VPN RA ASA IKEv2 avec clients VPN Windows 7 ou Android et configuration de l'authentification des certificats

Contenu

Introduction

Ce document décrit comment configurer Cisco Adaptive Security Appliance (ASA) Version 9.7.1 et ultérieure afin de permettre aux clients VPN natifs de Windows 7 et Android (réseau privé virtuel) d'établir une connexion VPN d'accès distant avec l'utilisation du protocole IKEv2 (Internet Key Exchange Protocol) et des certificats comme méthode d'authentification.

Avec la collaboration de David Rivera et Cesar Lopez Zamarripa, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Autorité de certification (CA)
- Infrastructure à clé publique (PKI)
- VPN RA avec IKEv2 sur ASA
- Client VPN intégré Windows 7
- Client VPN natif Android

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CISCO1921/K9 - 15.5(3)M4a en tant que serveur CA IOS
- ASA5506X - 9.7(1) en tant que tête de réseau VPN
- Windows 7 comme ordinateur client
- Galaxy J5 - Android 6.0.1 en tant que client mobile

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Aperçu

Voici les étapes à suivre pour configurer les clients VPN natifs Windows 7 et Android afin de se connecter à une tête de réseau ASA :

Configurer l'autorité de certification

L'autorité de certification permet d'incorporer l'utilisation de clé étendue (EKU) requise dans le certificat. Pour la tête de réseau ASA, l'unité EKU d'authentification du serveur de certificats est requise, tandis que le certificat client nécessite l'unité EKU d'authentification du client.

Plusieurs serveurs CA peuvent être utilisés, notamment :

- Serveur Cisco IOS CA
- Serveur OpenSSL CA
- Serveur Microsoft CA
- 3troisième CA des parties

IOS CA Server est utilisé pour cet exemple de configuration.

Cette section décrit la configuration de base permettant à un CISCO1921/K9 avec la version 15.5(3)M4a de fonctionner en tant que serveur AC.

Étape 1. Assurez-vous que le périphérique et la version prennent en charge la commande 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
```

Étape 2. Activez le serveur HTTP sur le routeur.

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

Étape 3. Générez une paire de clés RSA exportable.

```
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)
```

Étape 4. Configurez un point de confiance.

```
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>
```

> **Note**: L'adresse IP de la commande d'inscription est l'une des adresses IP configurées par le routeur pour une interface accessible.

Étape 5. Authentifiez le point de confiance (Obtenir le certificat de l'autorité de certification).

```
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.
```

Étape 6. Inscrivez le point de confiance (Obtenez le certificat d'identité).

```
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
```

Étape 7. Vérifiez les certificats.

```
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
```

Étape 8. Exportez le point de confiance HeadEnd vers le terminal au format PKCS12 pour obtenir le certificat d'identité. Le certificat de l'autorité de certification et la clé privée sont ajoutés dans un seul fichier.

```
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.
```


Étape 9. Créez un point de confiance vide sur l'ASA.

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

Étape 10. Importer le fichier 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
```


Étape 11. Vérifiez les informations de certificat.

```
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
```

Générer un certificat client

Étape 1. Générez une paire de clés RSA exportable.

```
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
```

Étape 2. Configurez un point de confiance.

```
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>
```

Étape 3. Authentifiez le point de confiance configuré (Obtenir le certificat de l'autorité de certification).

```
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.
```

Étape 4. Inscrivez le point de confiance authentifié (Obtenir le certificat d'identité).

```
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
```

Étape 5. Vérifiez les informations des certificats.

```
IOS-CA#show crypto pki certificates verbose <Win7_PC>
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 03
  Certificate Usage: General Purpose
  Issuer:
```

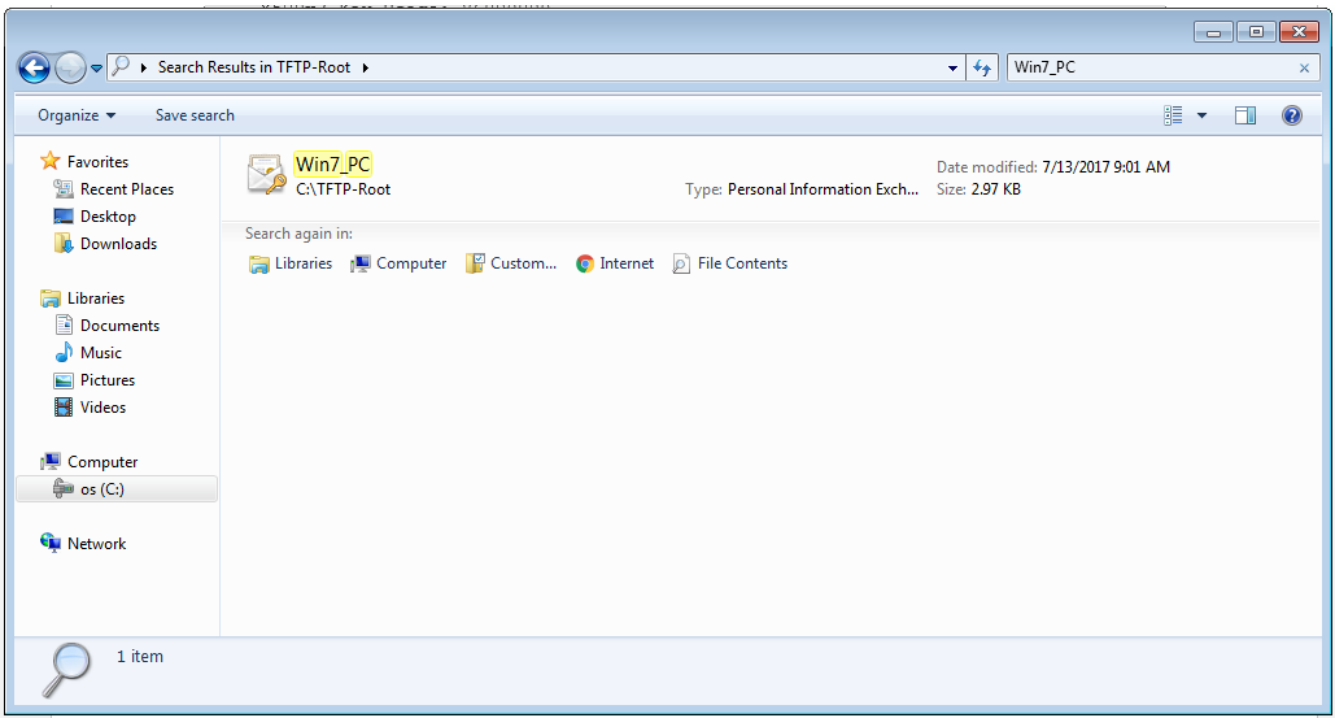
```
    cn=calo_root
  Subject:
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
    cn=Win7_PC.david.com
  Validity Date:
    start date: 13:29:51 UTC Jul 13 2017
    end   date: 13:29:51 UTC Jul 13 2018
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 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
```

