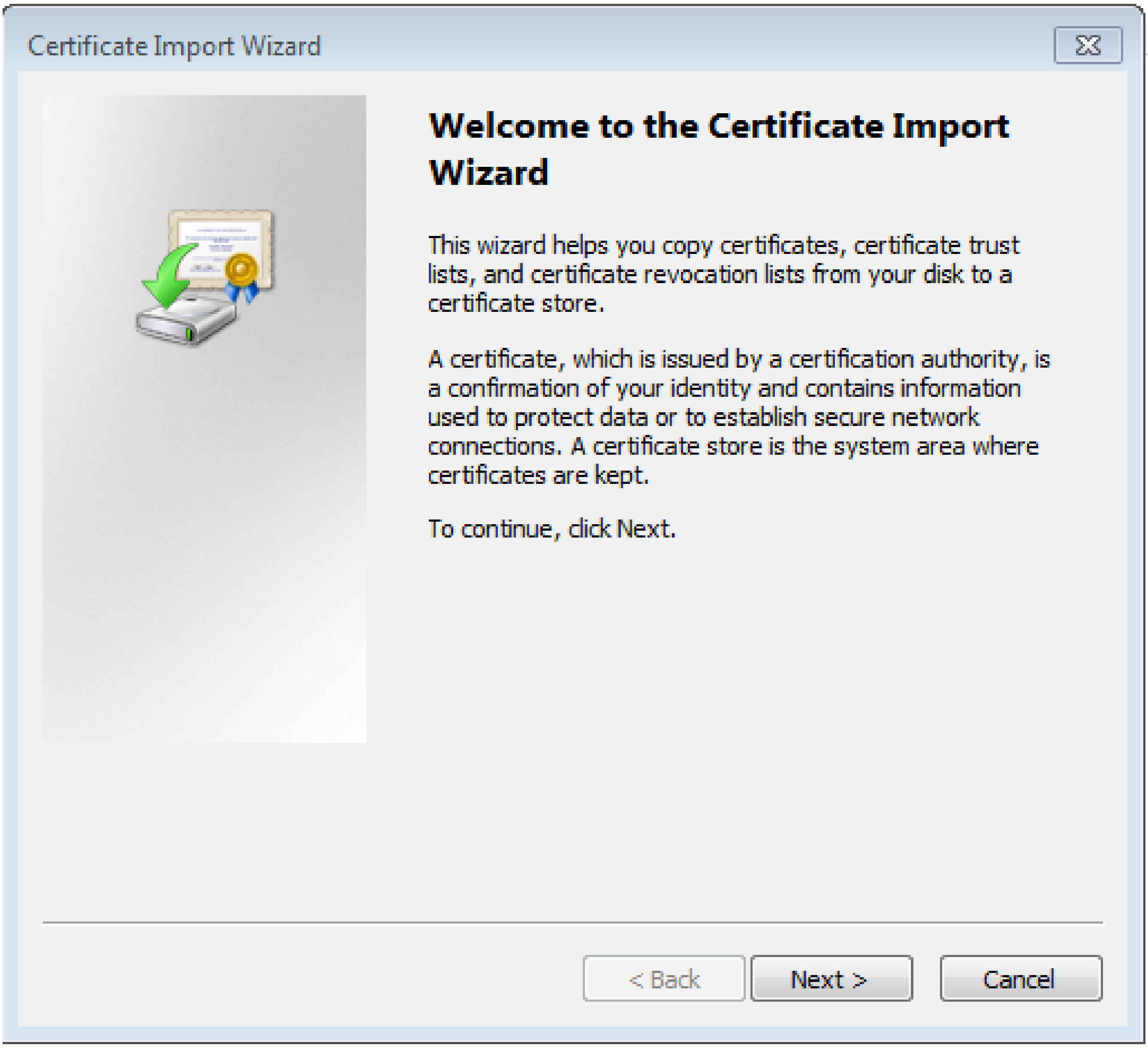
الخطوة 8. حدد OK.

الخطوة 9. انتقل إلى **الشهادات (الكمبيوتر المحلي)>الشهادات>الشخصية**، انقر بزر الماوس الأيمن فوق المجلد وانتقل إلى **جميع المهام>إستيراد**:



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na
DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<All>	<None>

Add a certificate to a store



Certificate Import Wizard

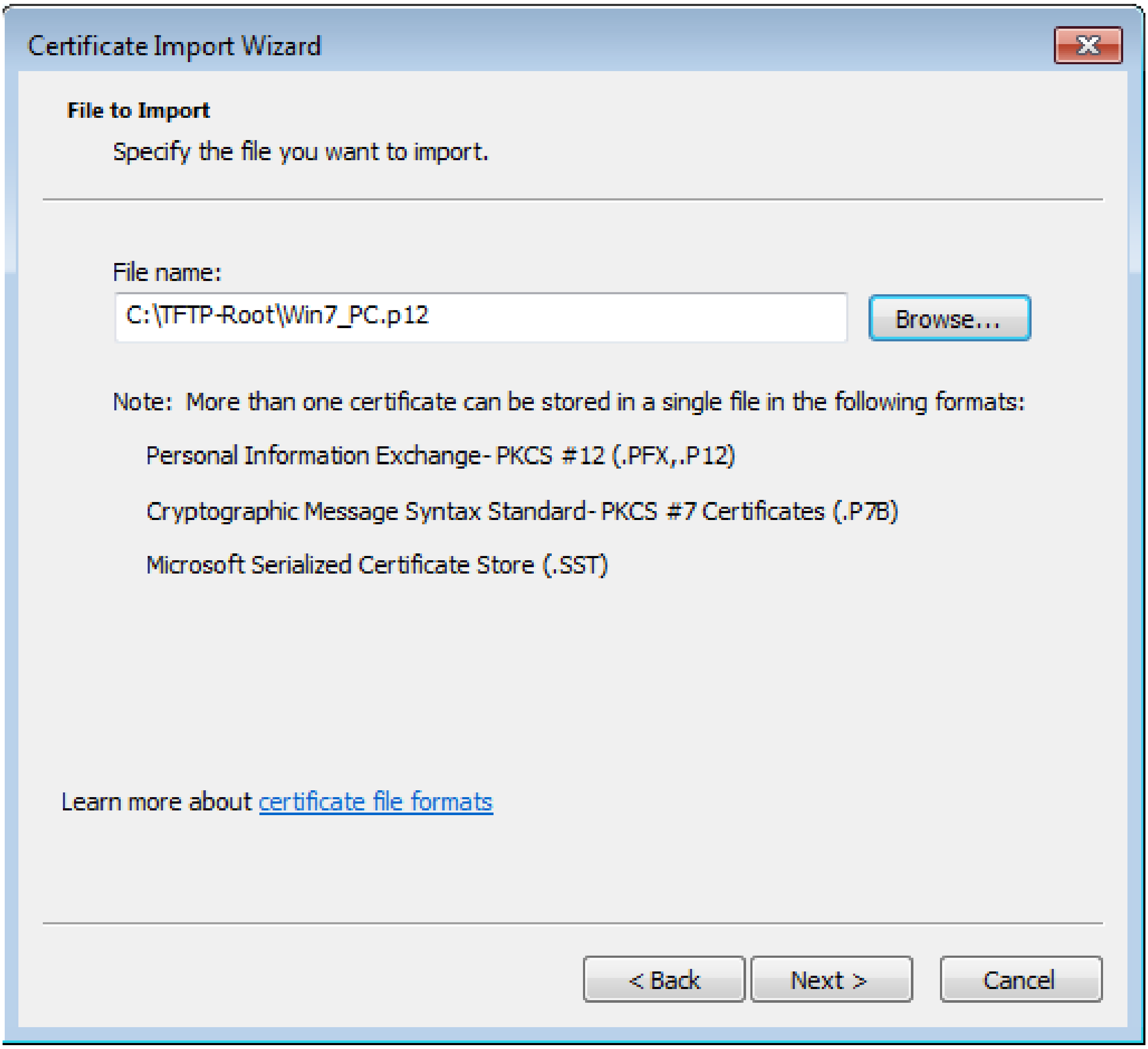
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

الخطوة 10. انقر فوق **Next (التالي)**. حدد المسار حيث يتم تخزين ملف PKCS12.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\TFTP-Root\Win7_PC.p12

Note: More than one certificate can be stored in a single file in the following formats:

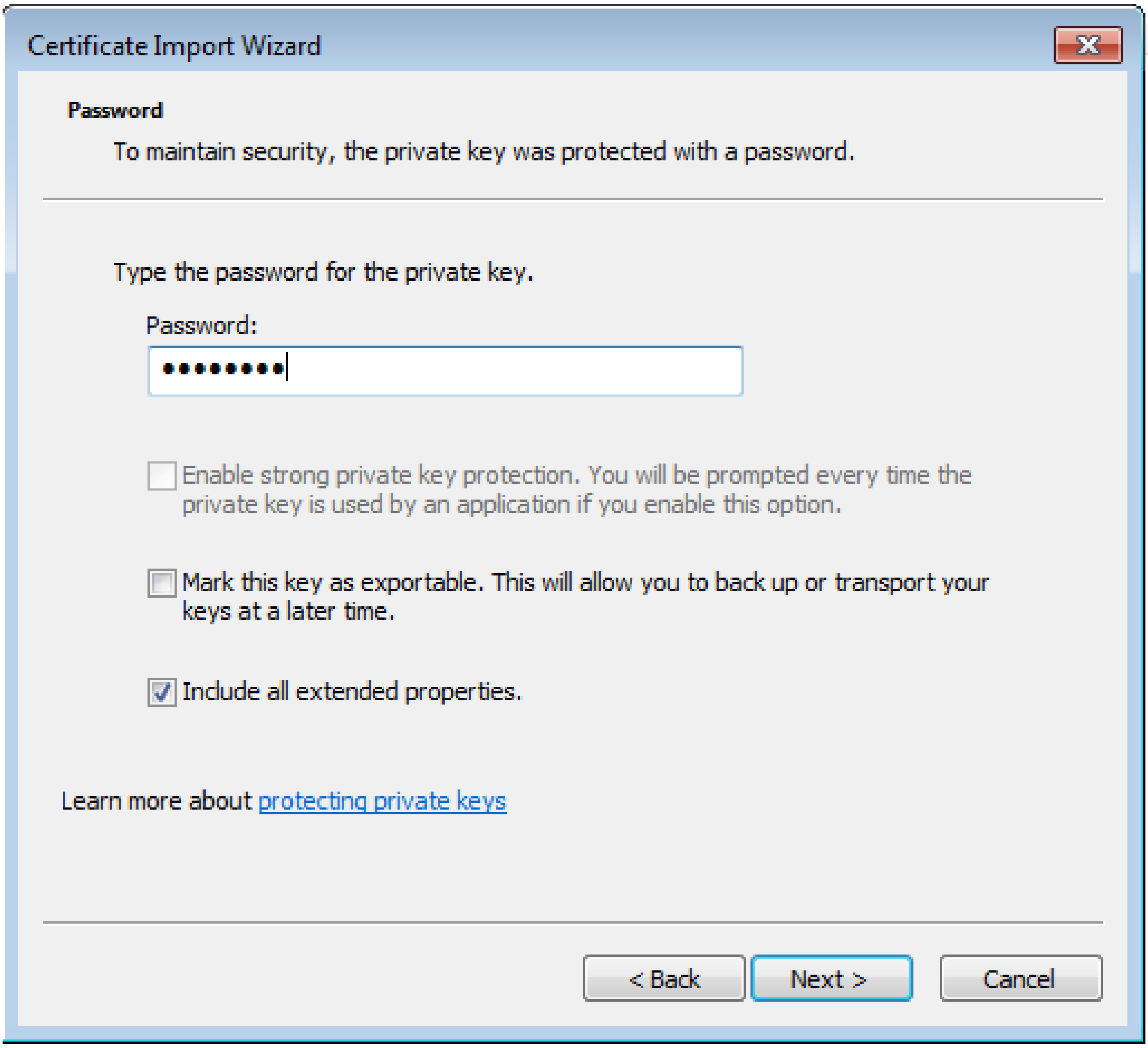
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

الخطوة 11. حدد **التالي** مرة أخرى واكتب كلمة المرور المدخلة في أمر *PKCS12> Win7_PC>*
tftp://10.152.206.175/ Win7_PC.p12>> كلمة المرور *<cisco123>*



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: ●●●●●●●●●

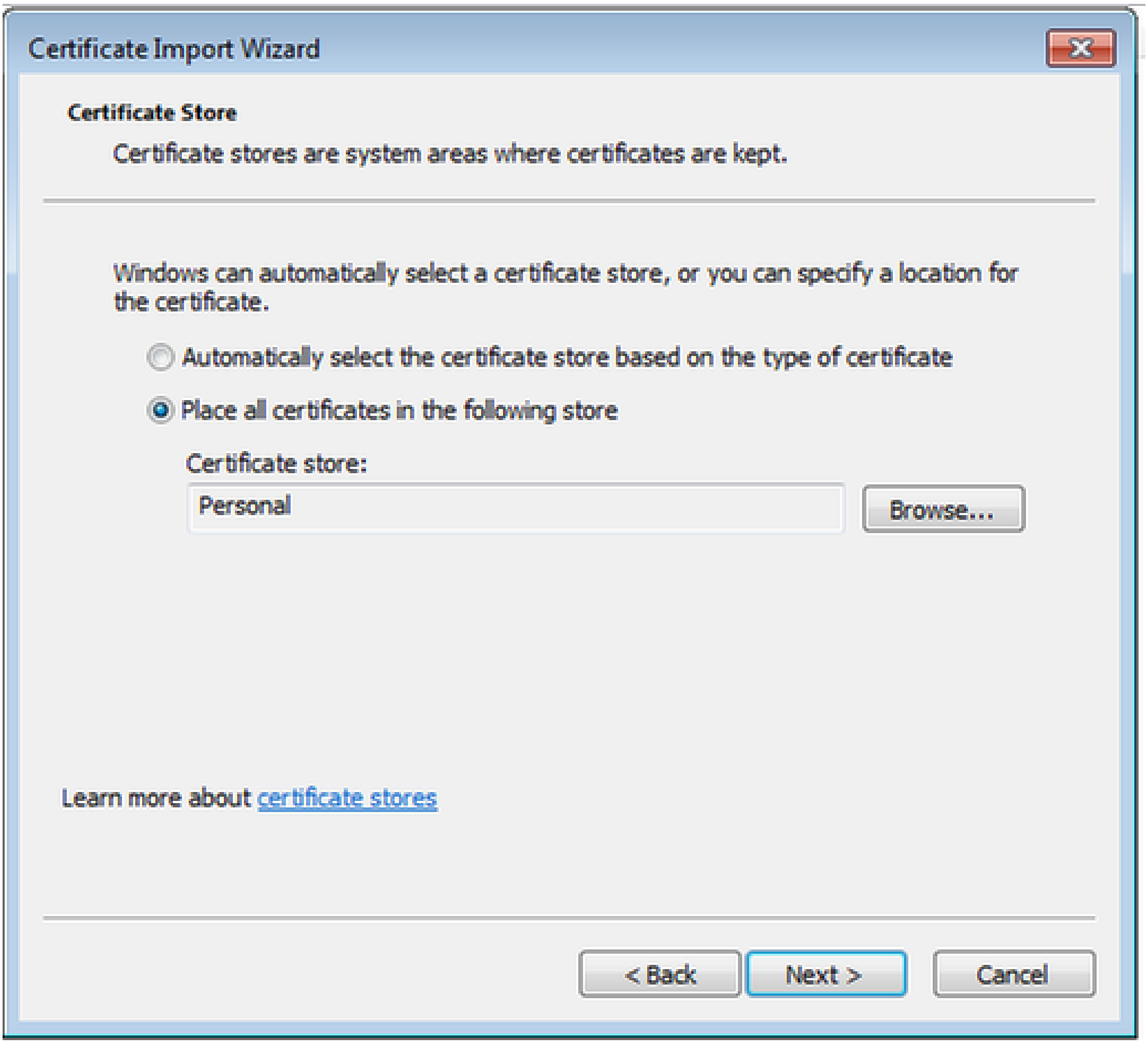
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

الخطوة 12. حدد **التالي**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

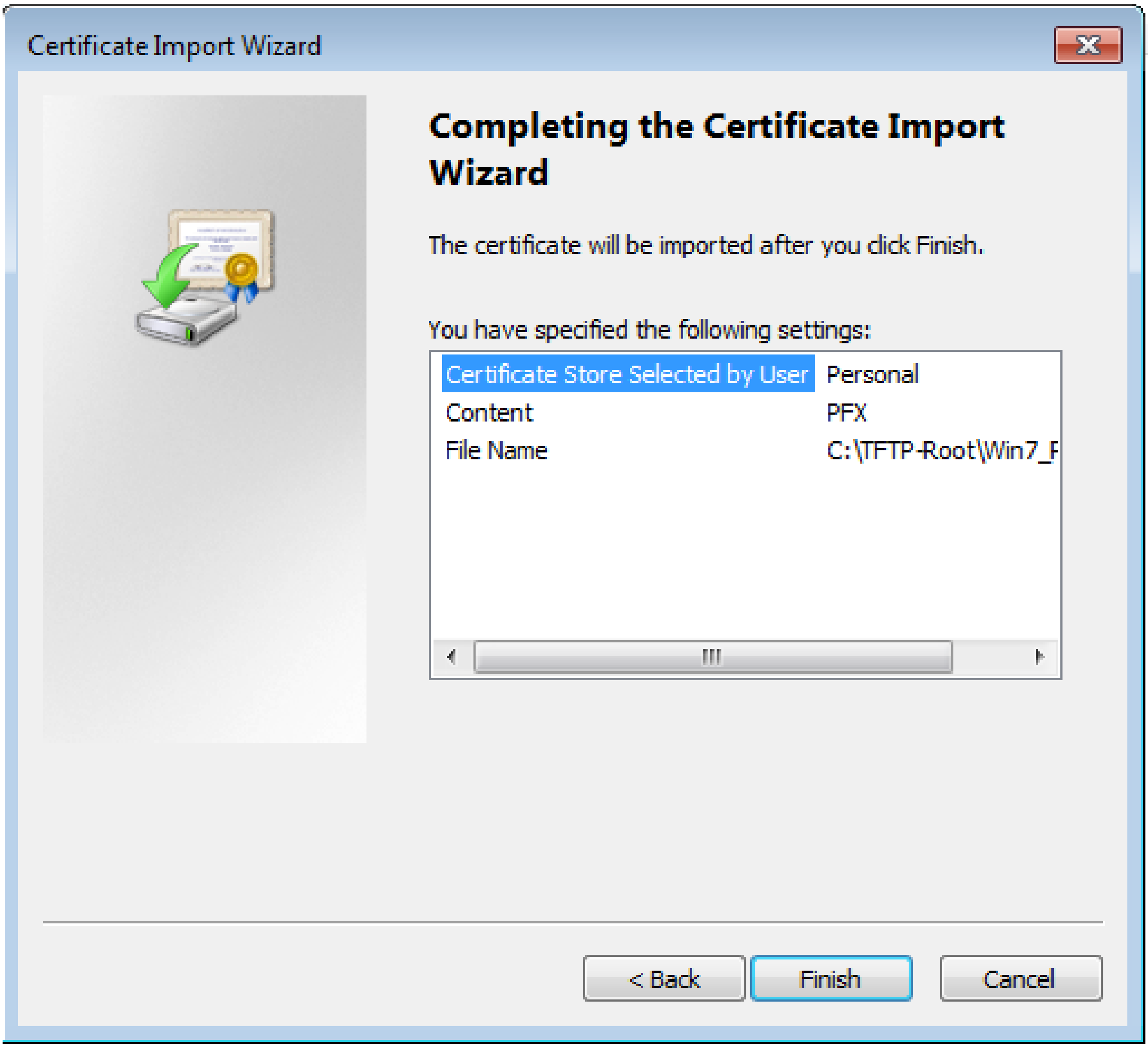
● Place all certificates in the following store

Certificate store:

Personal

Learn more about certificate stores

الخطوة 13. حدد المرة **التالية** مرة أخرى.