Installer le certificat d'identité sur l'ordinateur client Windows 7

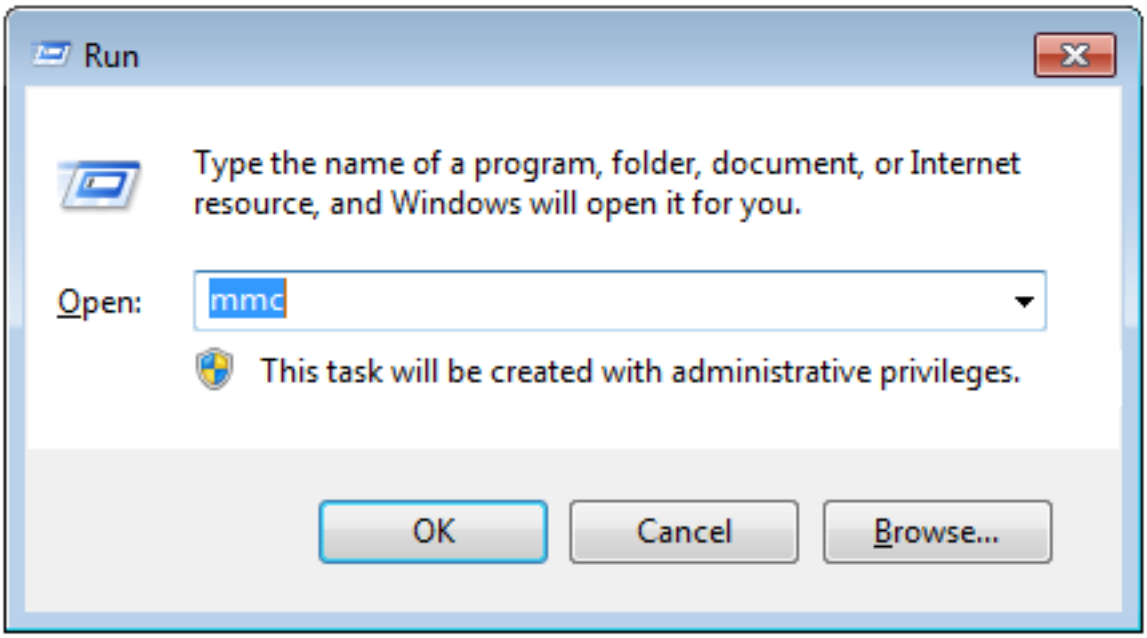
Étape 1. Exportez le point de confiance Win7_PC nommé vers un serveur FTP/TFTP (installé sur votre ordinateur Windows 7) au format PKCS12 (.p12) pour obtenir le certificat d'identité, le certificat d'autorité de certification et la clé privée dans un seul fichier.

```
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.
```

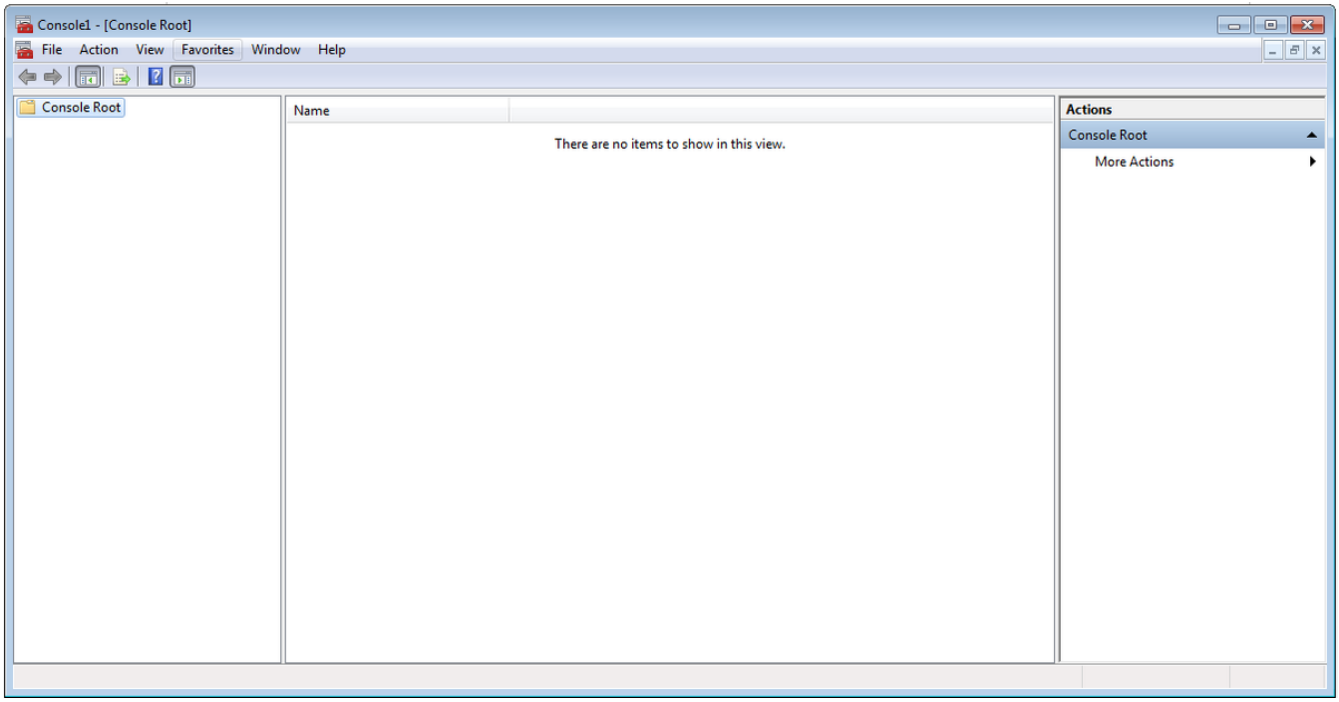
Voici l'aspect du fichier exporté sur une machine cliente.



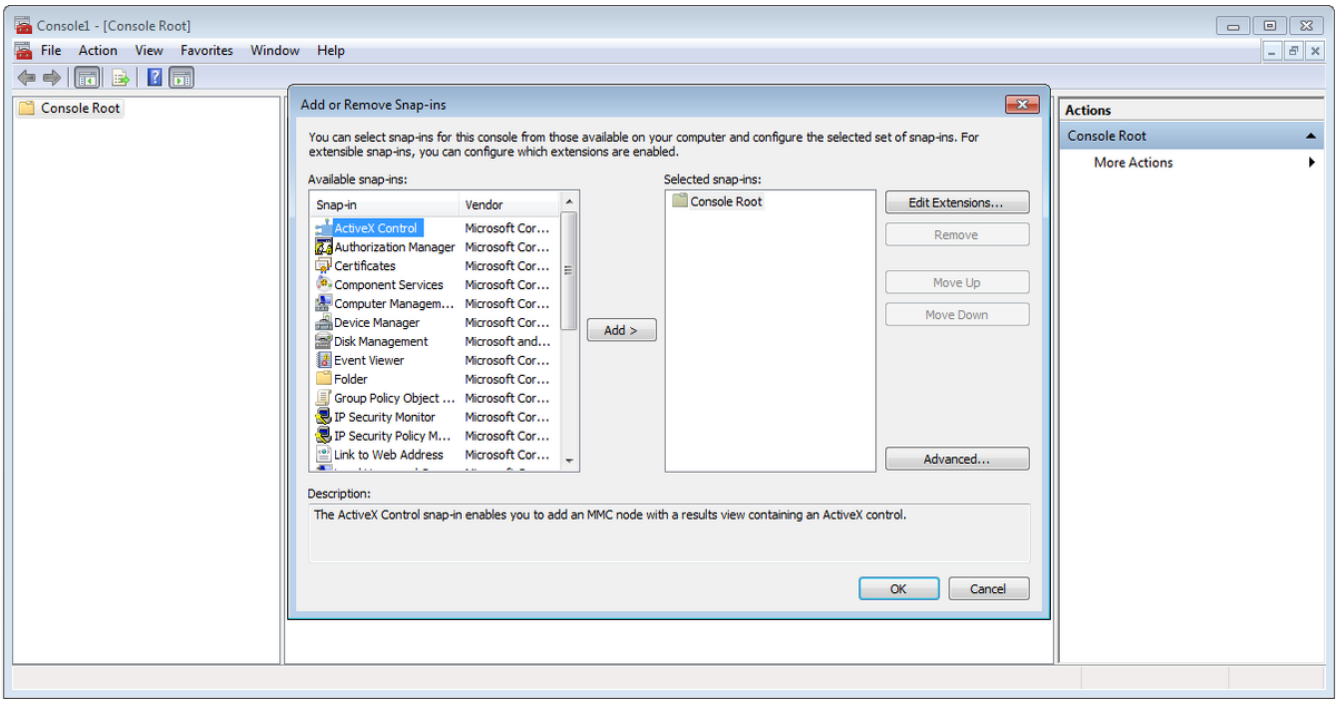
Étape 2. Appuyez sur **Ctrl + R** et tapez **mc** pour ouvrir Microsoft Management Console (MMC).



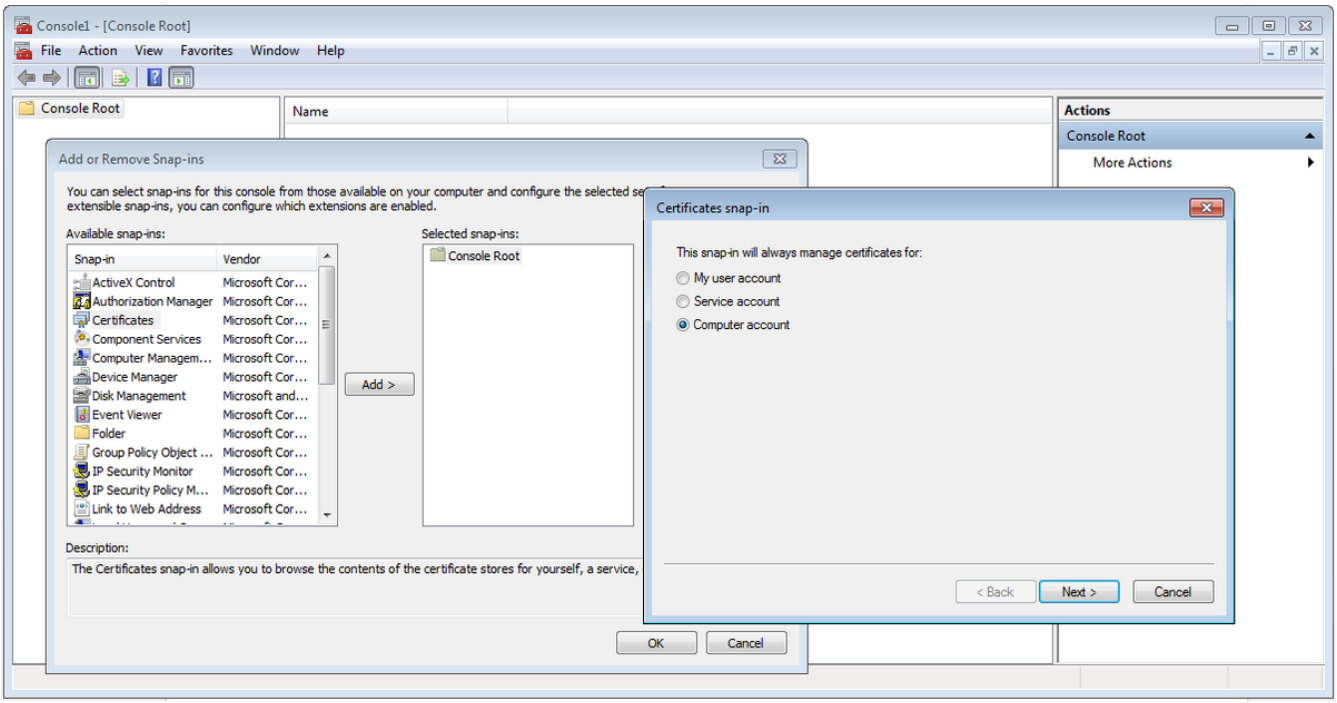
Étape 3. Sélectionnez **OK**.



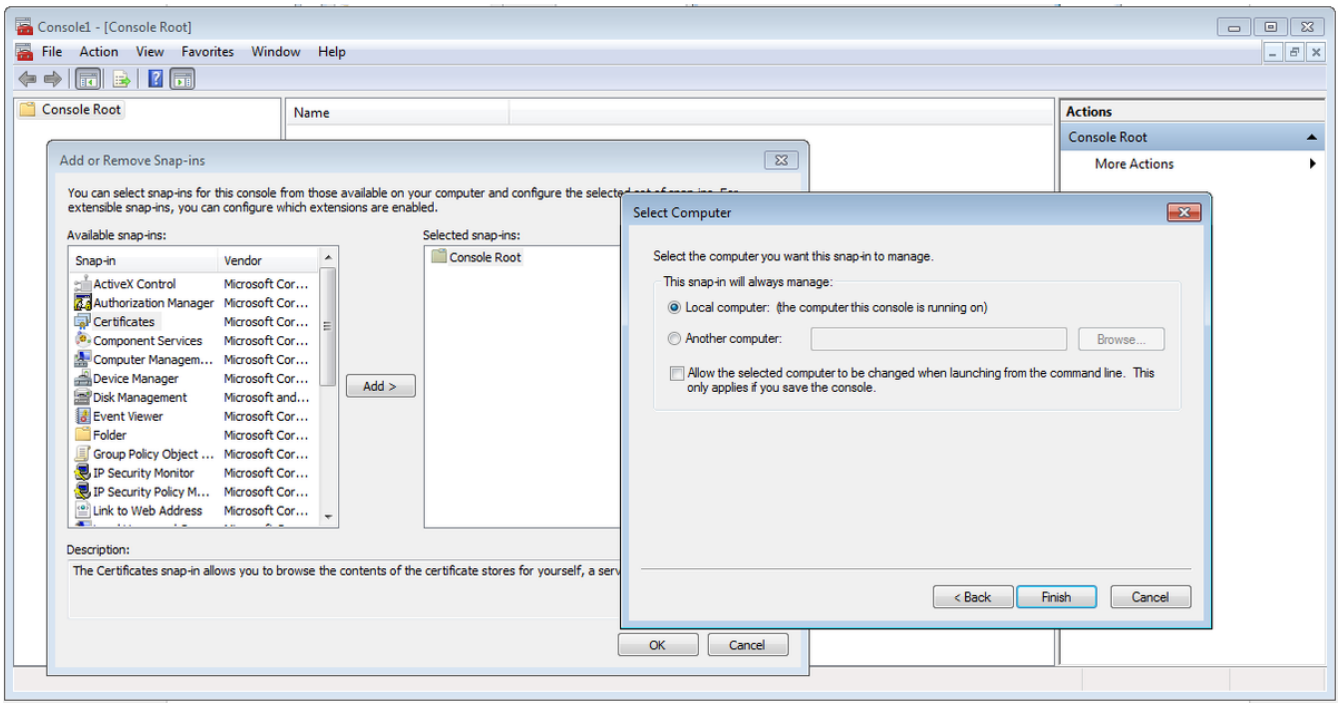
Étape 4. Accédez à **Fichier>Ajouter/Supprimer un composant logiciel enfichable**.