Certificate Import Wizard

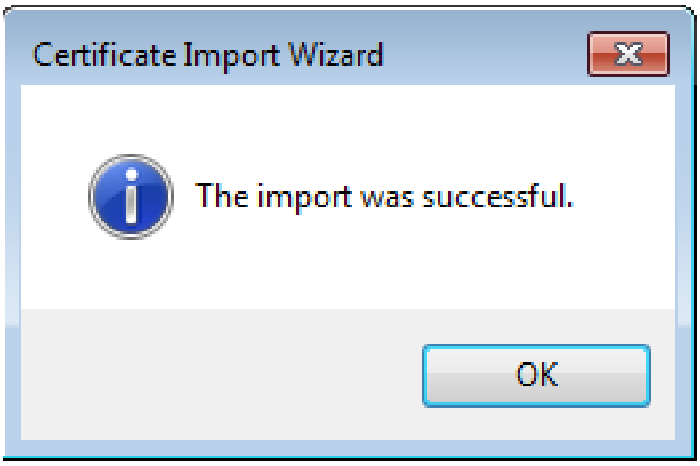
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\TFTP-Root\Win7_F

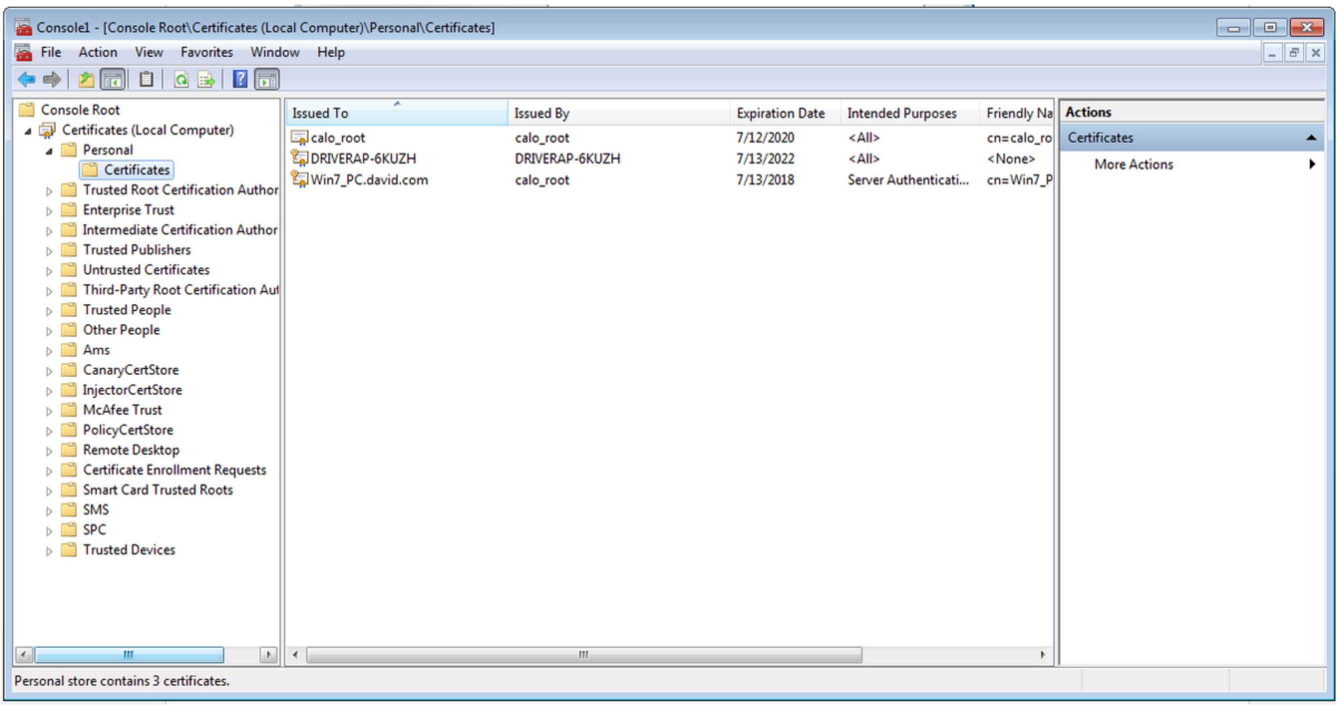
الخطوة 14. حدد **إنهاء**.



Certificate Import Wizard

The import was successful.

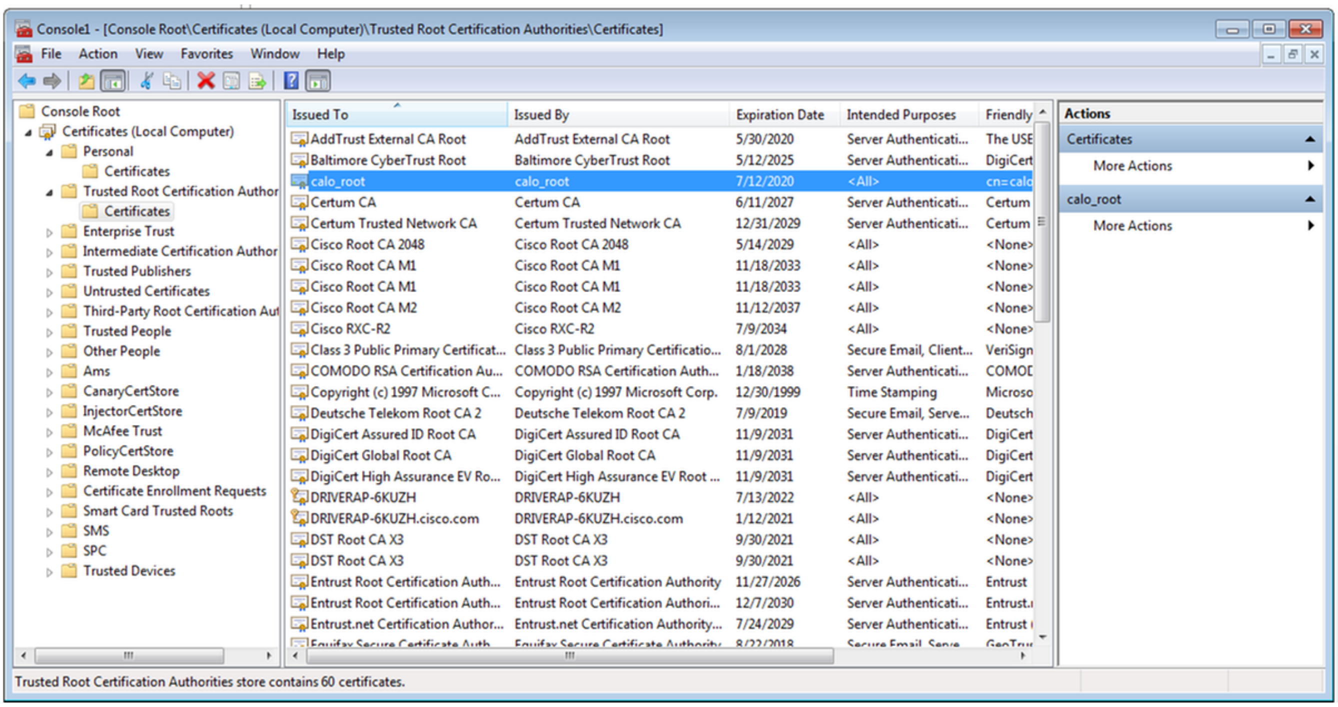
الخطوة 15. حدد **OK**. ستشاهد الآن الشهادات المثبتة (كل من شهادة CA وشهادة الهوية).



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na
calo_root	calo_root	7/12/2020	<All>	cn=calo_ro
DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<All>	<None>
Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati...	cn=Win7_P

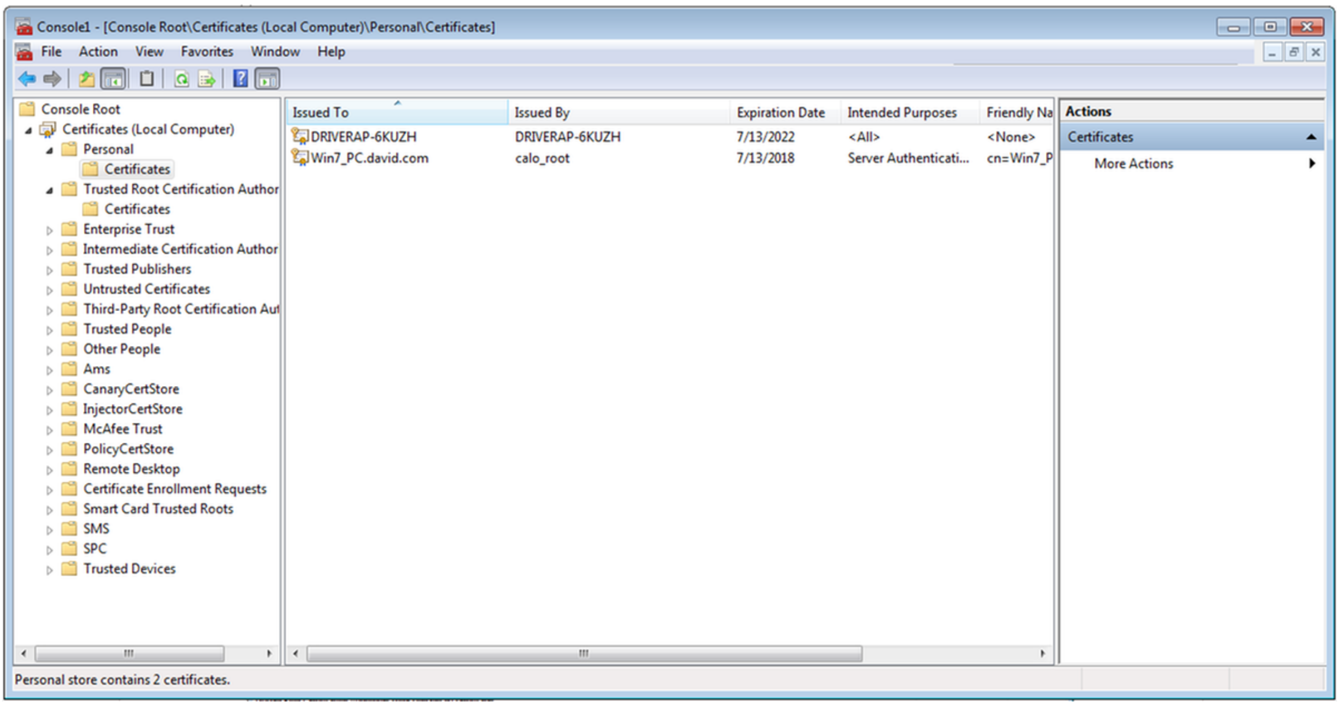
Personal store contains 3 certificates.

الخطوة 16. قم بسحب وإفلات شهادة المرجع المصدق من **الشهادات (الكمبيوتر المحلي)>الشهادات الشخصية** إلى **الشهادات (الكمبيوتر المحلي)>المرجع المصدق الجذر الموثوق فيه>الشهادات**.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	The USE
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert
calo_root	calo_root	7/12/2020	<All>	cn=calo
Certum CA	Certum CA	6/11/2027	Server Authenticati...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Certum
Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<All>	<None>
Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<All>	<None>
Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<All>	<None>
Cisco Root CA M2	Cisco Root CA M2	11/12/2037	<All>	<None>
Cisco RXC-R2	Cisco RXC-R2	7/9/2034	<All>	<None>
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038	Server Authenticati...	COMOD
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microso
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serve...	Deutsch
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert
DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<All>	<None>
DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com	1/12/2021	<All>	<None>
DST Root CA X3	DST Root CA X3	9/30/2021	<All>	<None>
DST Root CA X3	DST Root CA X3	9/30/2021	<All>	<None>
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Entrust.r
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTru

Trusted Root Certification Authorities store contains 60 certificates.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Author
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Author
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Aut
    - Trusted People
    - Other People
    - Ams
    - CanaryCertStore
    - InjectorCertStore
    - McAfee Trust
    - PolicyCertStore
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - SPC
    - Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na
DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<All>	<None>
Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati...	cn=Win7_P

Actions
Certificates
More Actions

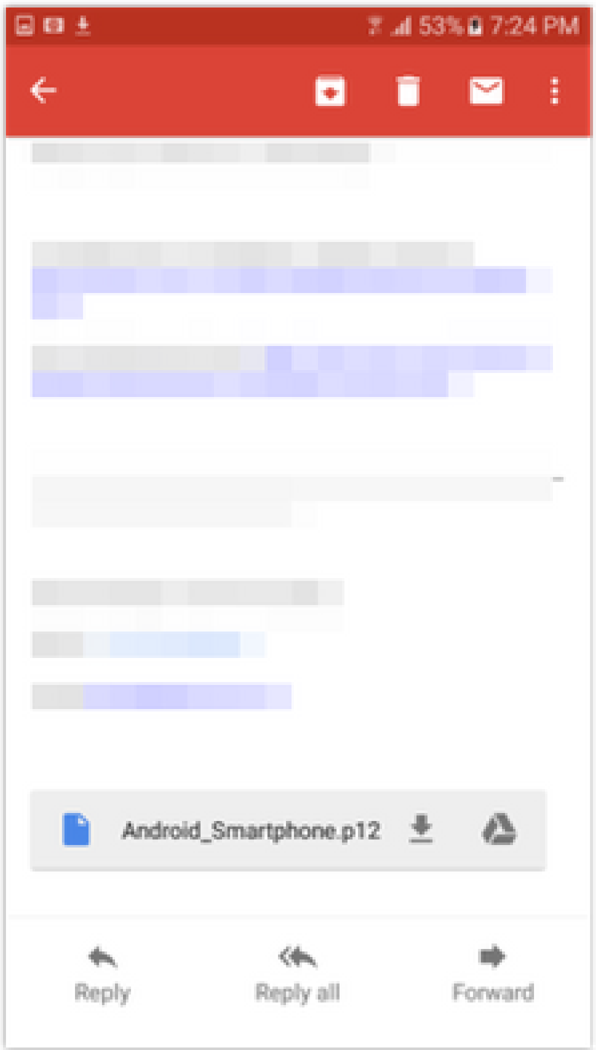
Personal store contains 2 certificates.

كيفية تثبيت "شهادة الهوية" على جهاز المحمول الذي يعمل بنظام التشغيل Android

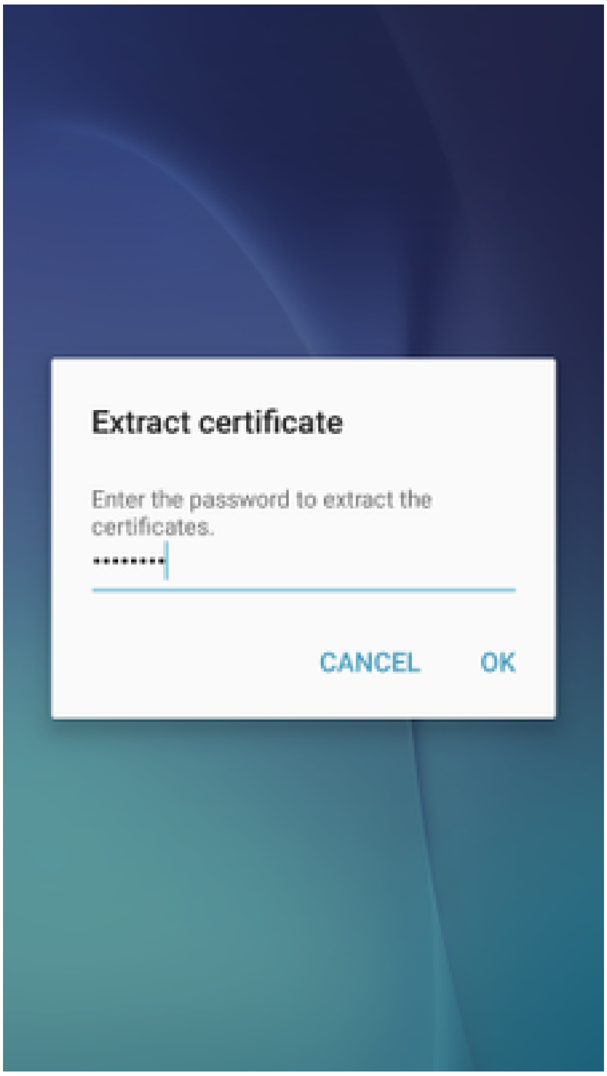
ملاحظة: يدعم Android ملفات مخزن مفاتيح PKCS#12 بامتداد .pfx أو .p12.

ملاحظة: يدعم Android شهادات X.509 SSL المرمزة من قبل DER فقط.

الخطوة 1. بعد تصدير شهادة العميل من خادم IOS CA بتنسيق PKCS12 (.p12)، قم بإرسال الملف إلى جهاز Android عبر البريد الإلكتروني. بمجرد وصوله إلى هناك، اضغط على اسم الملف لبدء التثبيت التلقائي. (**لا تقم بتنزيل الملف**)



الخطوة 2. دخلت الكلمة يستعمل أن يصدر الشهادة، في هذا مثال، الكلمة **cisco123**.

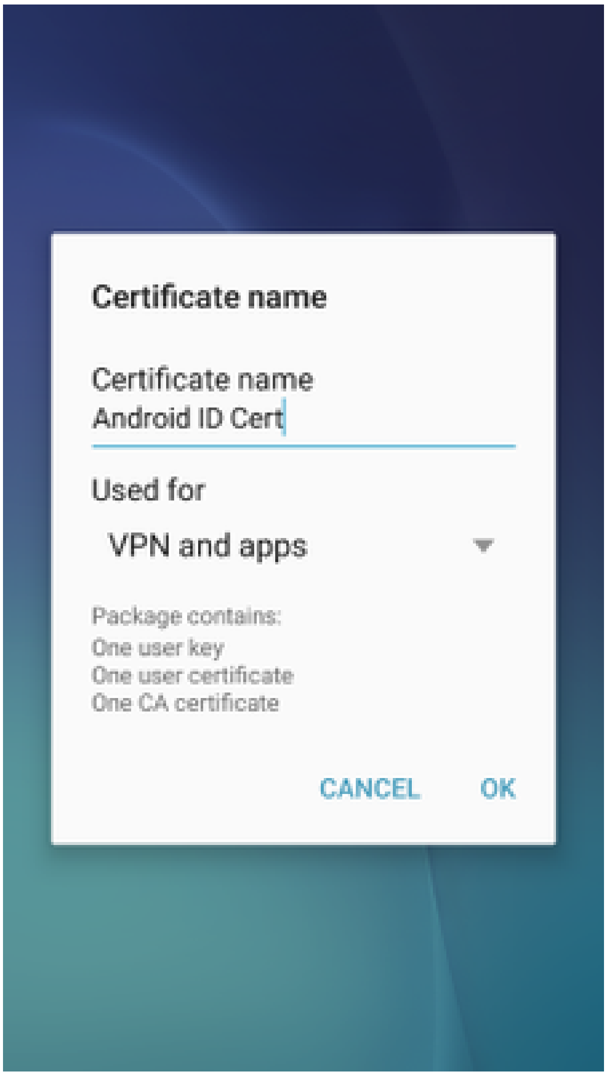


Extract certificate

Enter the password to extract the certificates.

•••••••••

الخطوة 3. حدد **موافق** وأدخل **اسم شهادة**. ممكن تكون أي كلمة في المثال ده الاسم شهادة **Android** .



Certificate name

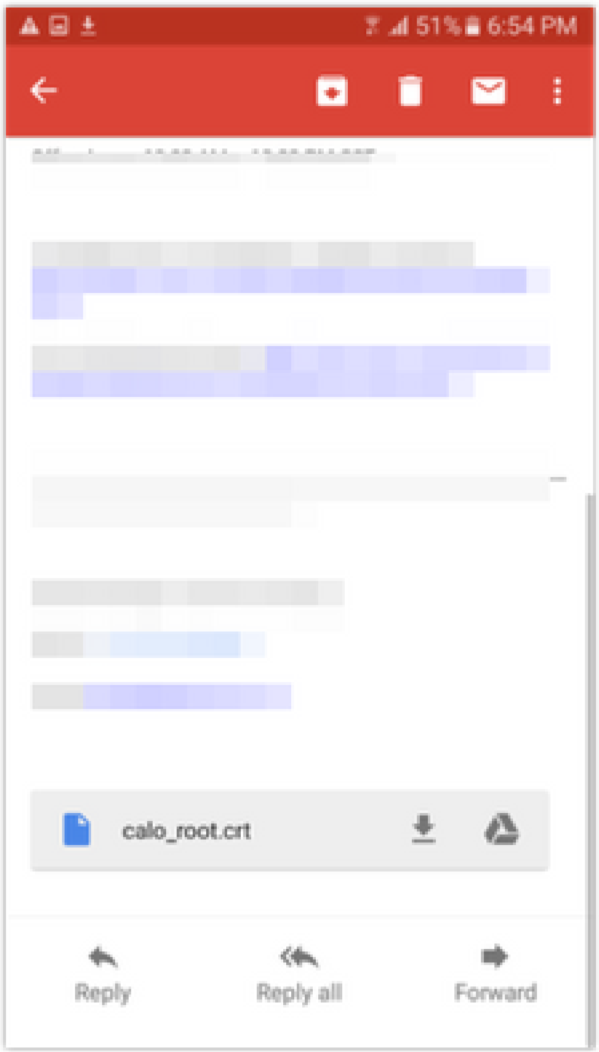
Certificate name
Android ID Cert

Used for
VPN and apps

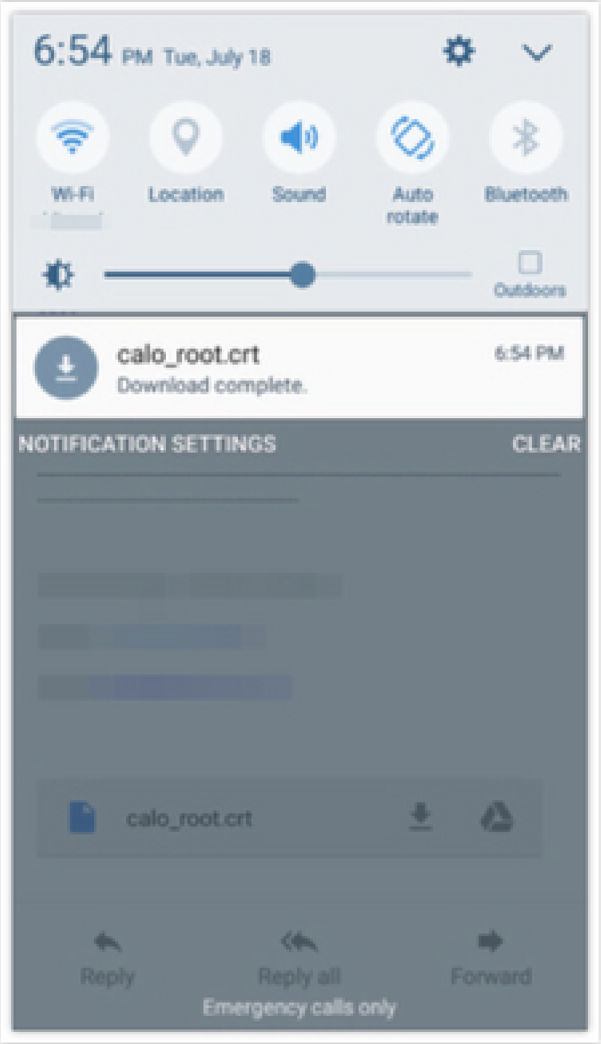
Package contains:
One user key
One user certificate
One CA certificate

الخطوة 4. حدد **OK** وتظهر الرسالة "Android Cert مثبت".

الخطوة 5. لتثبيت شهادة CA، استخرجها من خادم IOS CA بتنسيق base64 وحفظها بامتداد .crt. قم بإرسال الملف إلى جهاز Android الخاص بك عبر البريد الإلكتروني. هذه المرة تحتاج إلى تنزيل الملف عن طريق الضغط على السهم الموجود بجوار اسم الملف.