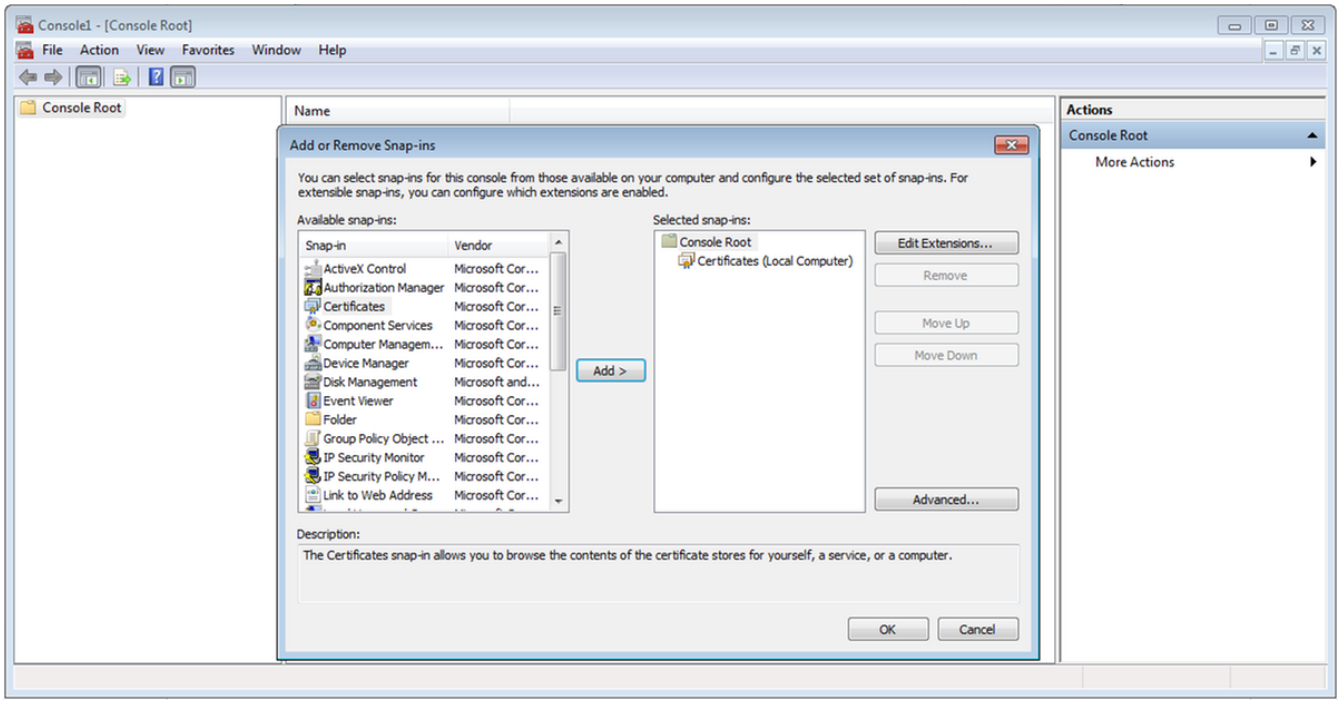
Étape 5. Sélectionnez **Certificats > Ajouter > Compte d'ordinateur**.



Étape 6. Sélectionnez **Suivant**,

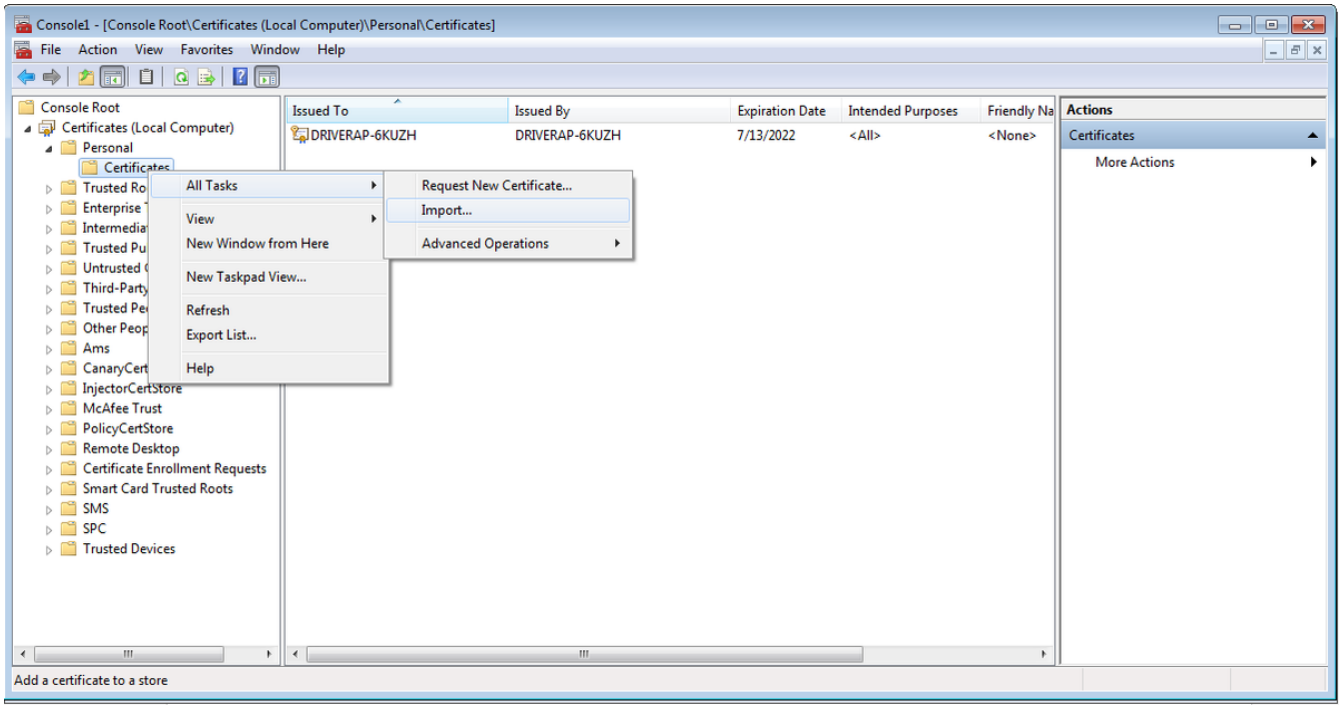


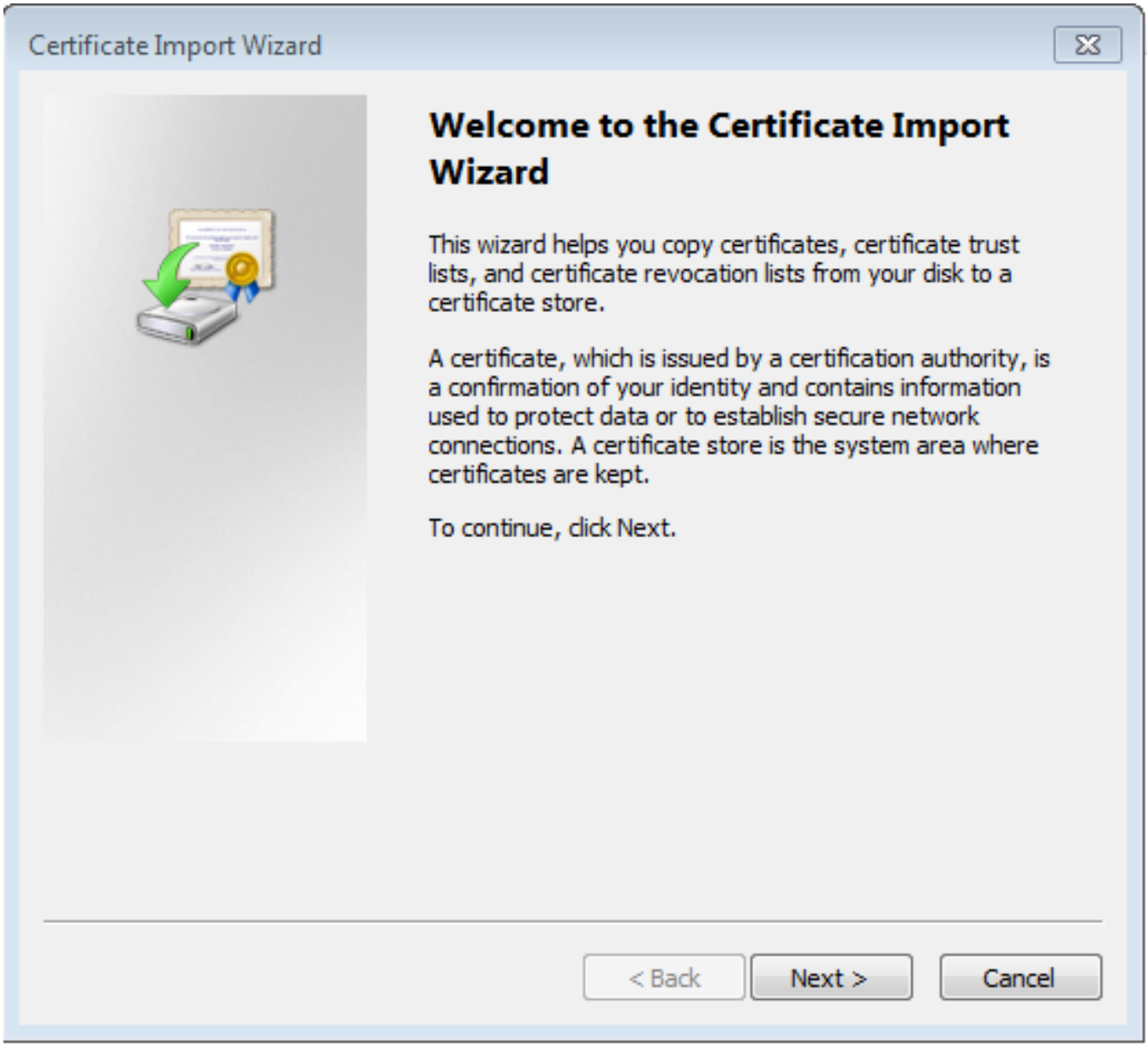
Étape 7. **Terminez**.



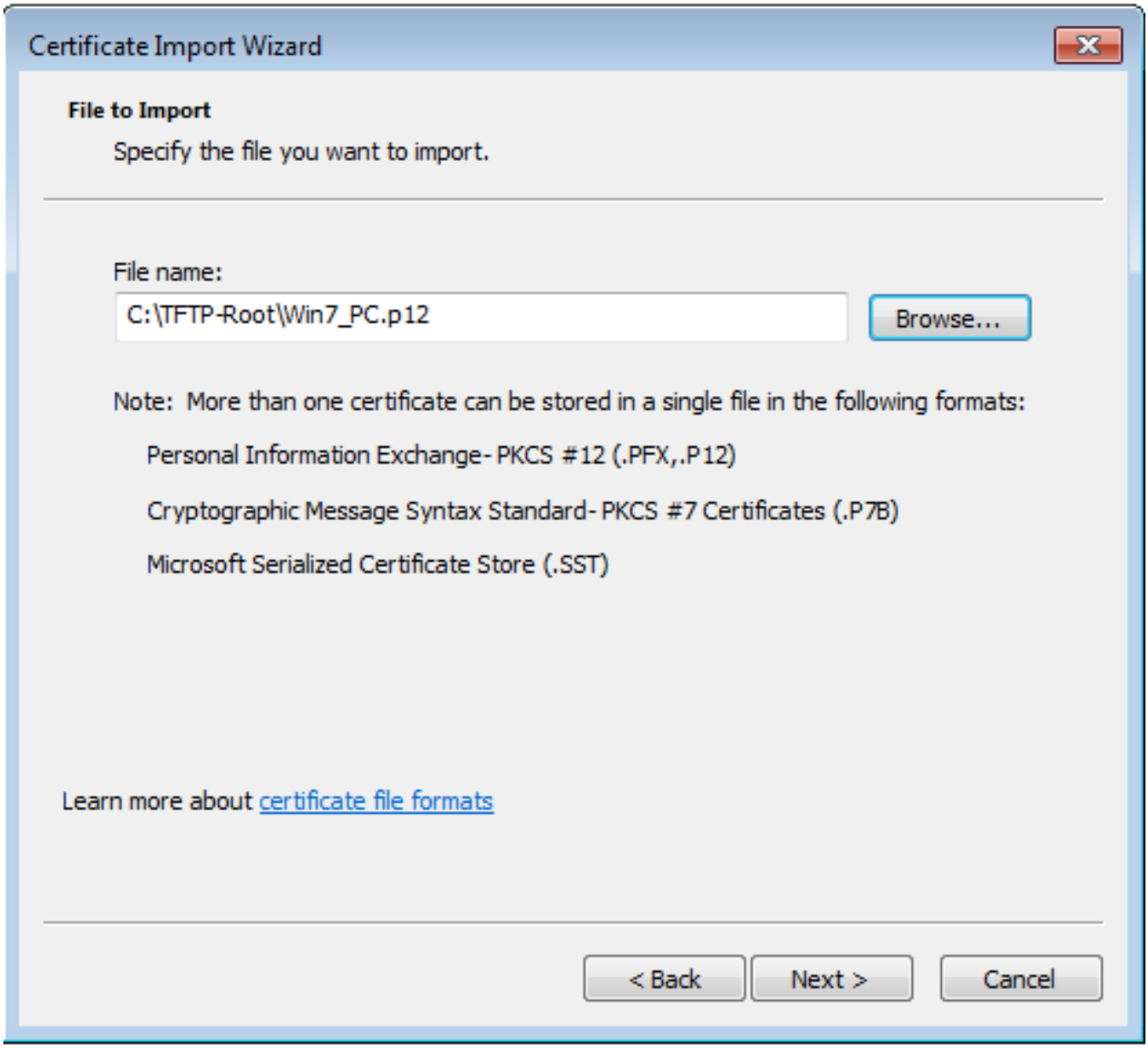
Étape 8. Sélectionnez **OK**.