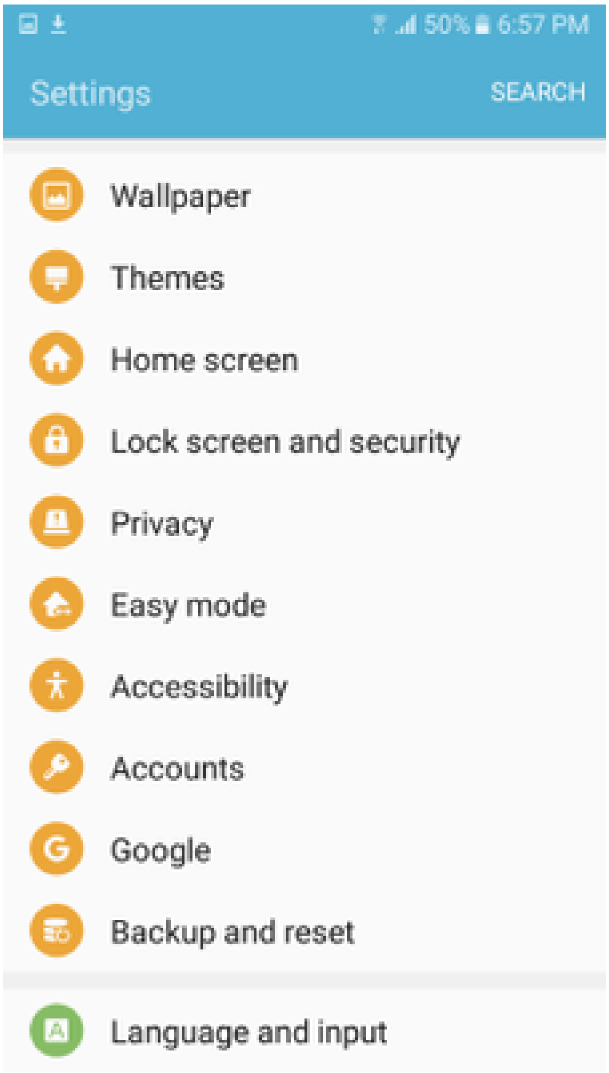
[redacted]



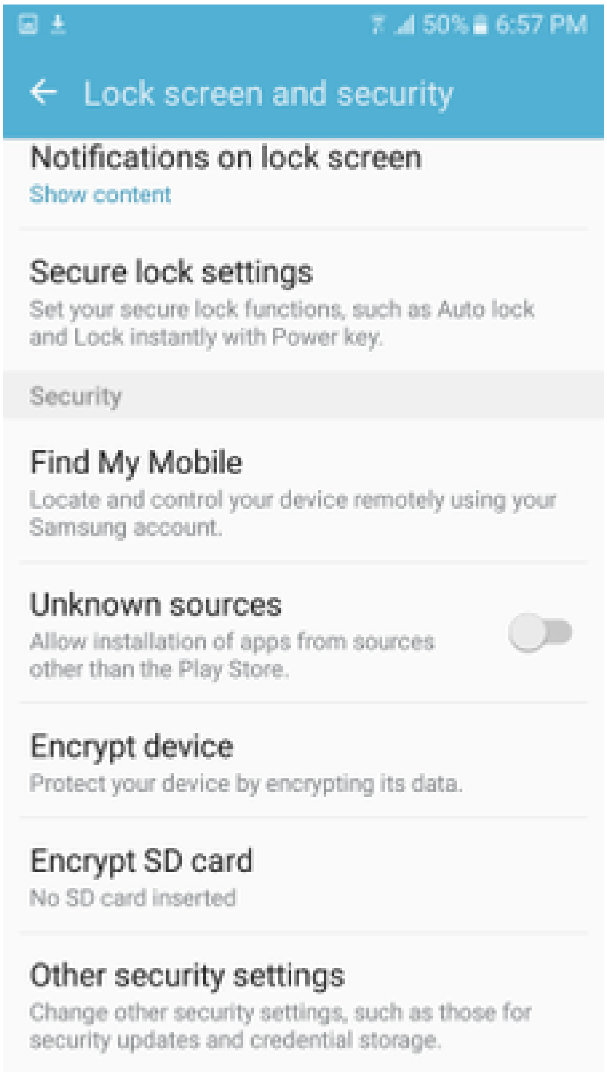
6:54 PM Tue, July 18

calo_root.crt 6:54 PM
Download complete.

الخطوة 6. انتقل إلى **الإعدادات** و**شاشة التأمين والأمان**.



الخطوة 7. حدد **إعدادات تأمين أخرى**.



6:57 PM 50%

Lock screen and security

Notifications on lock screen
Show content

Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.

Security

Find My Mobile
Locate and control your device remotely using your Samsung account.

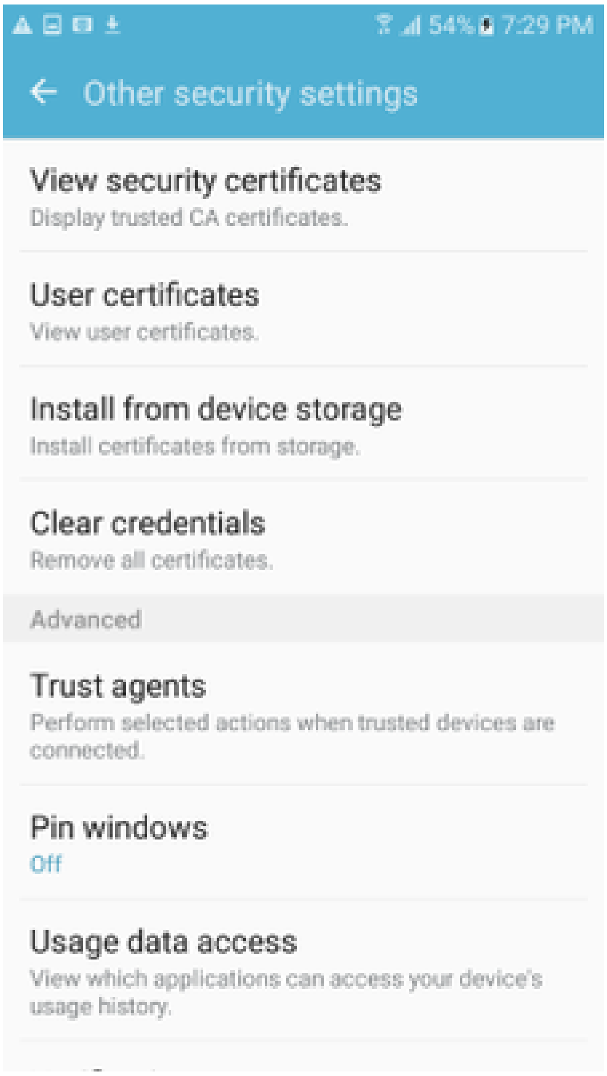
Unknown sources
Allow installation of apps from sources other than the Play Store.

Encrypt device
Protect your device by encrypting its data.

Encrypt SD card
No SD card inserted

Other security settings
Change other security settings, such as those for security updates and credential storage.

الخطوة 8. انتقل إلى **التثبيت من تخزين الجهاز**.



54% 7:29 PM

Other security settings

View security certificates
Display trusted CA certificates.

User certificates
View user certificates.

Install from device storage
Install certificates from storage.

Clear credentials
Remove all certificates.

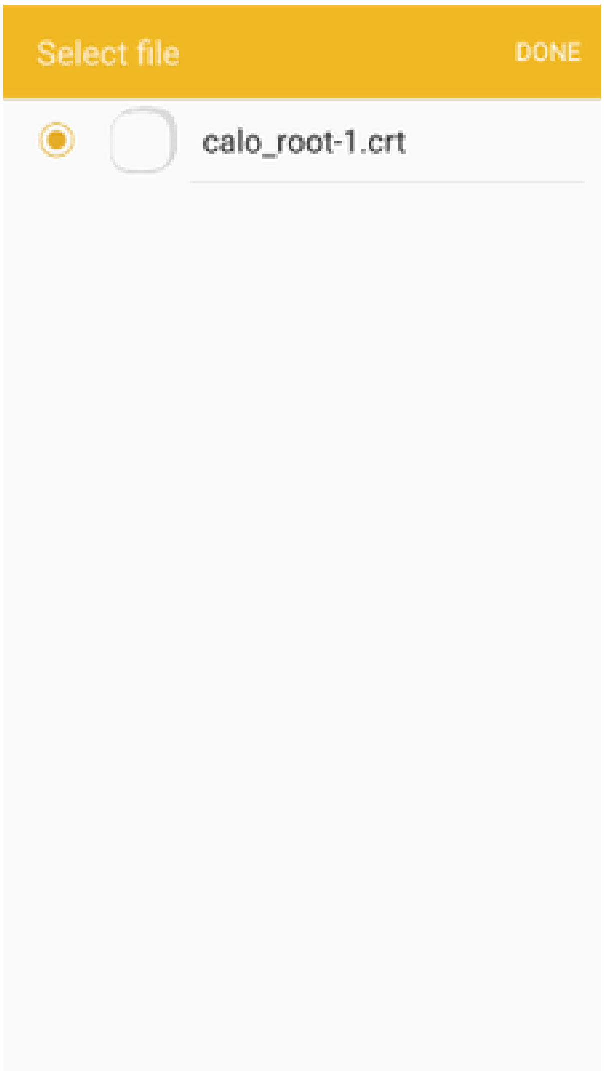
Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows
Off

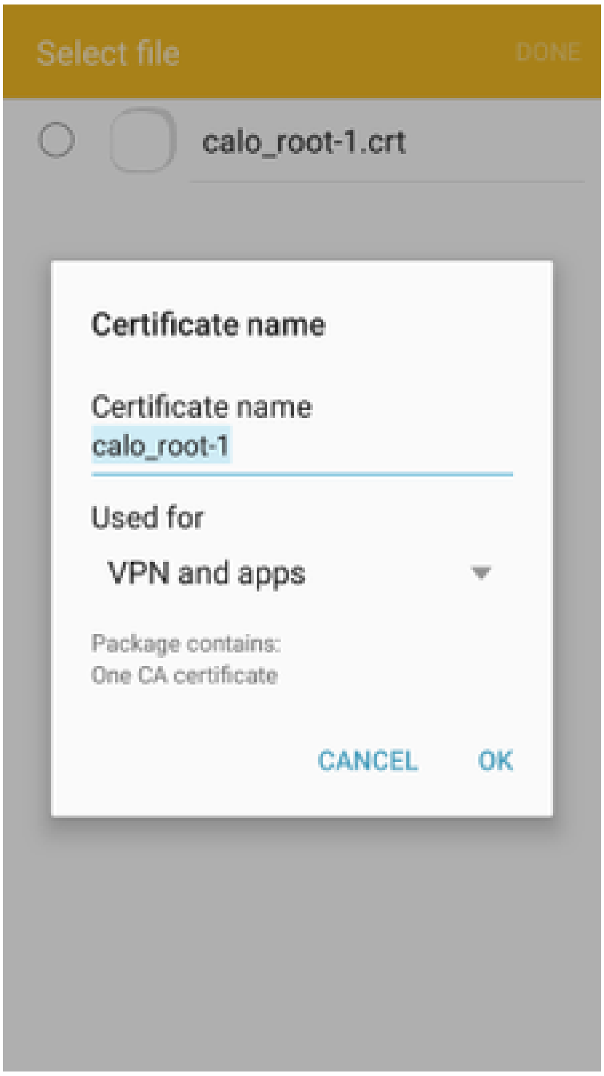
Usage data access
View which applications can access your device's usage history.

الخطوة 9. حدد ملف crt. واضغط على **تم**.



● calo_root-1.crt

الخطوة 10. أدخل **اسم شهادة**. من الممكن أن تكون أي كلمة، في هذا المثال، الاسم هو **calo_root-1**.



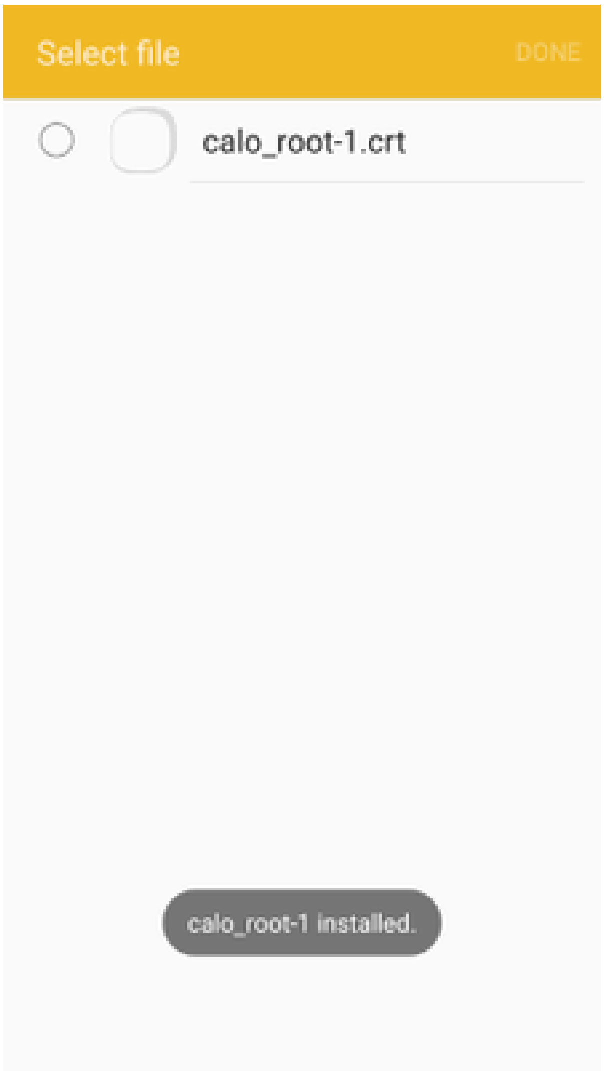
Certificate name

Certificate name
calo_root-1

Used for
VPN and apps

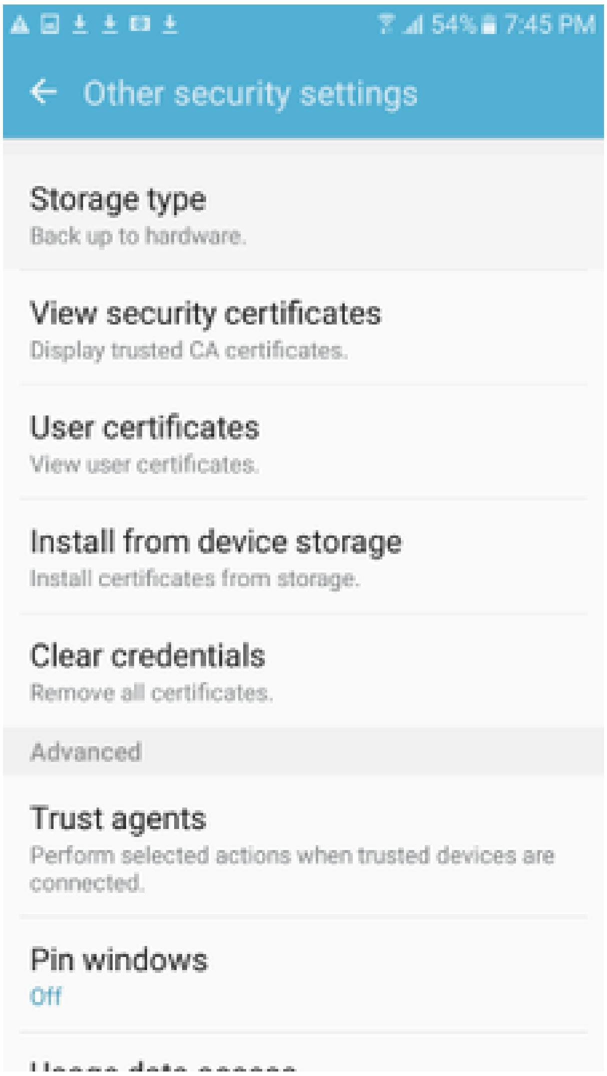
Package contains:
One CA certificate

الخطوة 10. حدد **موافق** وسترى الرسالة "calo_root-1 مثبتة".



calo_root-1 installed.

الخطوة 11. للتحقق من تثبيت شهادة الهوية، انتقل إلى **شاشة الإعدادات/التأمين التأمين/غير ذلك > إعدادات التأمين/شهادات المستخدم/علامة تبويب النظام.**



Other security settings

Storage type
Back up to hardware.

View security certificates
Display trusted CA certificates.

User certificates
View user certificates.

Install from device storage
Install certificates from storage.

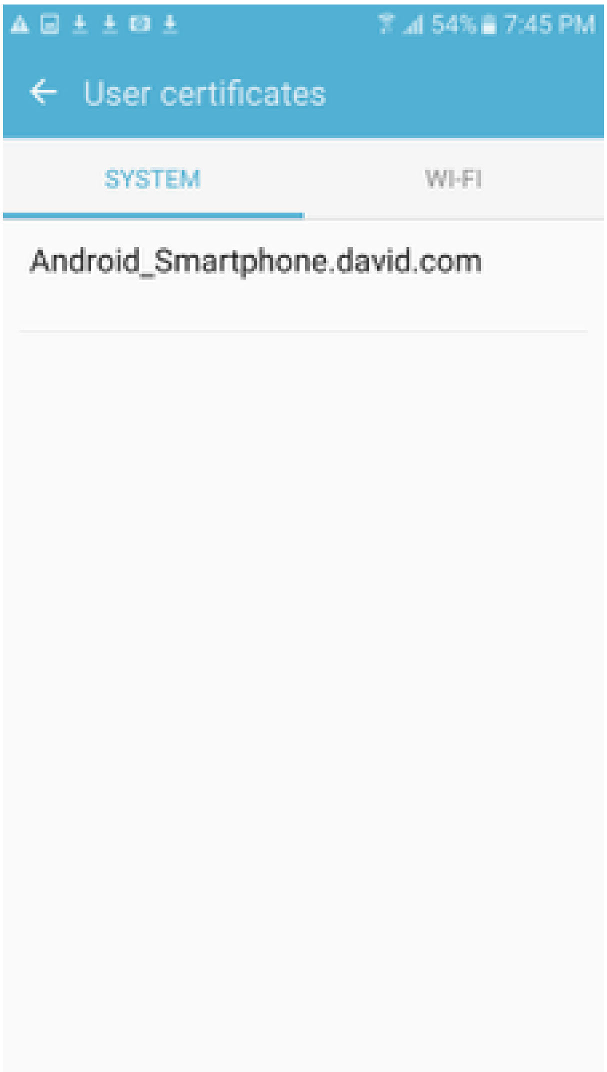
Clear credentials
Remove all certificates.

Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows
Off

Usage data access

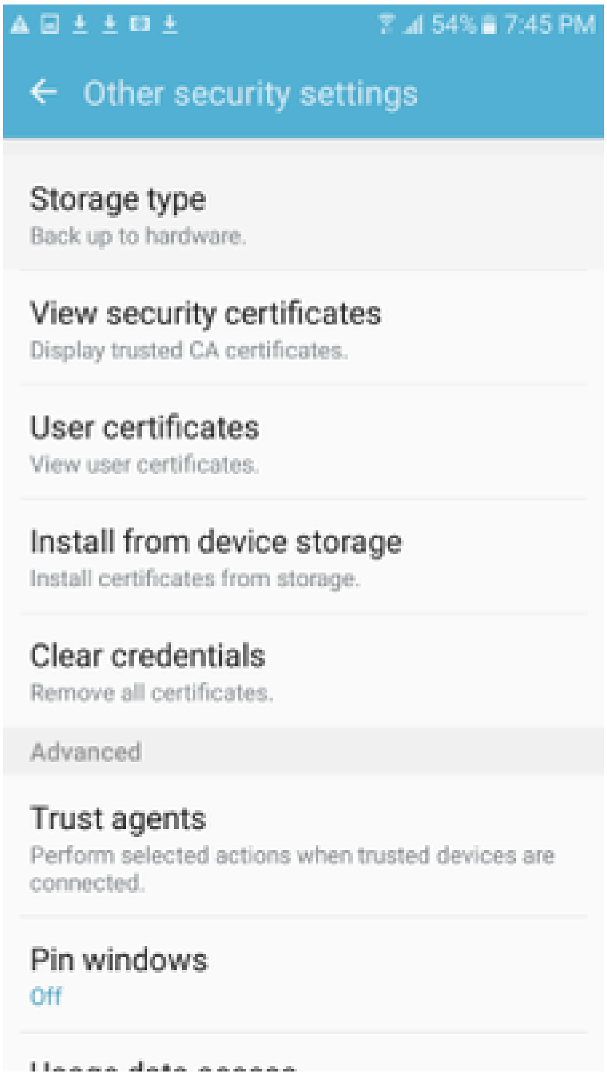


54% 7:45 PM

User certificates

Android_Smartphone.david.com

الخطوة 12. للتحقق من تثبيت شهادة CA، انتقل إلى **شاشة الإعدادات/التأمين/التأمين وإعدادات التأمين/غيرها/عرض شهادات التأمين/علامة تبويب المستخدم**.



7:45 PM 54%

Other security settings

Storage type
Back up to hardware.

View security certificates
Display trusted CA certificates.

User certificates
View user certificates.

Install from device storage
Install certificates from storage.