Étape 9. Accédez à **Certificates (Local Computer)>Personal>Certificates**, cliquez avec le bouton droit sur le dossier et accédez à **All Tasks>Import** :

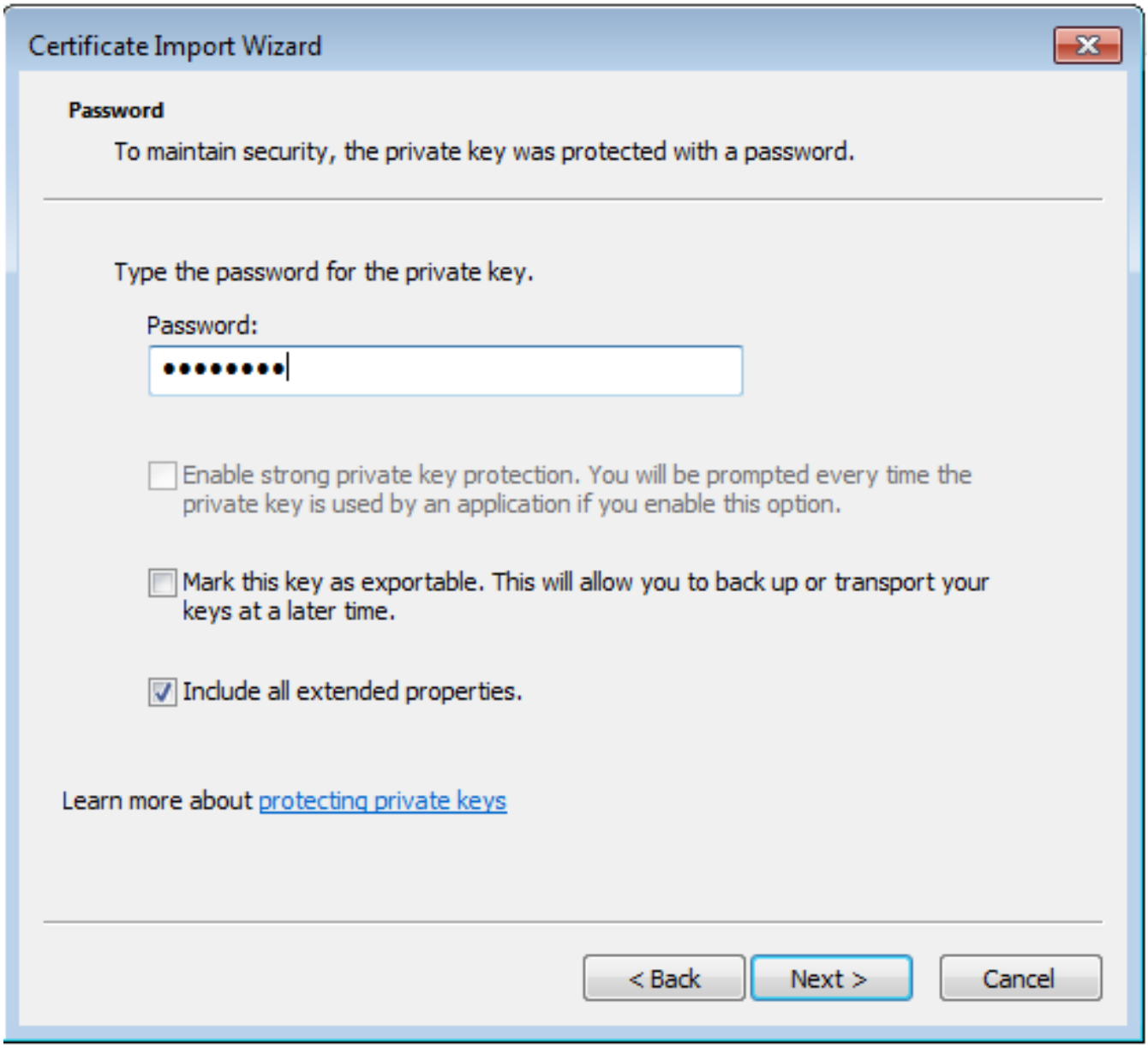




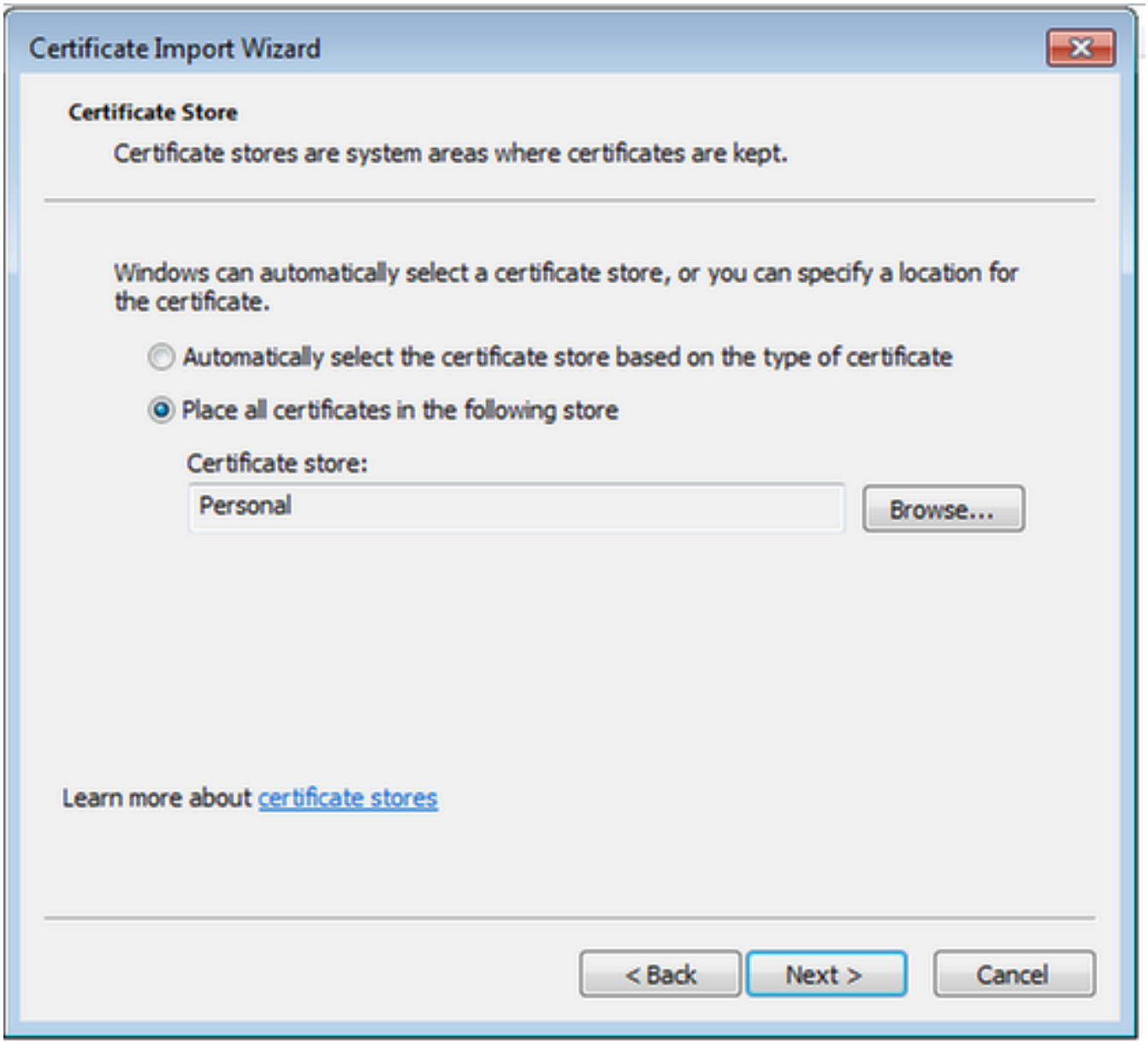
Étape 10. Cliquez sur **Next** (Suivant). Indiquez le chemin d'accès au fichier PKCS12.