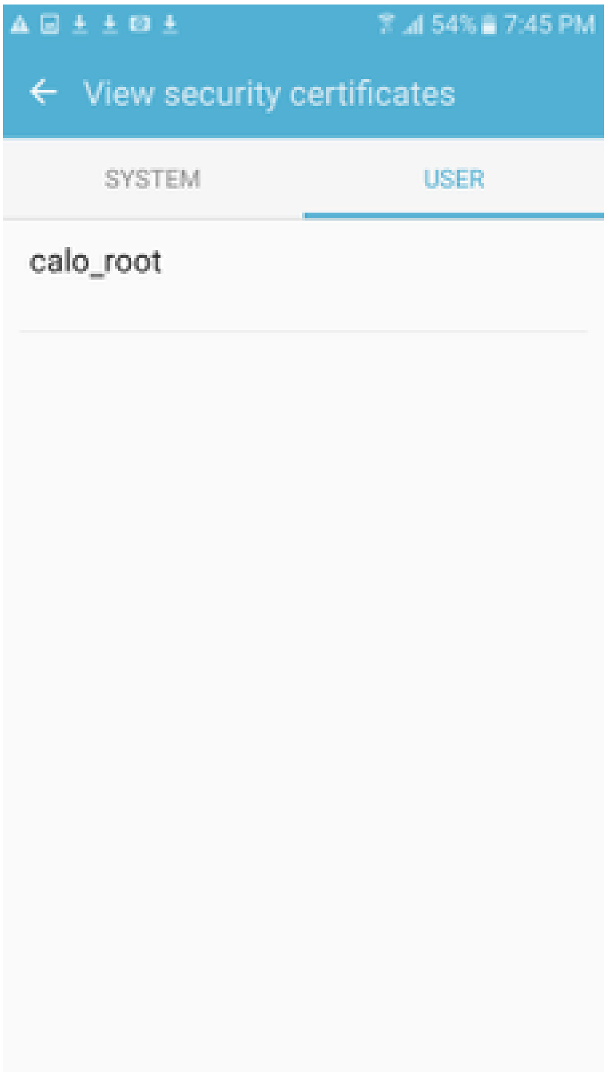
Clear credentials
Remove all certificates.

Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows
Off

Usage data access



calo_root

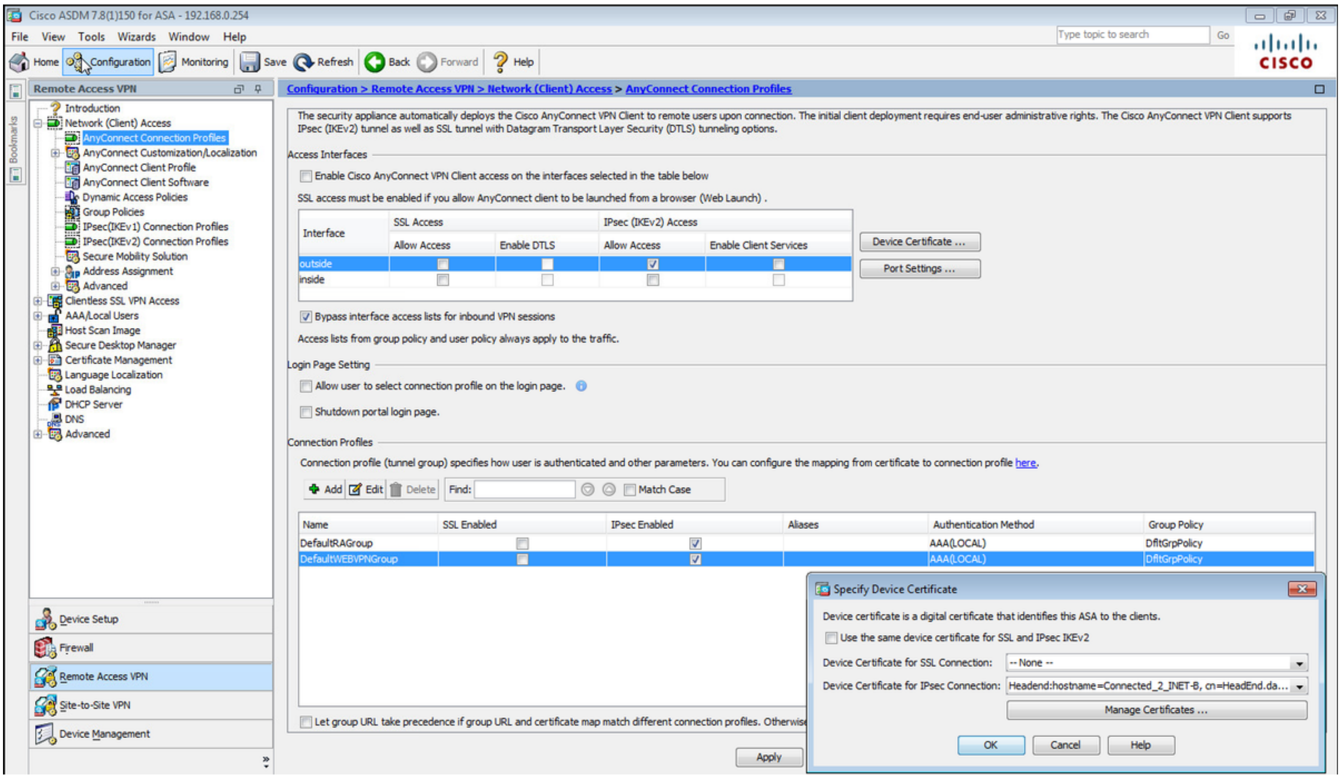
تكوين وحدة الاستقبال والبث ل ASA ل RA VPN باستخدام IKEv2

الخطوة 1. في ASDM، انتقل إلى **Configuration>Remote Access VPN (الوصول إلى الشبكة) (العميل)> ملفات تعريف اتصال AnyConnect**. حدد مربع **السماح بالوصول (IPSec (IKEv2** على الواجهة التي تواجه عملاء VPN (خيار **تمكين خدمات العملاء** غير ضروري).

الخطوة 2. حدد **شهادة الجهاز** وازل علامة التجزئة من **إستخدام نفس شهادة الجهاز ل SSL و IPSec IKEv2**.

الخطوة 3. حدد شهادة وحدة الاستقبال والبث لاتصال IPSec وحدد — بدون — لاتصال SSL.

يعمل هذا الخيار على وضع تكوين خريطة التشفير ikev2، crypto ipSec و crypto dynamic-map والتشفير.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

□ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	□	□	☑	□
inside	□	□	□	□

Device Certificate ... Port Settings ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

□ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: □ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise

Apply

Specify Device Certificate

Device certificate is a digital certificate that identifies this ASA to the clients.

□ Use the same device certificate for SSL and IPsec IKEv2

Device Certificate for SSL Connection: -- None --

Device Certificate for IPsec Connection: Headend:hostname=Connected_2_INET-B, cn=HeadEnd.da...

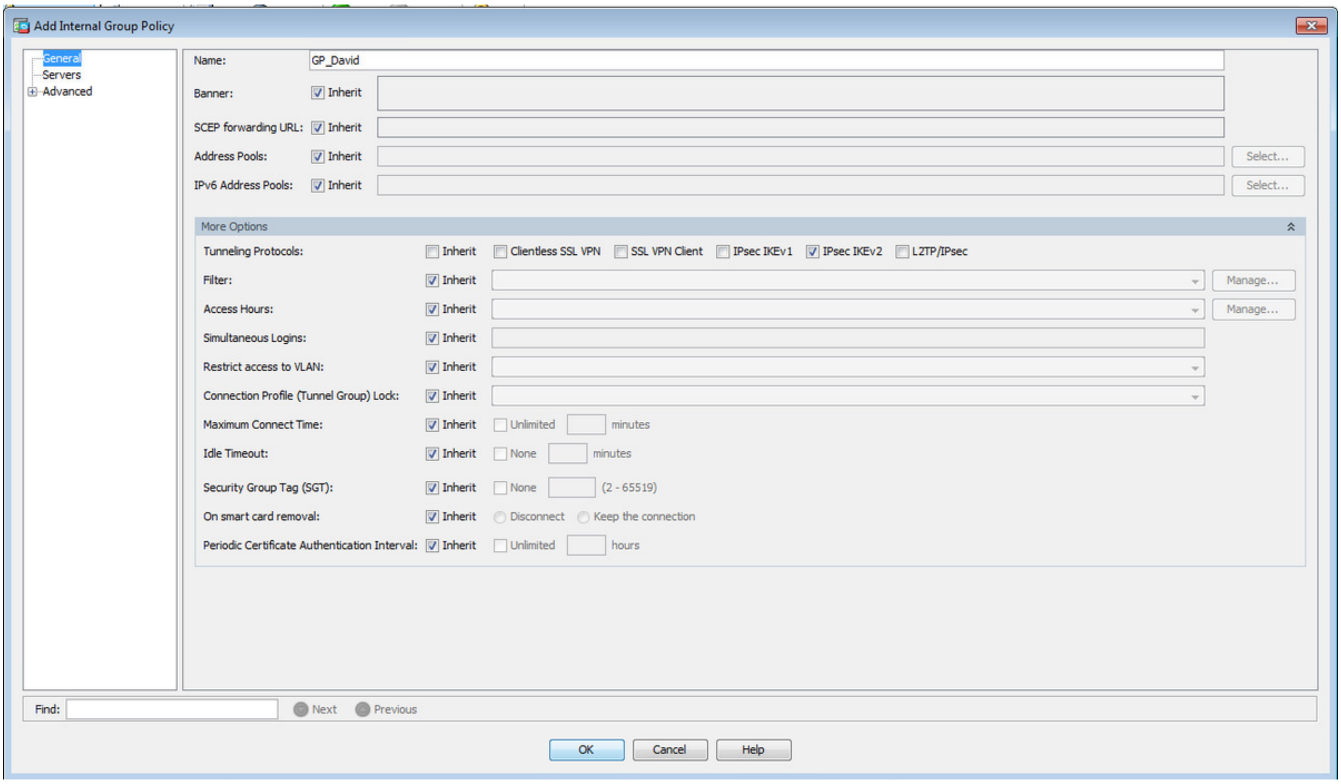
Manage Certificates ...

OK Cancel Help

هذه هي الطريقة التي يبدو بها التكوين على واجهة سطر الأوامر (CLI).

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

crypto ikev2 remote-access trustpoint HeadEnd
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5

crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256
crypto map outside_map 65535 ipsec-isakmp dynamic Anyconnect
crypto map outside_map interface outside
```

الخطوة 4. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Network (العملاء) > Access Group Policies لإنشاء نهج مجموعة



Add Internal Group Policy

Name:		GP_David
Banner:	☑ Inherit	
SCEP forwarding URL:	☑ Inherit	
Address Pools:	☑ Inherit	Select...
IPv6 Address Pools:	☑ Inherit	Select...

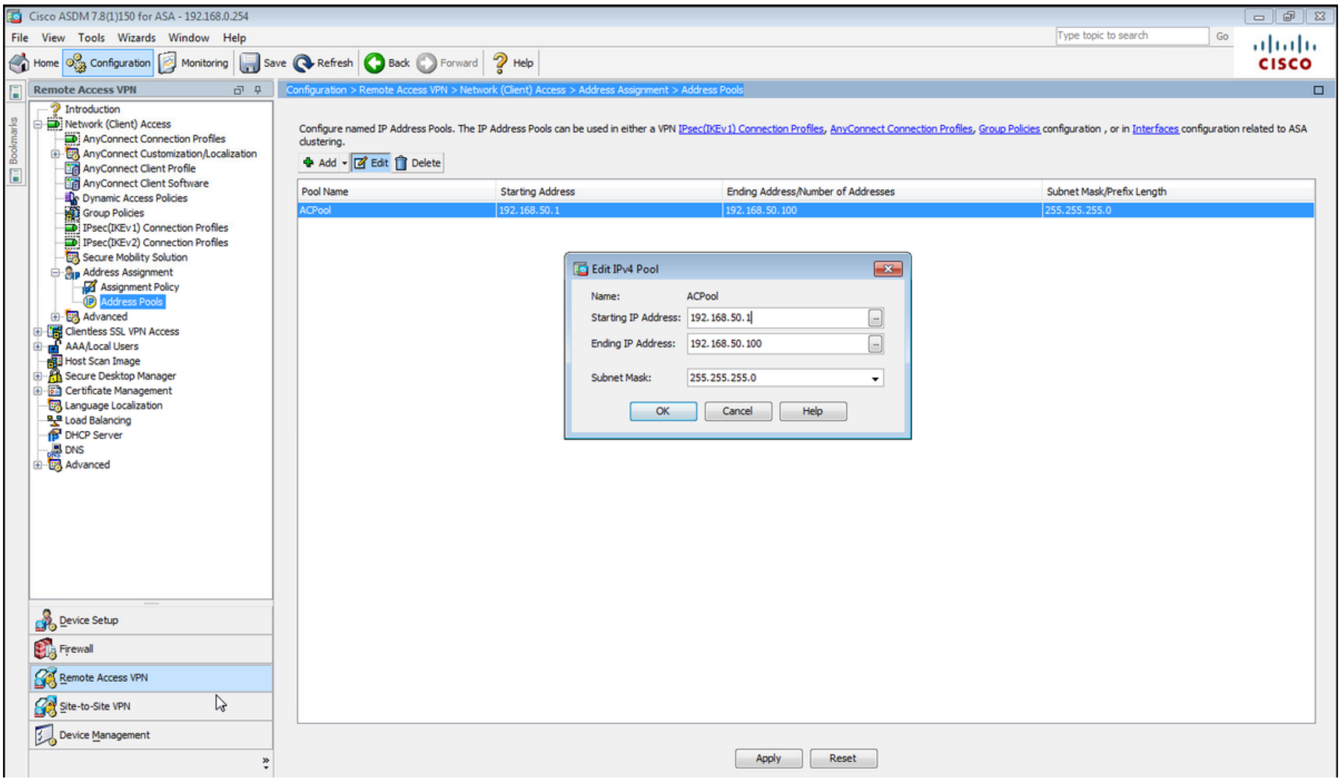
More Options

Tunneling Protocols:	□ Inherit	□ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 ☑ IPsec IKEv2 □ L2TP/IPsec
Filter:	☑ Inherit	Manage...
Access Hours:	☑ Inherit	Manage...
Simultaneous Logins:	☑ Inherit	
Restrict access to VLAN:	☑ Inherit	
Connection Profile (Tunnel Group) Lock:	☑ Inherit	
Maximum Connect Time:	☑ Inherit	□ Unlimited minutes
Idle Timeout:	☑ Inherit	□ None minutes
Security Group Tag (SGT):	☑ Inherit	□ None (2 - 65519)
On smart card removal:	☑ Inherit	○ Disconnect ○ Keep the connection
Periodic Certificate Authentication Interval:	☑ Inherit	□ Unlimited hours

واجهة سطر الأوامر (CLI).

```
group-policy GP_David internal
group-policy GP_David attributes
 vpn-tunnel-protocol ikev2
```

الخطوة 5. انتقل إلى **التكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > تجمعات العناوين** وحدد **Add** لإنشاء تجمع IPv4.



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools

Configure named IP Address Pools. The IP Address Pools can be used in either a VPN IPsec(IKEv1) Connection Profiles, AnyConnect Connection Profiles, Group Policies configuration , or in Interfaces configuration related to ASA clustering.

Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
ACPool	192.168.50.1	192.168.50.100	255.255.255.0

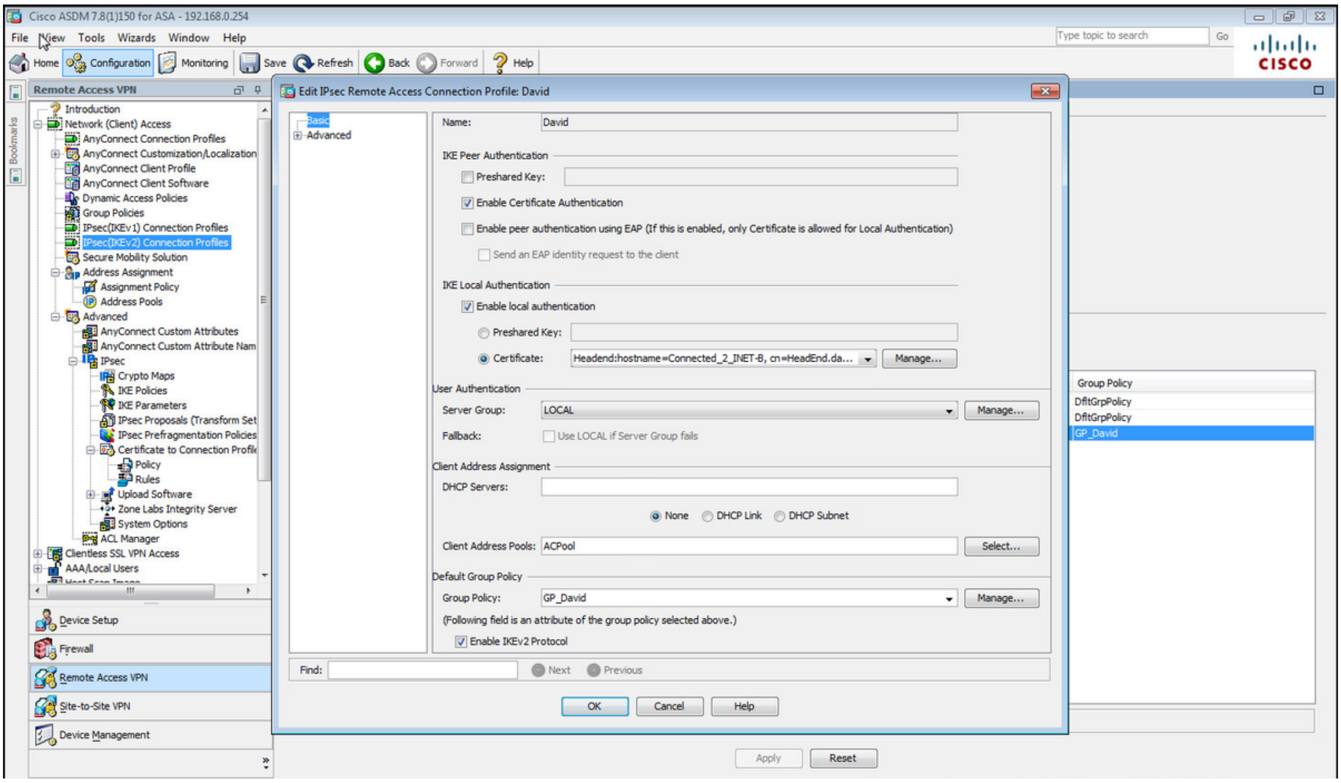
Edit IPv4 Pool

Name:	ACPool
Starting IP Address:	192.168.50.1
Ending IP Address:	192.168.50.100
Subnet Mask:	255.255.255.0

واجهة سطر الأوامر (CLI).

```
ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0
```

الخطوة 6. انتقل إلى **التكوين > Remote Access VPN (الوصول عن بعد) > Network (Client) Access > ملفات تعريف اتصال IPSec(IKEv2)** وحدد **Add** لإنشاء مجموعة أنفاق جديدة.



Edit IPsec Remote Access Connection Profile: David

Name: David

IKE Peer Authentication

☐ Preshared Key:

☑ Enable Certificate Authentication

☐ Enable peer authentication using EAP (If this is enabled, only Certificate is allowed for Local Authentication)

☐ Send an EAP identity request to the client

IKE Local Authentication

☑ Enable local authentication

○ Preshared Key:

● Certificate: Headend:hostname=Connected_2_INET-B, cn=HeadEnd.da...

User Authentication

Server Group: LOCAL

Fallback: ☐ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: ACPool

Default Group Policy

Group Policy: GP_David

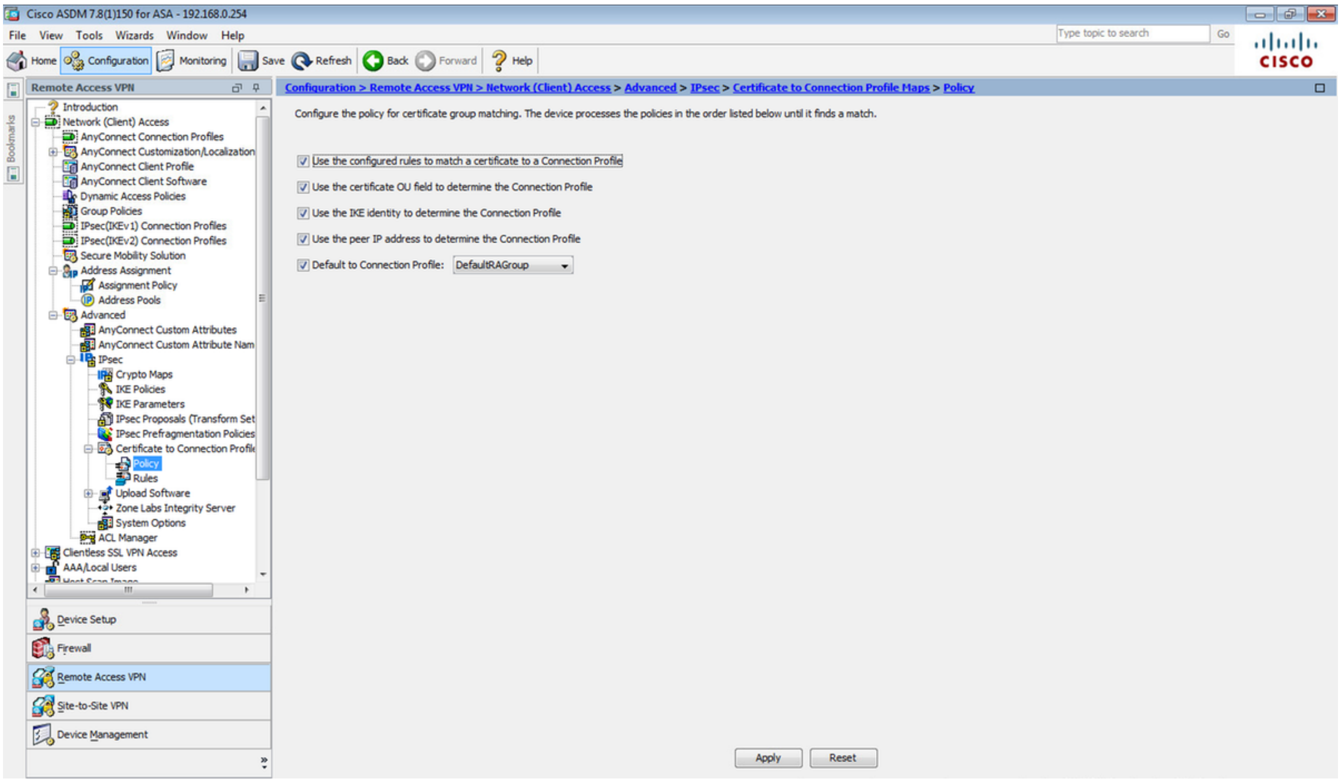
(Following field is an attribute of the group policy selected above.)

☑ Enable IKEv2 Protocol

واجهة سطر الأوامر (CLI).