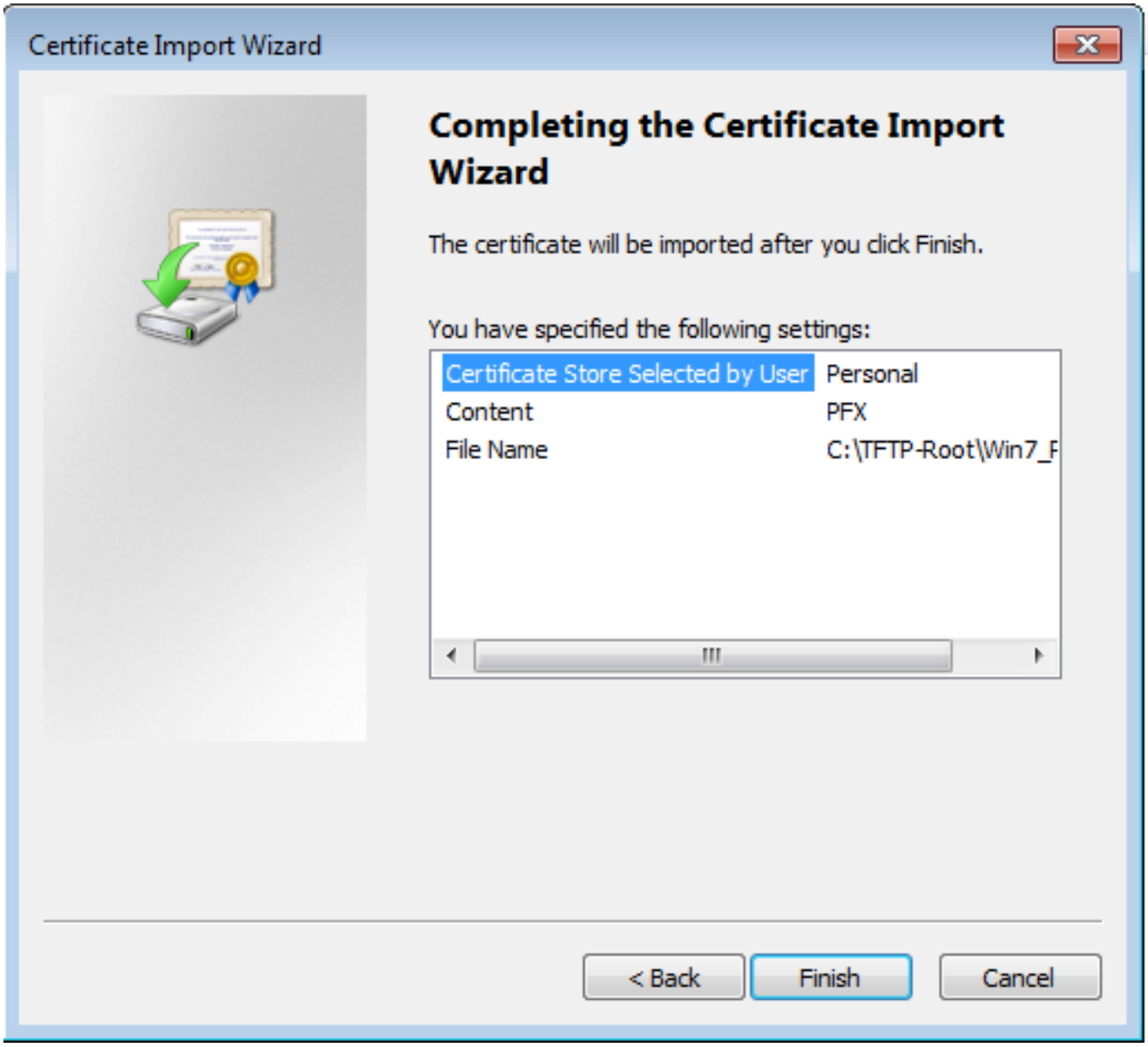
Étape 11. Sélectionnez **Suivant** à nouveau et tapez le mot de passe entré dans la commande *crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>*



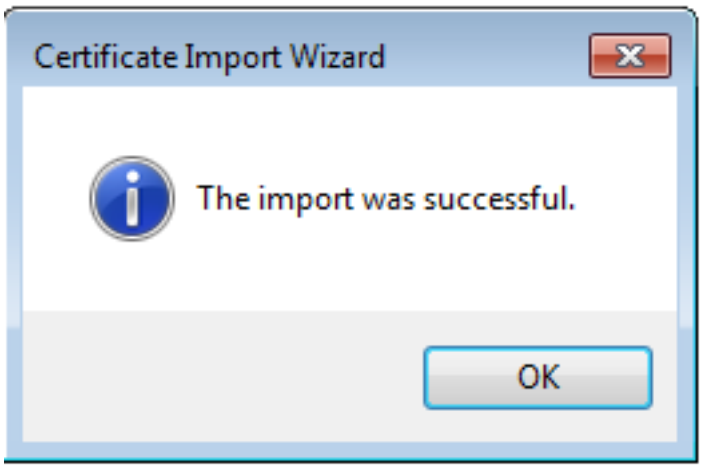
Étape 12. Sélectionnez **Suivant**.