```
tunnel-group David type remote-access
tunnel-group David general-attributes
 address-pool ACPool
 default-group-policy GP_David
 authentication-server-group LOCAL
tunnel-group David webvpn-attributes
 authentication certificate
tunnel-group David ipsec-attributes
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate HeadEnd
```

الخطوة 7. انتقل إلى **التكوين > Remote Access VPN (التكوين) > Network (العميل) > Advanced > Access Certificate to Connection Profile Maps > IPsec (شهادة إلى الاتصال) > Policy** وحدد **القواعد المستخدمة المستخدمة لحساب الشهادة إلى** مربع **ملف تعريف الاتصال**.



Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Policy

Configure the policy for certificate group matching. The device processes the policies in the order listed below until it finds a match.

☑ Use the configured rules to match a certificate to a Connection Profile

☑ Use the certificate OU field to determine the Connection Profile

☑ Use the IKE identity to determine the Connection Profile

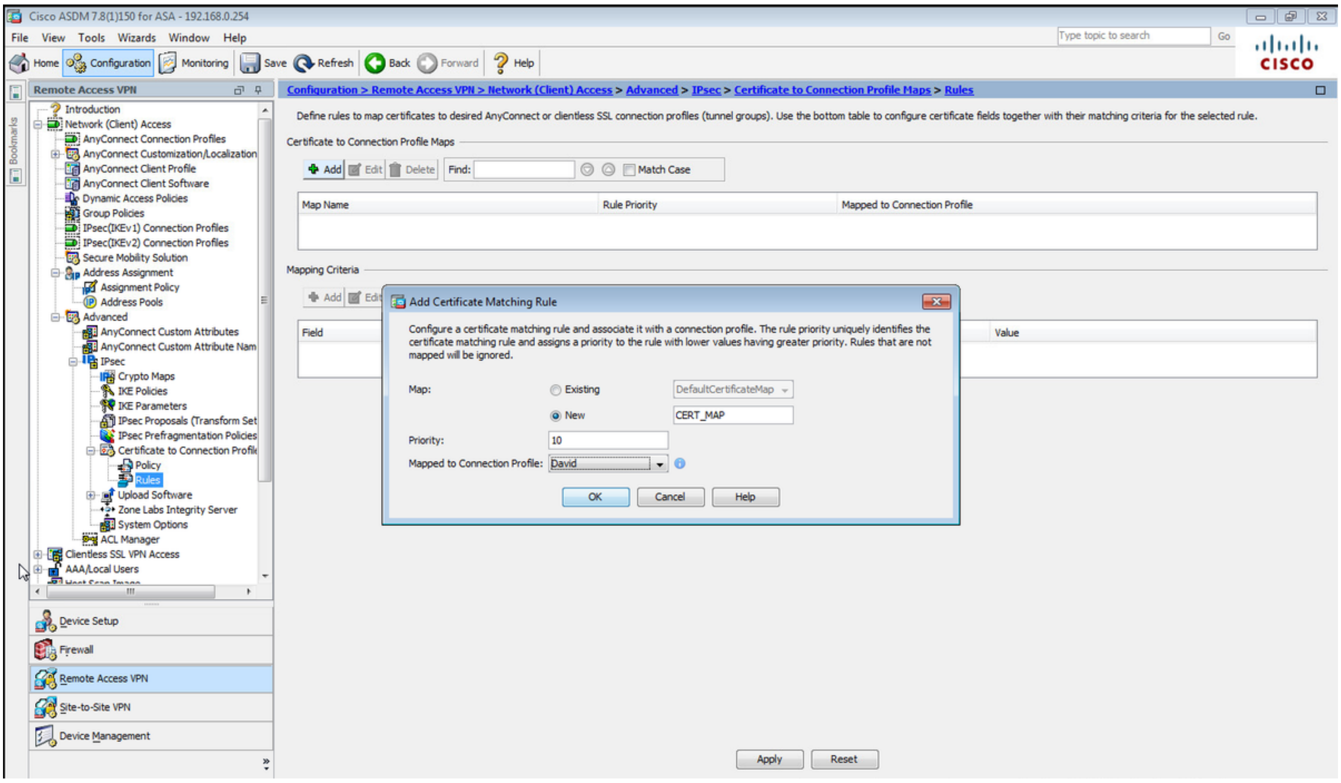
☑ Use the peer IP address to determine the Connection Profile

☑ Default to Connection Profile: DefaultRAGroup

واجهة سطر الأوامر (CLI).

```
tunnel-group-map enable rules
```

الخطوة 8. انتقل إلى **التكوين** > Remote Access VPN (الوصول عن بعد) > Network (Client) Access (الوصول إلى الشبكة) > Advanced > IPsec > Certificate to Connection Profile Maps > Rules وإنشاء خريطة شهادة جديدة. حدد **إضافة** وإقرانه بمجموعة النفق. في هذا المثال تسمى مجموعة الأنفاق **ديفيد**.



Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules

Define rules to map certificates to desired AnyConnect or clientless SSL connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Add Certificate Matching Rule

Configure a certificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the certificate matching rule and assigns a priority to the rule with lower values having greater priority. Rules that are not mapped will be ignored.

Map: ○ Existing DefaultCertificateMap

● New CERT_MAP

Priority: 10

Mapped to Connection Profile: David

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254
Certificate to Connection Profile Maps
Map Name
Rule Priority
Mapped to Connection Profile
Mapping Criteria
Field
Value
OK
Cancel
Help
Apply
Reset

واجهة سطر الأوامر (CLI).

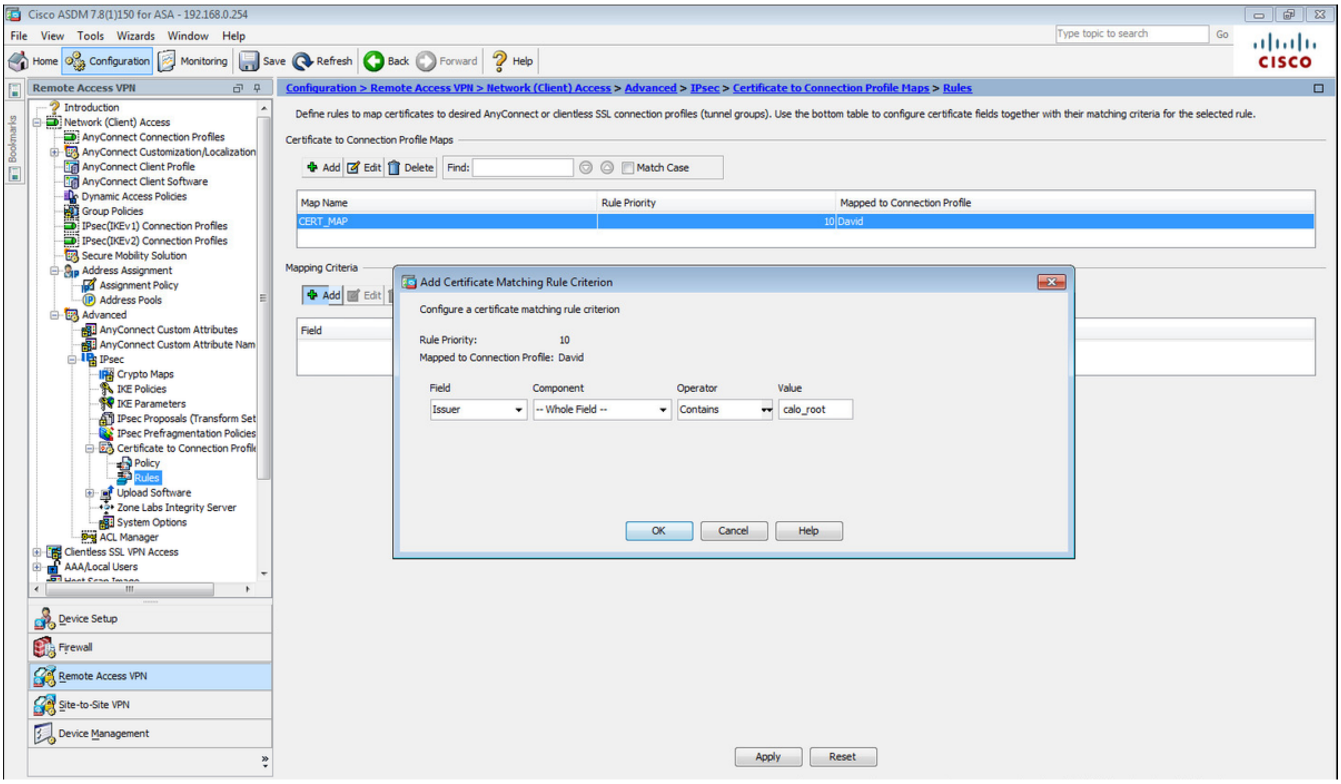
```
tunnel-group-map CERT_MAP 10 David
```

الخطوة 9. حدد **إضافة** في قسم **معايير التعيين** وأدخل هذه القيم.

الحقل: المصدر

عامل التشغيل: يحتوي على

القيمة: calo_root



Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules

Define rules to map certificates to desired AnyConnect or clientless SSL connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Certificate to Connection Profile Maps

Map Name	Rule Priority	Mapped to Connection Profile
CERT_MAP	10	David

Mapping Criteria

Add Certificate Matching Rule Criterion

Configure a certificate matching rule criterion

Rule Priority: 10

Mapped to Connection Profile: David

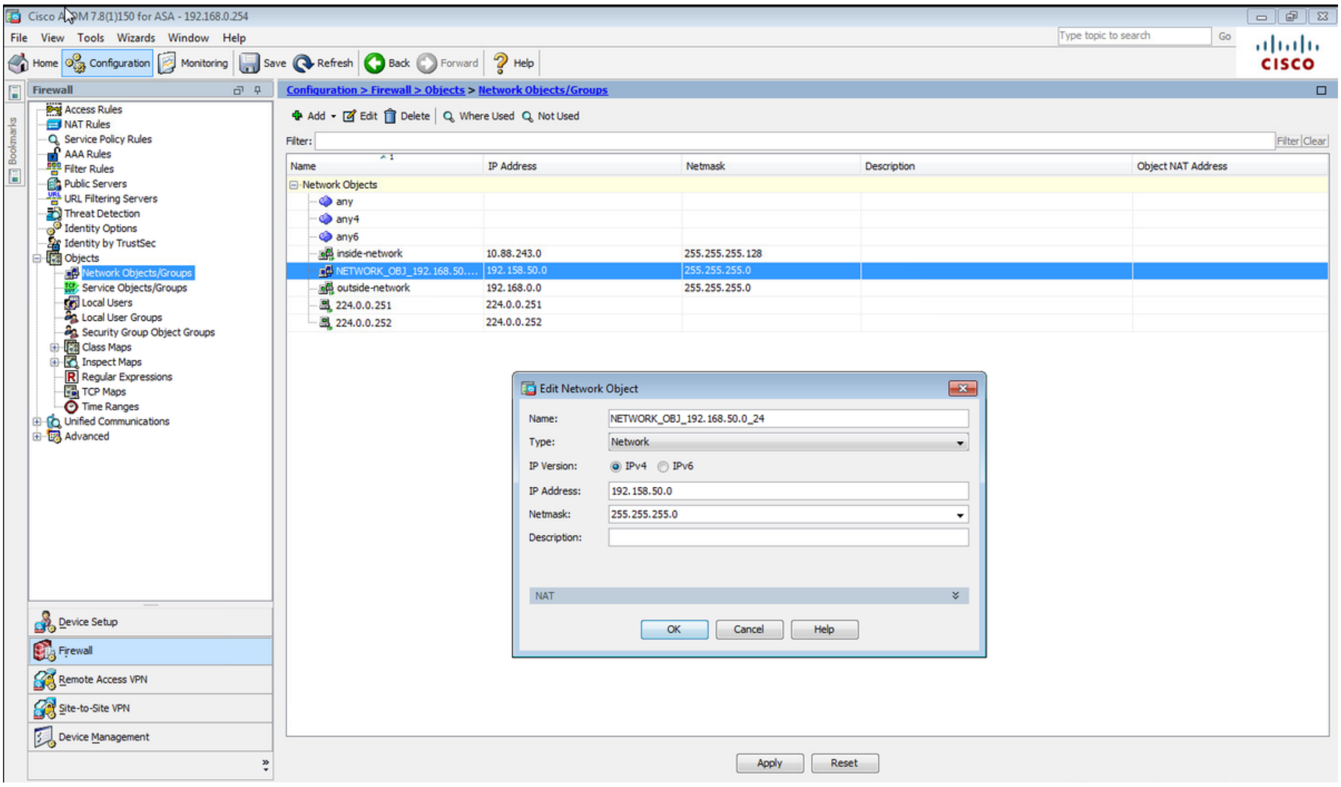
Field	Component	Operator	Value
Issuer	-- Whole Field --	Contains	calo_root

File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Assignment Policy
Address Pools
Advanced
AnyConnect Custom Attributes
AnyConnect Custom Attribute Nam
IPsec
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Set
IPsec Prefragmentation Policies
Certificate to Connection Profil
Policy
Rules
Upload Software
Zone Labs Integrity Server
System Options
ACL Manager
Clientless SSL VPN Access
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Add Edit Delete Find: Match Case
Field
OK Cancel Help
Apply Reset

واجهة سطر الأوامر (CLI).

```
crypto ca certificate map CERT_MAP 10
 issuer-name co calo_root
```

الخطوة 10. قم بإنشاء كائن باستخدام شبكة تجمع IP لاستخدامه لإضافة قاعدة إستثناء nat (ترجمة عنوان الشبكة) عند **التكوين > جدار الحماية > الكائنات > كائنات/مجموعات الشبكة> إضافة**.



Configuration > Firewall > Objects > Network Objects/Groups

Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
any				
any4				
any6				
inside-network	10.88.243.0	255.255.255.128		
NETWORK_OBJ_192.168.50....	192.158.50.0	255.255.255.0		
outside-network	192.168.0.0	255.255.255.0		
224.0.0.251	224.0.0.251			
224.0.0.252	224.0.0.252			

Edit Network Object

Name: NETWORK_OBJ_192.168.50.0_24

Type: Network

IP Version: ● IPv4 ○ IPv6

IP Address: 192.158.50.0

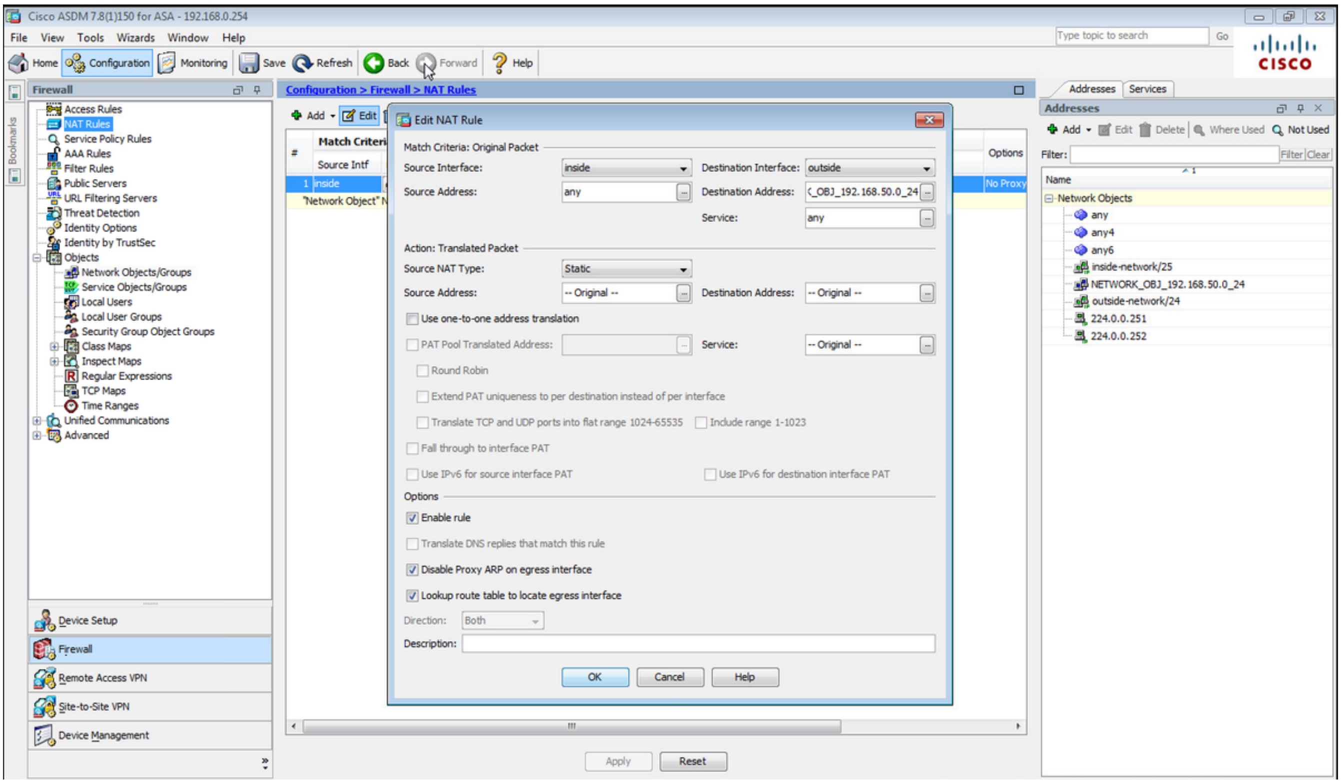
Netmask: 255.255.255.0

Description:

واجهة سطر الأوامر (CLI).

```
object network NETWORK_OBJ_192.168.50.0_24
  subnet 192.168.50.0 255.255.255.0
```

الخطوة 11. انتقل إلى **تكوين > جدار حماية > قواعد nat** وحدد **إضافة** لإنشاء قاعدة إستثناء nat لحركة مرور RA VPN.



Configuration > Firewall > NAT Rules

Edit NAT Rule

Match Criteria: Original Packet

Source Interface: inside Destination Interface: outside

Source Address: any Destination Address: <_OBJ_192.168.50.0_24

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original -- Destination Address: -- Original --

□ Use one-to-one address translation

□ PAT Pool Translated Address: Service: -- Original --

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT

□ Use IPv6 for source interface PAT □ Use IPv6 for destination interface PAT

Options

☑ Enable rule

□ Translate DNS replies that match this rule

☑ Disable Proxy ARP on egress interface

☑ Lookup route table to locate egress interface

Direction: Both

Description:

واجهة سطر الأوامر (CLI).

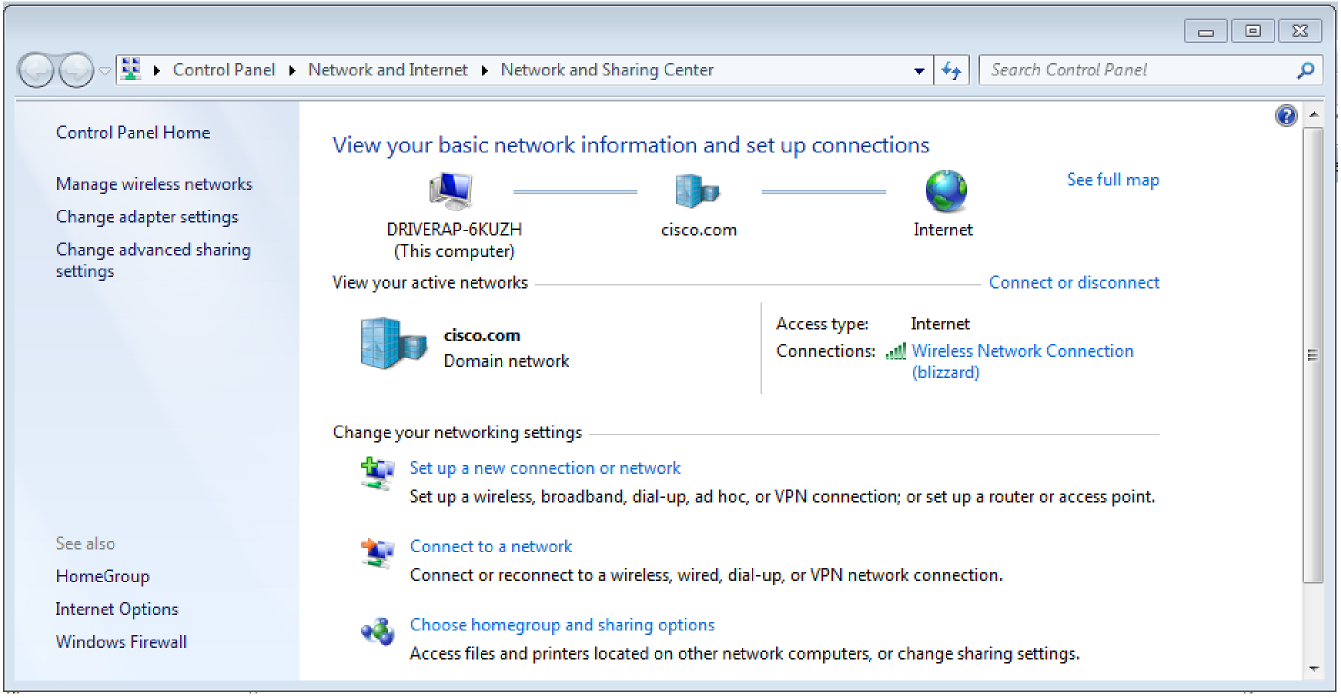
```
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup
```

هذا هو تكوين ASA الكامل المستخدم لهذا المثال.

```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.88.243.108 255.255.255.128

object network NETWORK_OBJ_192.168.50.0_24
 subnet 192.168.50.0 255.255.255.0
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24
ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

crypto ikev2 remote-access trustpoint HeadEnd

group-policy GP_David internal
group-policy GP_David attributes
 vpn-tunnel-protocol ikev2

tunnel-group David type remote-access
tunnel-group David general-attributes
 address-pool ACPool
 default-group-policy GP_David
 authentication-server-group LOCAL
tunnel-group David webvpn-attributes
 authentication certificate
tunnel-group David ipsec-attributes
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate HeadEnd

tunnel-group-map enable rules
crypto ca certificate map CERT_MAP 10
 issuer-name co calo_root
tunnel-group-map CERT_MAP 10 David

crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5

crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256
crypto map outside_map 65535 ipsec-isakmp dynamic Anyconnect
crypto map outside_map interface outside
```

تكوين العميل المدمج لنظام التشغيل Windows 7

الخطوة 1. انتقل إلى **لوحة التحكم > الشبكة والإنترنت > مركز الشبكات والمشاركة**.



Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

DRIVERAP-6KUZH (This computer) — cisco.com — Internet

See full map

View your active networks — Connect or disconnect

cisco.com
Domain network

Access type: Internet
Connections: Wireless Network Connection (blizzard)

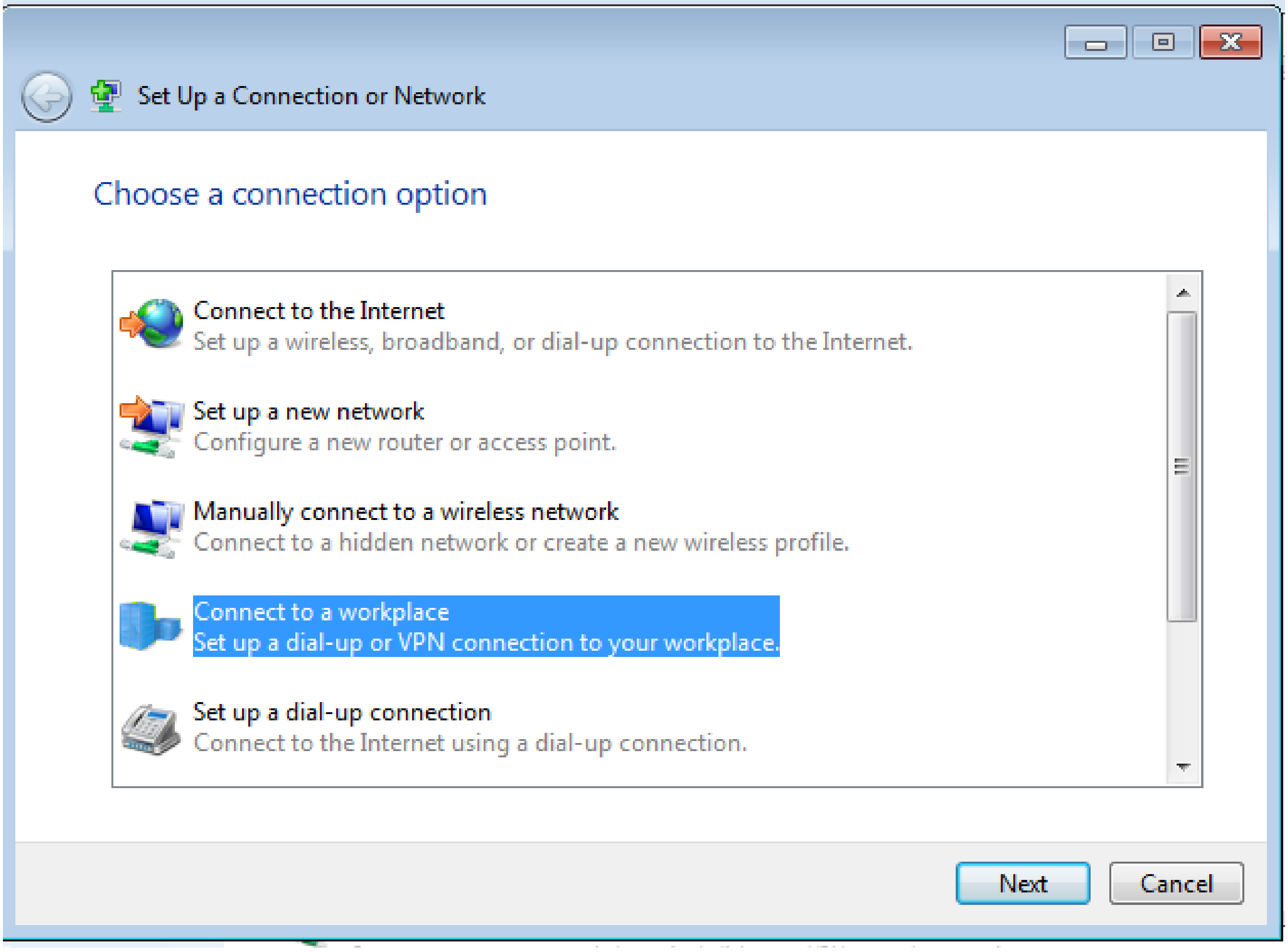
Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

الخطوة 2. حدد **إعداد اتصال أو شبكة جديدة**.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

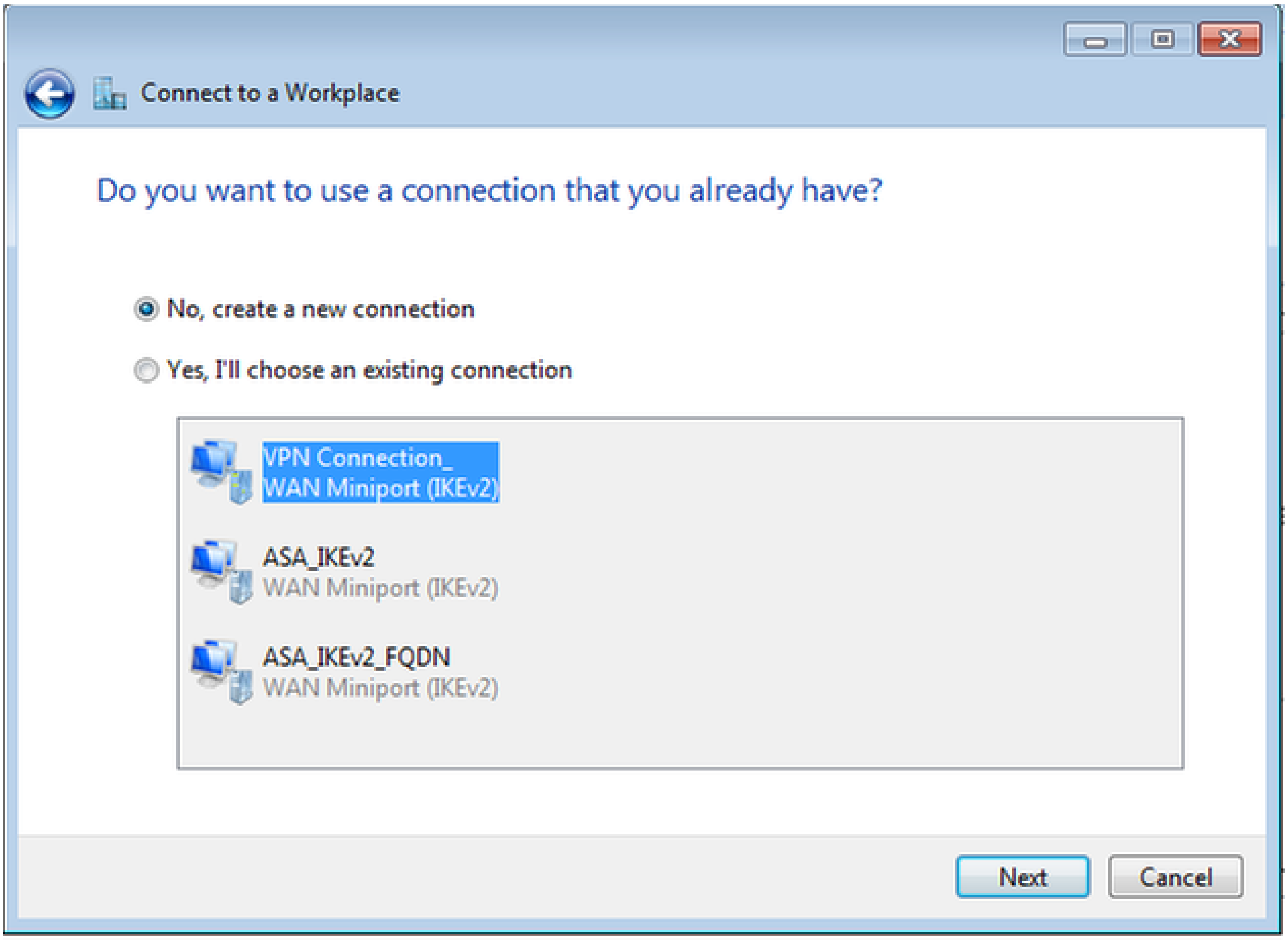
Set up a new network
Configure a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

الخطوة 3. حدد **الاتصال بمساحة العمل والتالي**.



Connect to a Workplace

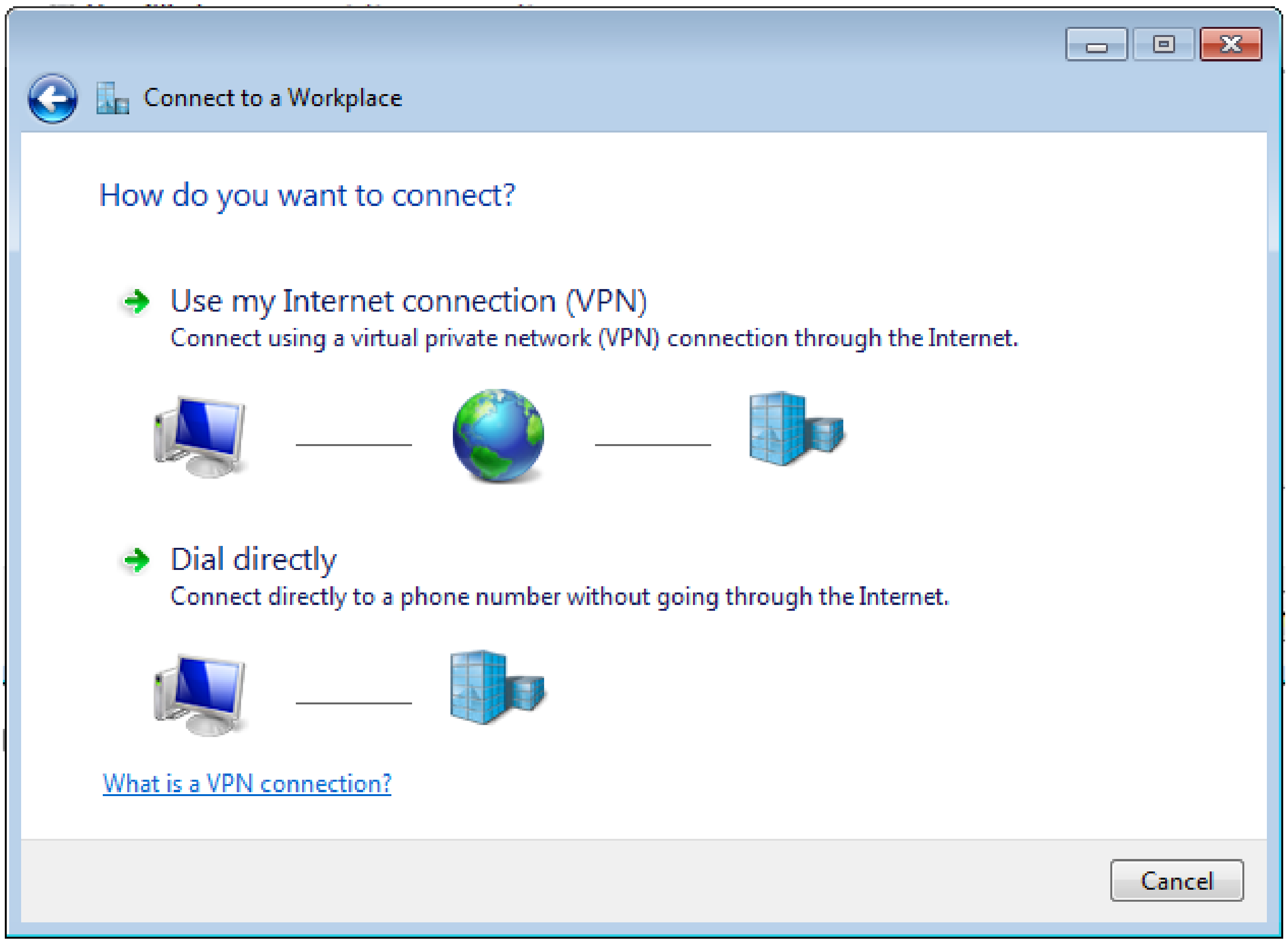
Do you want to use a connection that you already have?

● No, create a new connection

○ Yes, I'll choose an existing connection

VPN Connection_ WAN Miniport (IKEv2)
ASA_IKEv2 WAN Miniport (IKEv2)
ASA_IKEv2_FQDN WAN Miniport (IKEv2)

الخطوة 4. حدد **لا، قم بإنشاء اتصال جديد والتالي**.



Connect to a Workplace

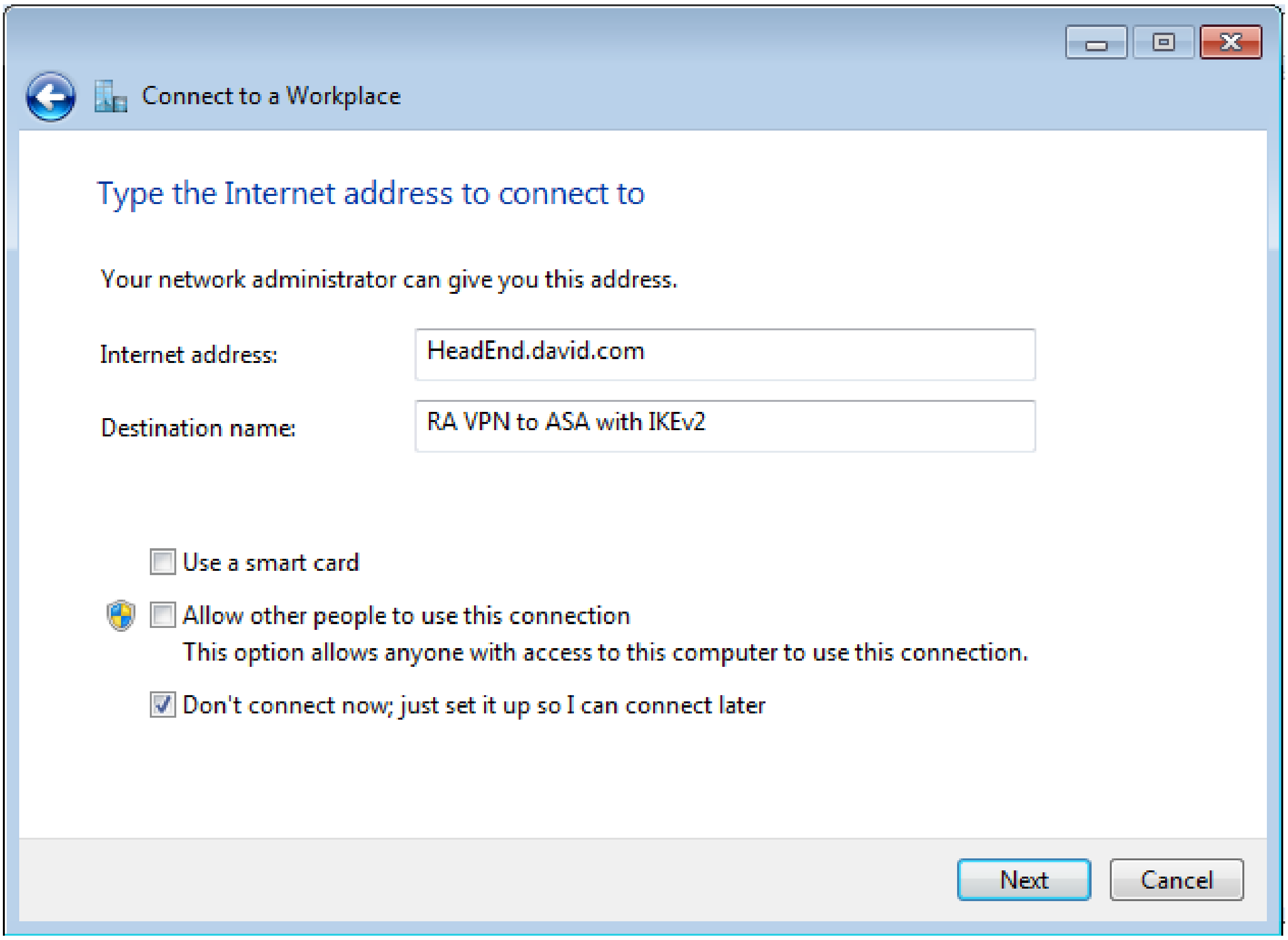
How do you want to connect?

➔ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

➔ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

الخطوة 5. حدد **إستخدام اتصال الإنترنت (VPN)** وأضف سلسلة الاسم الشائع لشهادة (CN (HeadEnd في حقل **عنوان الإنترنت**. في حقل **اسم الوجهة** اكتب اسم الاتصال. يمكن أن تكون أي سلسلة. تأكد من تحديد **مربع عدم الاتصال الآن؛ قم فقط بإعداده بحيث يمكنني الاتصال لاحقا**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: HeadEnd.david.com

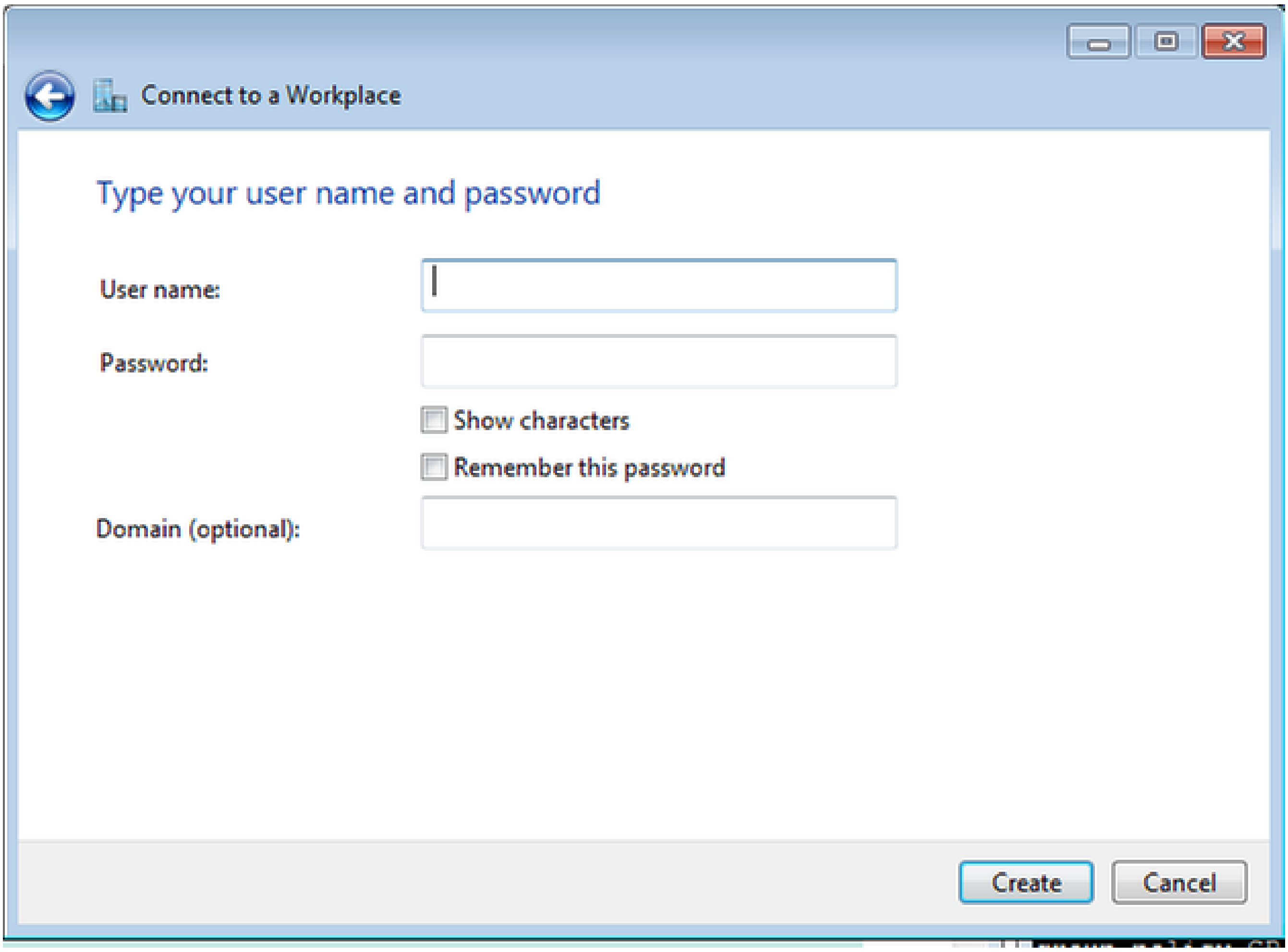
Destination name: RA VPN to ASA with IKEv2

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

الخطوة 6. حدد **التالي**.



Connect to a Workplace

Type your user name and password

User name:

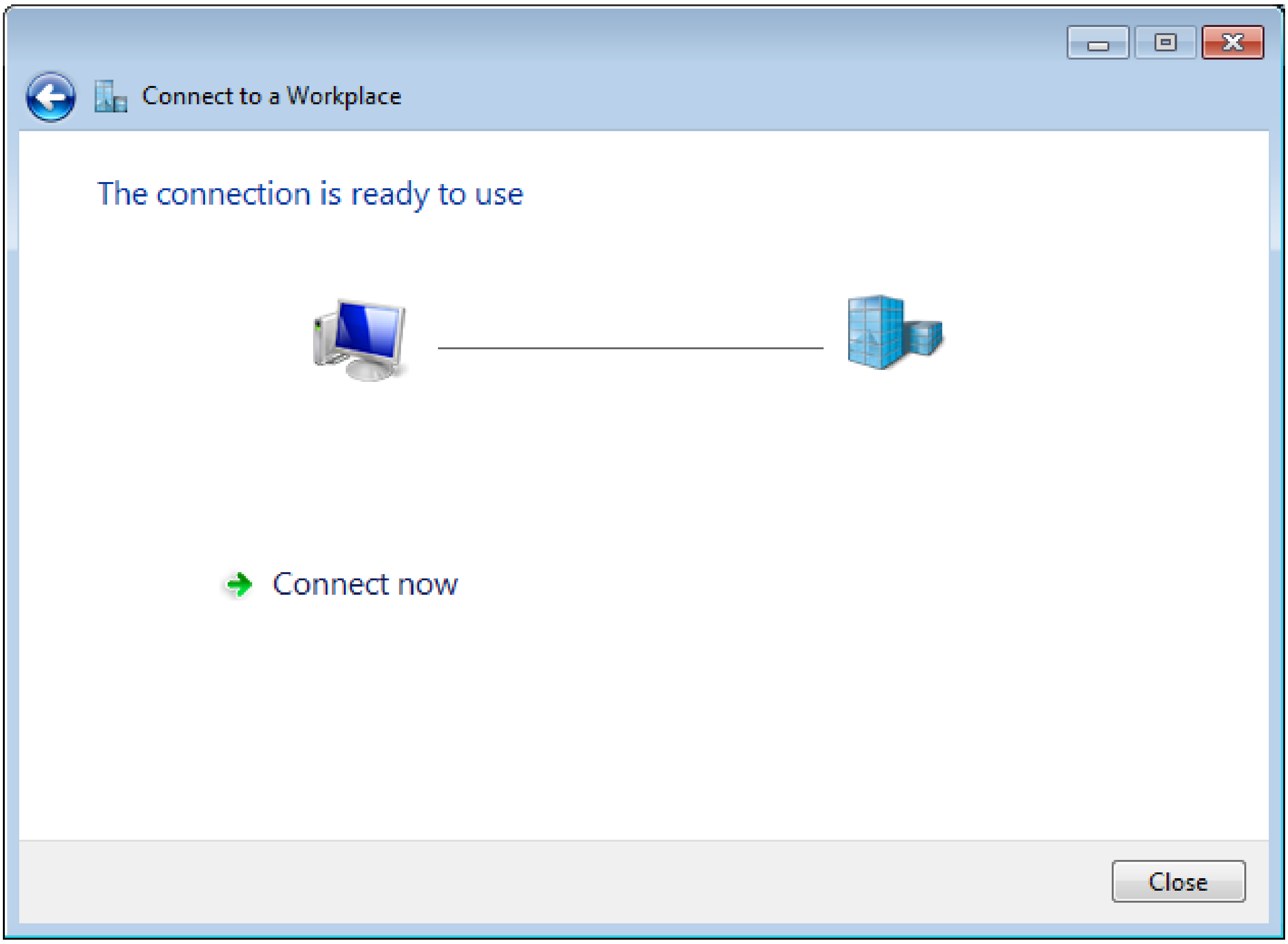
Password:

□ Show characters

□ Remember this password

Domain (optional):

الخطوة 7. حدد **إنشاء**.



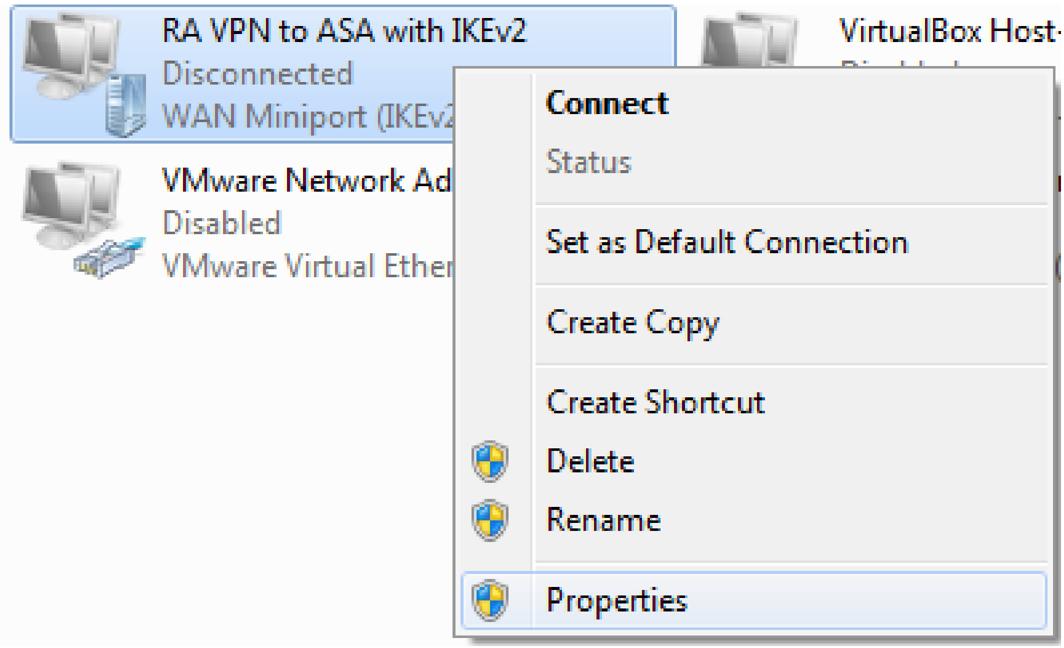
Connect to a Workplace

The connection is ready to use

Connect now

Close

الخطوة 8. حدد **إغلاق** وتصفح إلى **لوحة التحكم > الشبكة والإنترنت > إتصالات الشبكة**. حدد اتصال الشبكة الذي تم إنشاؤه وانقر فوقه بزر الماوس الأيمن. حدد **خصائص**.

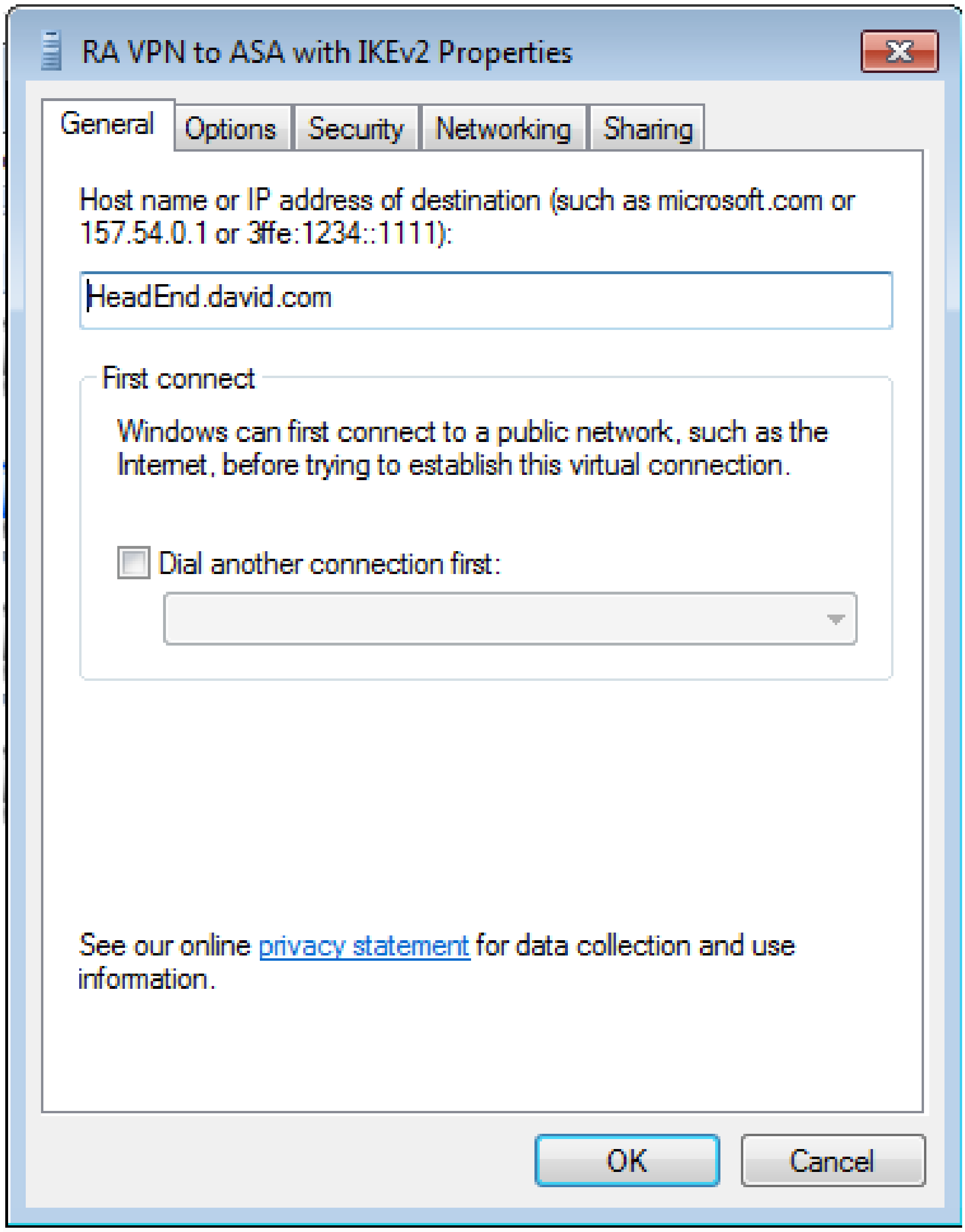


RA VPN to ASA with IKEv2
Disconnected
WAN Miniport (IKEv2

VirtualBox Host-

VMware Network Ad
Disabled
VMware Virtual Ether

الخطوة 9. في علامة التبويب **عام** يمكنك التحقق من صحة اسم المضيف المناسب لنقطة الاستقبال. سيقوم الكمبيوتر بحل هذا الاسم إلى عنوان ASA IP المستخدم لتوصيل مستخدمي RA VPN.



Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

HeadEnd.david.com

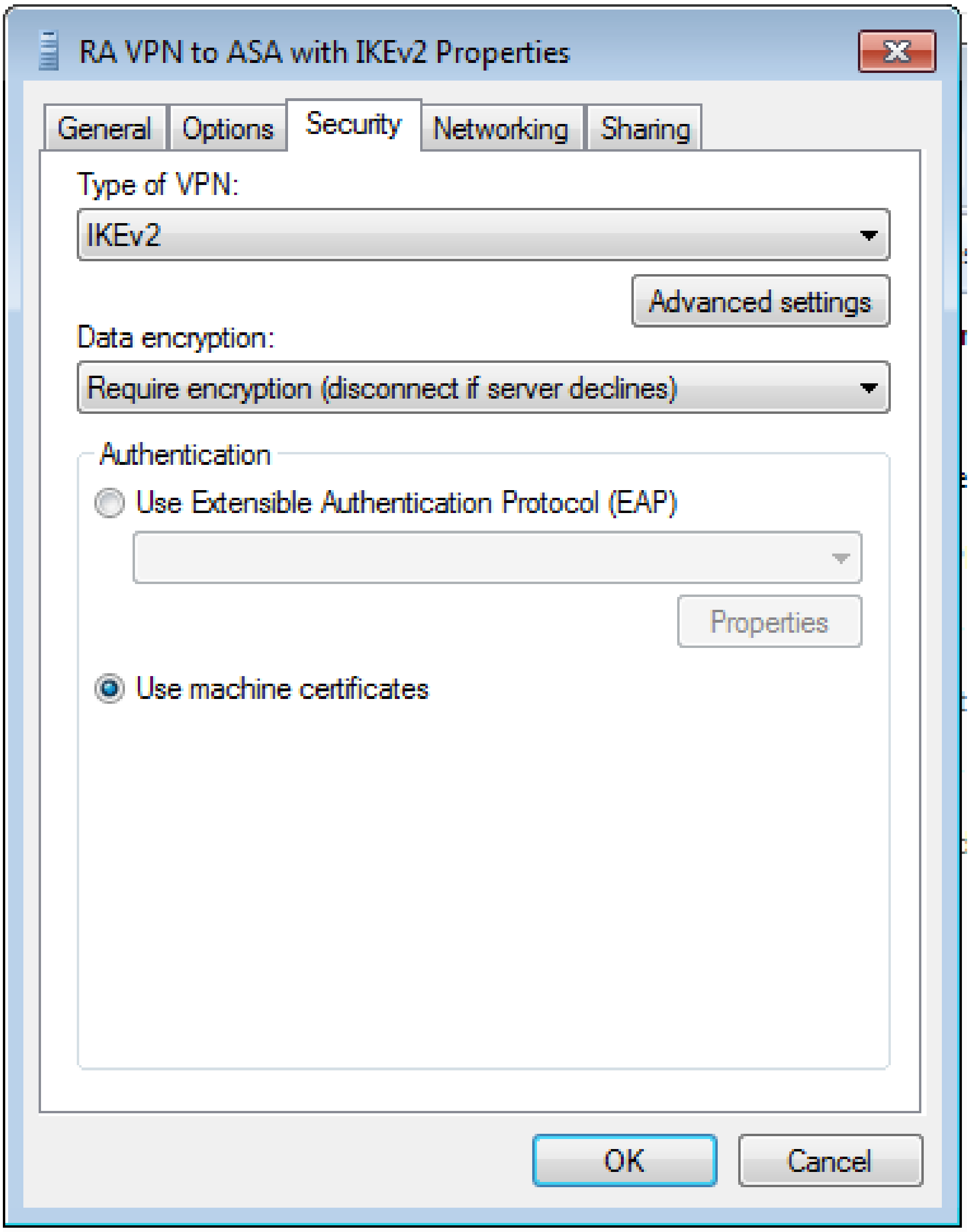
First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:

See our online privacy statement for data collection and use information.

الخطوة 10. انتقل إلى علامة التبويب **الأمان** وحدد **IKEv2** ليكون **نوع شبكة** VPN. في **قسم المصادقة** حدد **إستخدام شهادات الجهاز**.



RA VPN to ASA with IKEv2 Properties

Type of VPN:
IKEv2

Data encryption:
Require encryption (disconnect if server declines)

Authentication

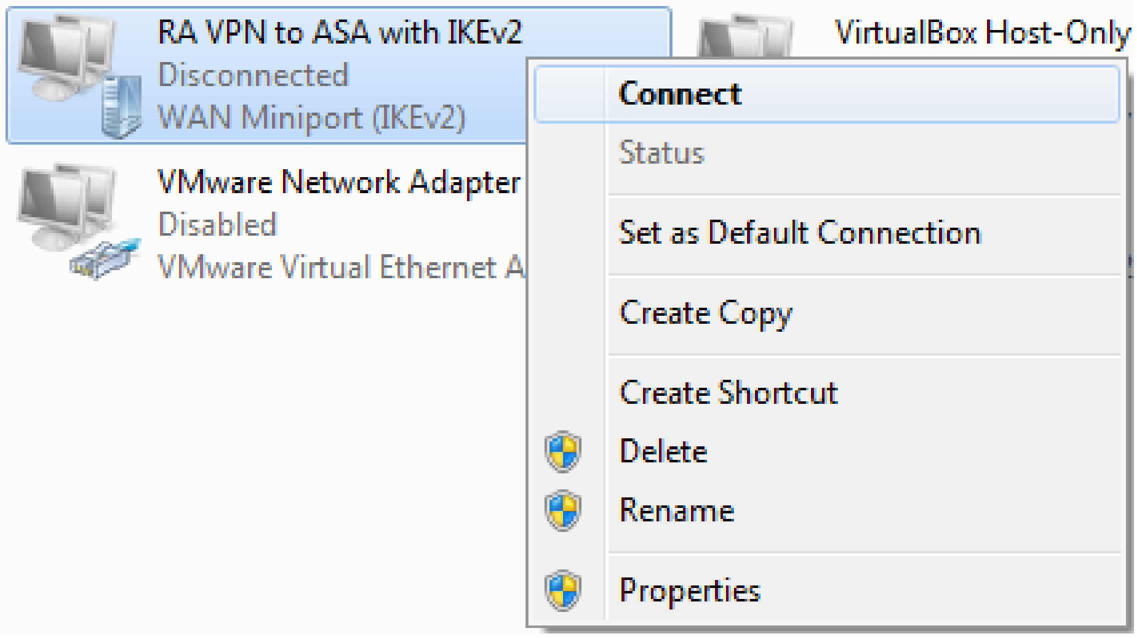
○ Use Extensible Authentication Protocol (EAP)

● Use machine certificates

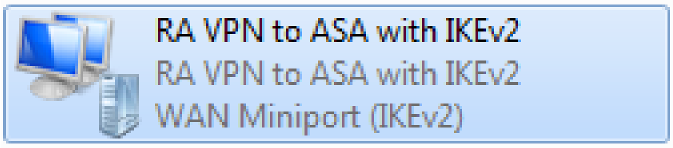
الخطوة 11. حدد **موافق** وانتقل إلى **C:\Windows\System32\drivers\etc**. افتح ملف **الأجهزة المضيفة** باستخدام محرر نصي. قم بتكوين إدخال لحل شبكة FQDN (اسم المجال المؤهل بالكامل) التي تم تكوينها في اتصال الشبكة بعنوان IP الخاص بنقطة الاستقبال والبث الخاصة بك (في هذا المثال، الواجهة الخارجية).

```
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
10.88.243.108 HeadEnd.david.com
```

الخطوة 12. ارجع إلى **لوحة التحكم > الشبكة والإنترنت > إتصالات الشبكة**. حدد اتصال الشبكة الذي أنشأته. انقر بزر الماوس الأيمن فوقه ثم حدد **اتصال**.



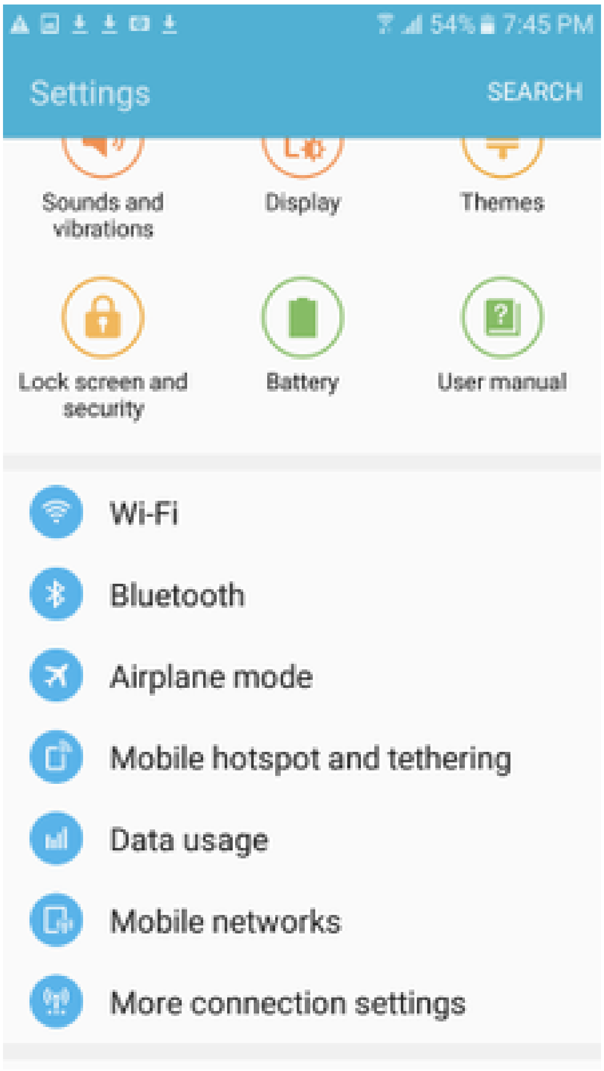
الخطوة 13. انتقالات حالة اتصال الشبكة من "غير متصل" إلى "متصل" ثم إلى "متصل". وأخيرا، يظهر الاسم الذي حددته لاتصال الشبكة.



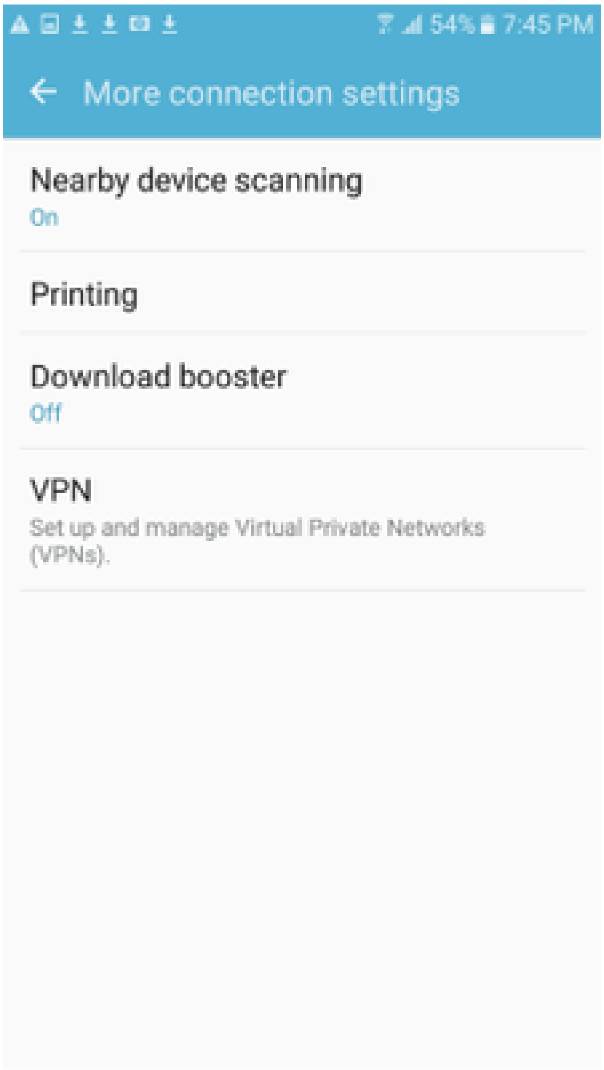
يتم توصيل الكمبيوتر بنقطة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN) عند هذه النقطة.

تكوين عميل VPN الأصلي من Android

الخطوة 1. انتقل إلى **الإعدادات>مزيد من إعدادات الاتصال**



الخطوة 2. تحديد VPN



54% 7:45 PM

More connection settings

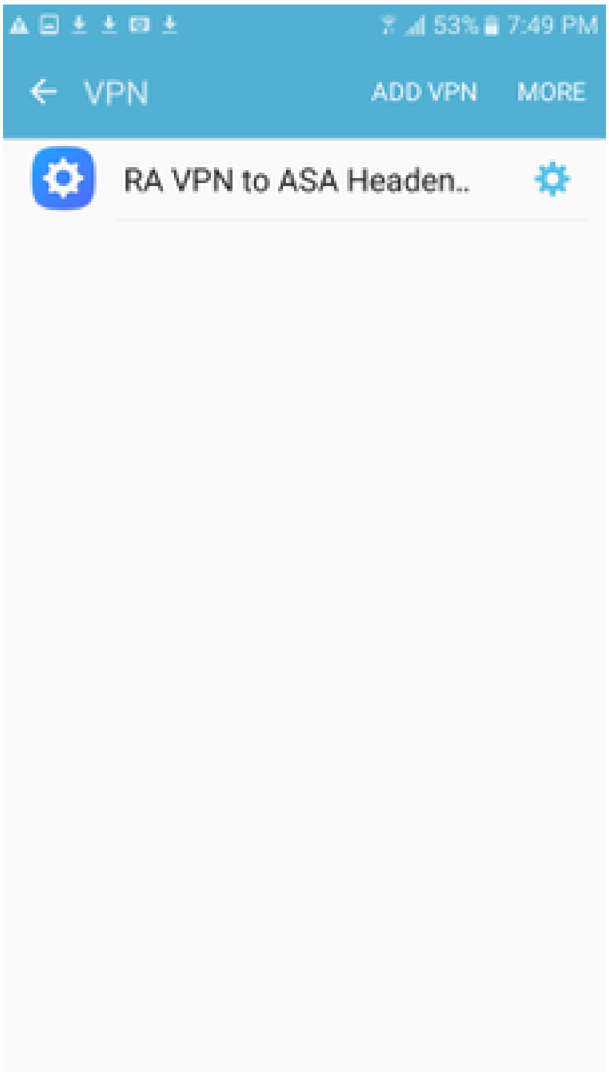
Nearby device scanning
On

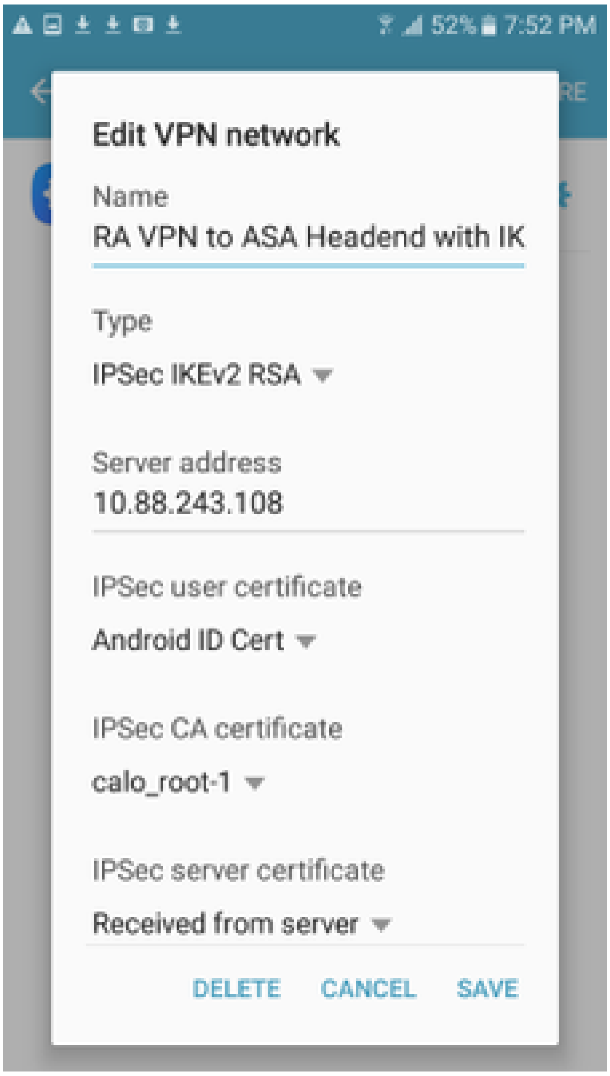
Printing

Download booster
Off

VPN
Set up and manage Virtual Private Networks (VPNs).

الخطوة 3. حدد **إضافة VPN**. إذا تم إنشاء الاتصال بالفعل كما في هذا المثال، فاضغط على رمز المحرك لتحريره. حدد IPSec IKEv2 RSA في حقل **النوع**. **عنوان الخادم** هو عنوان IP لواجهة ASA التي تم تمكين IKEv2 بها. بالنسبة **لشهادة مستخدم IPSec** و**شهادة IPSec CA**، حدد الشهادات المثبتة بالضغط على القوائم المنسدلة. أترك **شهادة خادم IPSec** مع الخيار الافتراضي، الذي تم إستلامه من الخادم.


53% 7:49 PM
VPN
ADD VPN
MORE
RA VPN to ASA Headen..



Edit VPN network

Name
RA VPN to ASA Headend with IK

Type
IPSec IKEv2 RSA

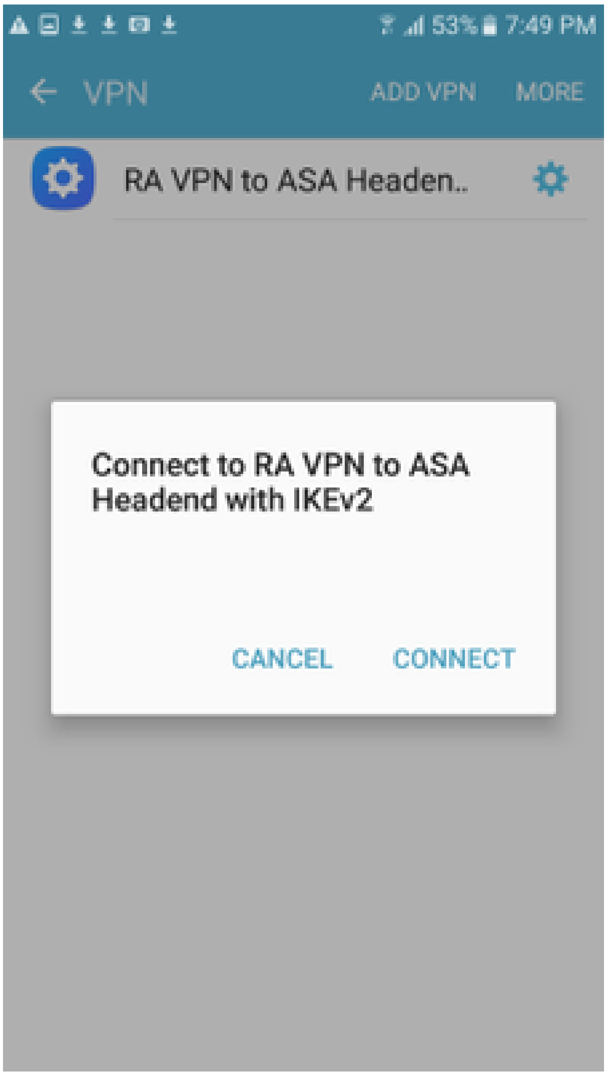
Server address
10.88.243.108

IPSec user certificate
Android ID Cert

IPSec CA certificate
calo_root-1

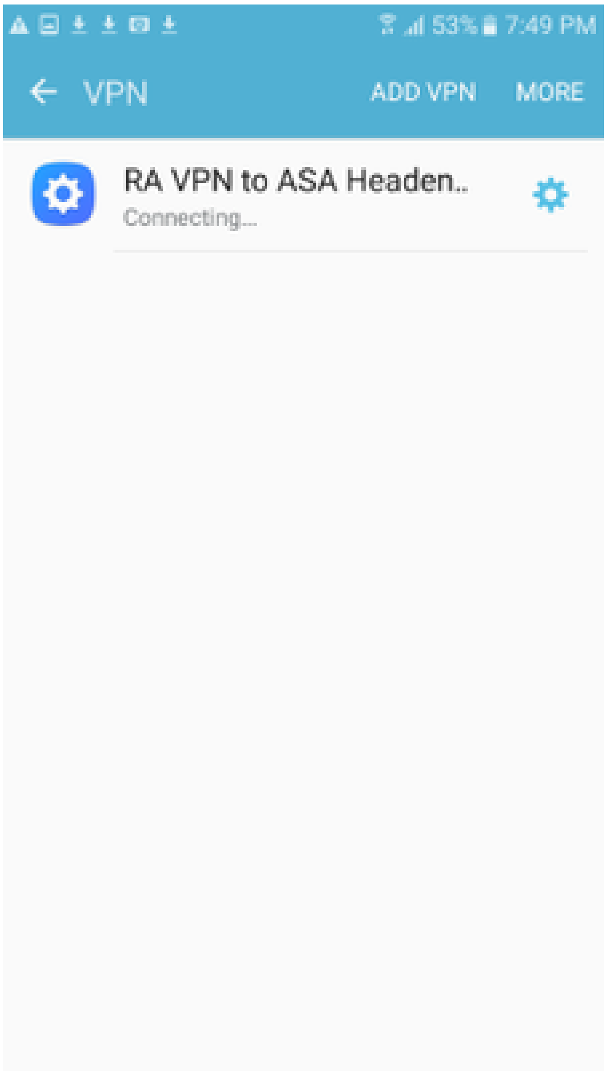
IPSec server certificate
Received from server

الخطوة 4. حدد **حفظ** ثم اضغط على اسم اتصال VPN الجديد.



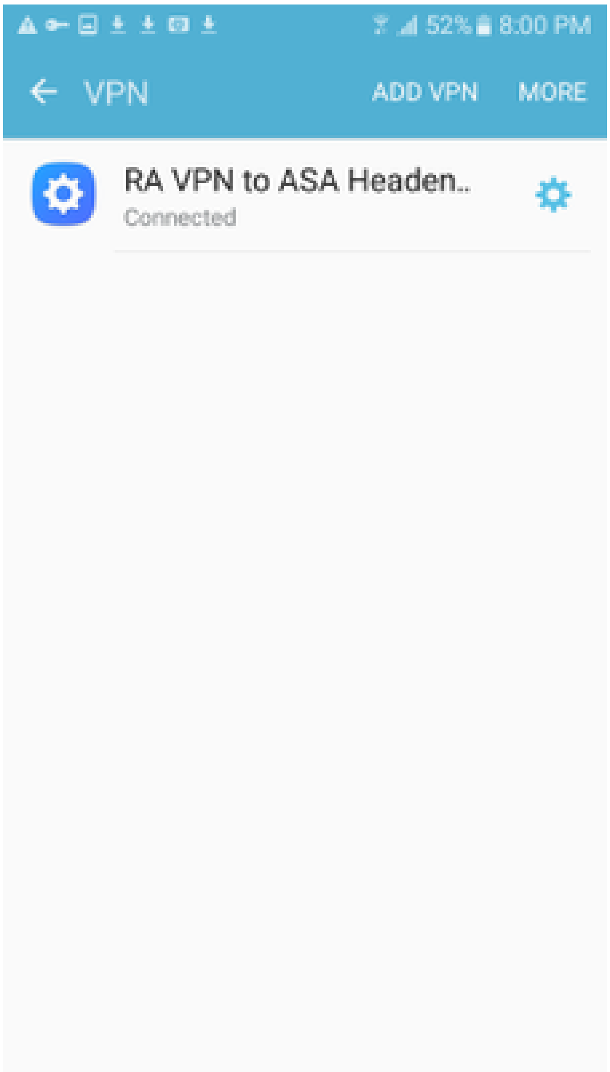
Connect to RA VPN to ASA Headend with IKEv2

الخطوة 5. حدد **اتصال**.



RA VPN to ASA Headen..

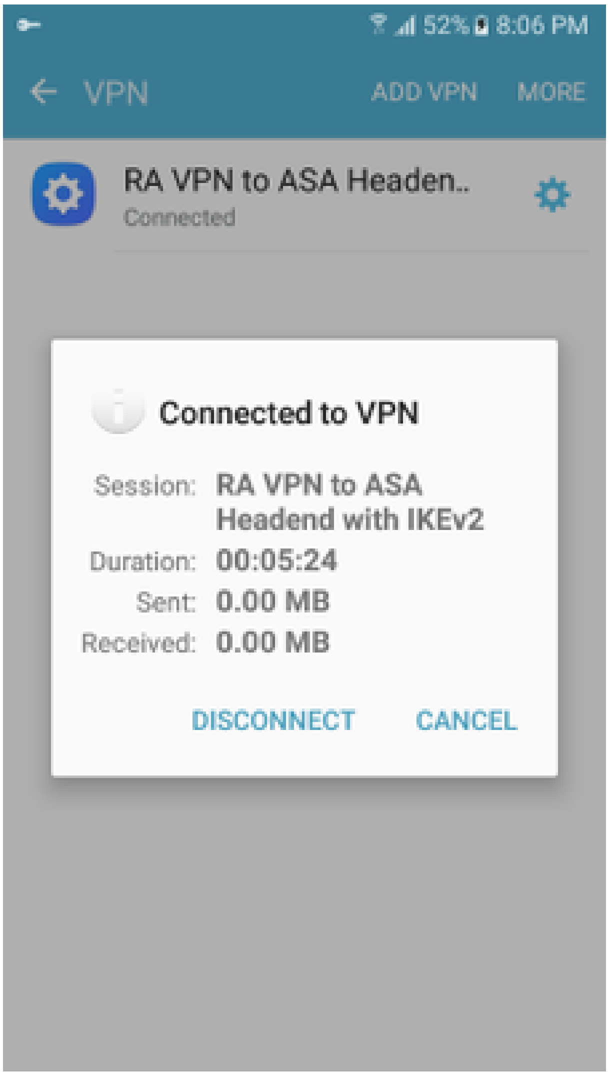
Connecting...



RA VPN to ASA Headen..

Connected

الخطوة 6. اكتب اتصال VPN مرة أخرى للتحقق من الحالة. يتم عرضه الآن على أنه **متصل**.



Connected to VPN

Session: RA VPN to ASA Headend with IKEv2

Duration: 00:05:24

Sent: 0.00 MB

Received: 0.00 MB

التحقق من الصحة

أوامر التحقق من الصحة على وحدة الاستقبال والبث ASA:

```
ASA#show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username     : Win7_PC.david.com      Index        : 24
Assigned IP  : 192.168.50.1           Public IP    : 10.152.206.175
Protocol     : IKEv2 IPsec
License      : AnyConnect Premium
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 16770
Pkts Tx      : 0                      Pkts Rx      : 241
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GP_David               Tunnel Group : David
Login Time   : 08:00:01 UTC Tue Jul 18 2017
Duration     : 0h:00m:21s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a0a0a0100018000596dc001
Security Grp : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1
:IKEv2
Tunnel ID    : 24.1
```

```
                                   UDP Src Port : 4500                   UDP Dst Port : 4500
                                                                Rem Auth Mode: rsaCertificate
                                                                Loc Auth Mode: rsaCertificate
                                   Encryption   : AES256                 Hashing      : SHA1
                          Rekey Int (T): 86400 Seconds          Rekey Left(T): 86379 Seconds
                                      PRF          : SHA1                   D/H Group    : 2
                                                                               :  Filter Name
                                                                                         :IPsec
                                                                          Tunnel ID    : 24.2
                                                          Local Addr   : 0.0.0.0/0.0.0.0/0/0
                                             Remote Addr  : 192.168.50.1/255.255.255.255/0/0
                                   Encryption   : AES256                 Hashing      : SHA1
                                                                        Encapsulation: Tunnel
                          Rekey Int (T): 28800 Seconds          Rekey Left(T): 28778 Seconds
                             Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
                         Conn Time Out: 518729 Minutes         Conn TO Left : 518728 Minutes
                                  Bytes Tx     : 0                      Bytes Rx     : 16947
                                    Pkts Tx      : 0                      Pkts Rx      : 244

                                                                      ASA# show crypto ikev2 sa
                                                                                     :IKEv2 SAs
                                   Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1
                 Tunnel-id                 Local                Remote     Status         Role
READY    RESPONDER      Encr: AES-      10.152.206.175/4500   10.88.243.108/4500    2119549341
                    CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: RSA
                                                          Life/Active Time: 86400/28 sec
                                   Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                                 remote selector 192.168.50.1/0 - 192.168.50.1/65535
                                               ESP spi in/out: 0xbfff64d7/0x76131476
                                                                      ASA# show crypto ipsec sa
                                                                             interface: outside
                     Crypto map tag: Anyconnect, seq num: 65535, local addr: 10.88.243.108
                                (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
                  (remote ident (addr/mask/prot/port): (192.168.50.1/255.255.255.255/0/0
                               current_peer: 10.152.206.175, username: Win7_PC.david.com
                                                 dynamic allocated peer ip: 192.168.50.1
                                                dynamic allocated peer ip(ipv6): 0.0.0.0

                                      pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0#
                                pkts decaps: 339, #pkts decrypt: 339, #pkts verify: 339#
                                              pkts compressed: 0, #pkts decompressed: 0#
                   pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0#
                    pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
                PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                                              TFC rcvd: 0, #TFC sent: 0#
                                Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0#
                                                        send errors: 0, #recv errors: 0#

      local crypto endpt.: 10.88.243.108/4500, remote crypto endpt.: 10.152.206.175/4500
                                    path mtu 1496, ipsec overhead 58(44), media mtu 1500
                                        PMTU time remaining (sec): 0, DF policy: copy-df
                                  ICMP error validation: disabled, TFC packets: disabled
                                                          current outbound spi: 76131476
                                                          current inbound spi : BFFF64D7
                                                                           :inbound esp sas
                                                            (spi: 0xBFFF64D7 (3221185751
                                   transform: esp-aes-256 esp-sha-hmac no compression
                                               { ,in use settings ={RA, Tunnel, IKEv2
                                      slot: 0, conn_id: 98304, crypto-map: Anyconnect
                                       sa timing: remaining key lifetime (sec): 28767
                                                                     IV size: 16 bytes
                                                          replay detection support: Y
                                                                   :Anti replay bitmap
                                                                0xFFFFFFFF 0xFFFFFFFF
```

```
                                                      :outbound esp sas
                                         (spi: 0x76131476 (1980961910
                transform: esp-aes-256 esp-sha-hmac no compression
                            { ,in use settings ={RA, Tunnel, IKEv2
                   slot: 0, conn_id: 98304, crypto-map: Anyconnect
                    sa timing: remaining key lifetime (sec): 28767
                                                 IV size: 16 bytes
                                       replay detection support: Y
                                               :Anti replay bitmap
                                            0x00000000 0x00000001
                                     ASA#show vpn-sessiondb license-summary
---------------------------------------------------------------------------
                                 VPN Licenses and Configured Limits Summary
---------------------------------------------------------------------------
Status : Capacity : Installed :  Limit
-----------------------------------------
AnyConnect Premium               :  ENABLED :       50 :        50 :   NONE
AnyConnect Essentials            : DISABLED :       50 :         0 :   NONE
Other VPN (Available by Default) :  ENABLED :       10 :        10 :   NONE
                                Shared License Server            : DISABLED
                                Shared License Participant       : DISABLED
(AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials
              (Advanced Endpoint Assessment     :  ENABLED(Requires Premium
                                AnyConnect for Cisco VPN Phone   :  ENABLED
                                VPN-3DES-AES                     :  ENABLED
                                VPN-DES                          :  ENABLED
---------------------------------------------------------------------------

---------------------------------------------------------------------------
                                                 VPN Licenses Usage Summary
---------------------------------------------------------------------------
      :  .Local : Shared :   All  :   Peak :  Eff
In Use : In Use : In Use : In Use :  Limit : Usage
----------------------------------------------------
AnyConnect Premium     :      1 :      0 :      1 :      1 :     50 :    2%
AnyConnect Client    :                 :      0 :      1          :    0%
AnyConnect Mobile  :                 :      0 :      0          :    0%
Clientless VPN       :                 :      0 :      0          :    0%
Generic IKEv2 Client :                 :      1 :      1          :    2%
Other VPN              :                 :      0 :      0 :     10 :    0%
Cisco VPN Client     :                 :      0 :      0          :    0%
                                                                L2TP Clients
Site-to-Site VPN     :                 :      0 :      0          :    0%
---------------------------------------------------------------------------
                                                         ASA# show vpn-sessiondb
---------------------------------------------------------------------------
                                                        VPN Session Summary
---------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
AnyConnect Client            :      0 :        11 :           1 :        0
SSL/TLS/DTLS               :      0 :         1 :           1 :        0
IKEv2 IPsec                :      0 :        10 :           1 :        0
           Generic IKEv2 Remote Access  :      1 :          14 :           1
---------------------------------------------------------------------------
Total Active and Inactive    :      1           Total Cumulative :     25
                                      Device Total VPN Capacity    :     50
                                      Device Load                  :     2%
---------------------------------------------------------------------------

---------------------------------------------------------------------------
                                                            Tunnels Summary
---------------------------------------------------------------------------
       Active : Cumulative : Peak Concurrent
```

```
----------------------------------------------
      IKEv2                          :      1 :         25 :                 1
      IPsec                          :      1 :         14 :                 1
      IPsecOverNatT                  :      0 :         11 :                 1
      AnyConnect-Parent              :      0 :         11 :                 1
      SSL-Tunnel                     :      0 :          1 :                 1
      DTLS-Tunnel                    :      0 :          1 :                 1
--------------------------------------------------------------------------
                        Totals                     :      2 :          63
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم المعلومات التي يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر تصحيح الأخطاء قبل أن تستخدم أوامر debugcommands.

تحذير: على ASA، يمكنك تعيين مستويات تصحيح أخطاء متنوعة؛ بشكل افتراضي، يتم إستخدام المستوى 1. إذا قمت بتغيير مستوى تصحيح الأخطاء، فإن اتساع تصحيح الأخطاء يزداد. افعل ذلك بحذر، خاصة في بيئات الإنتاج.

- **تصحيح أخطاء بروتوكول ikev2 الإصدار 15**
- **النظام الأساسي Debug crypto ikev2 Platform 15**
- **debug crypto ca 255**

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).