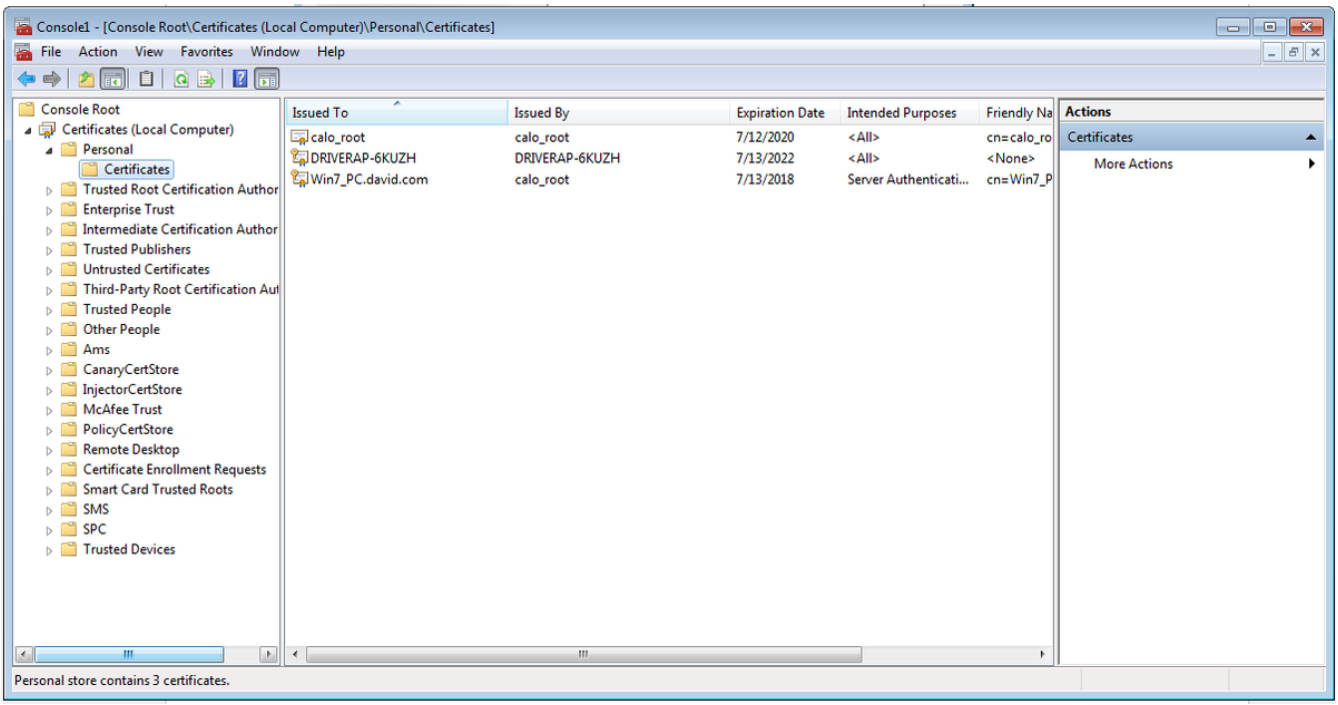
Étape 13. Sélectionnez **Suivant** une fois de plus.



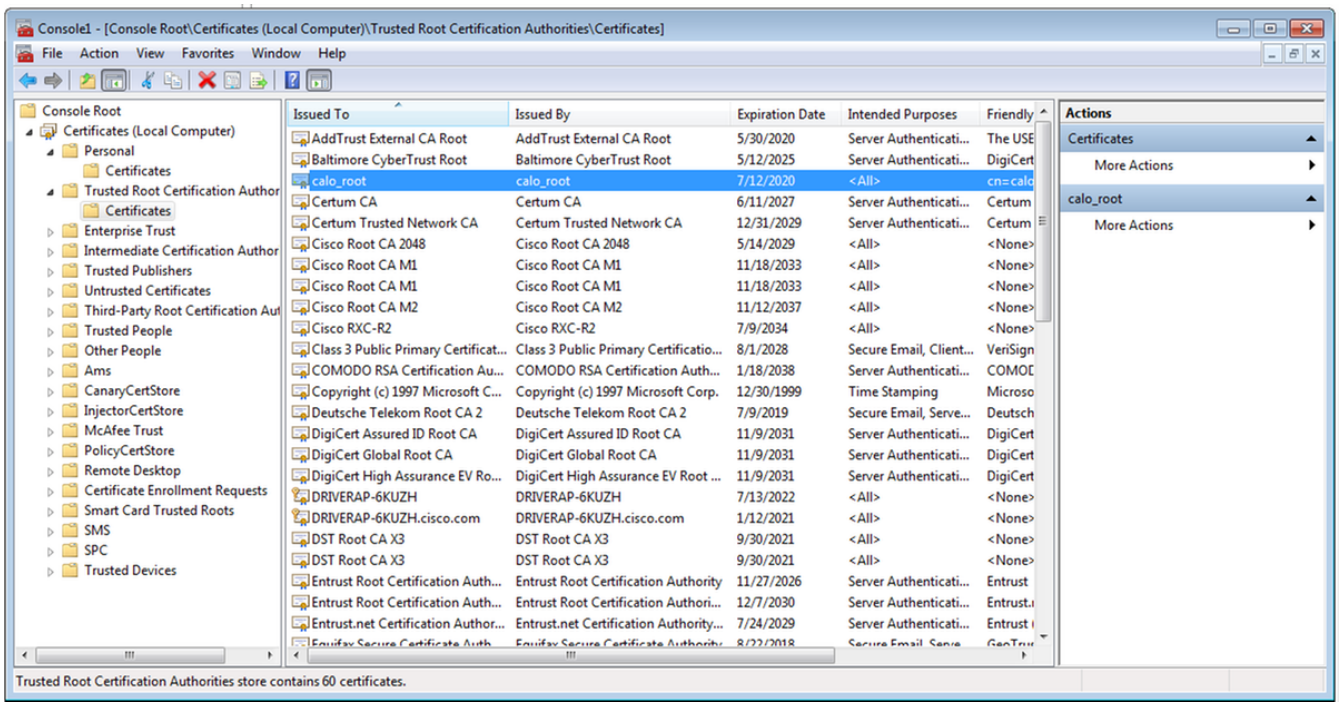
Étape 14. Sélectionnez **Terminer**.

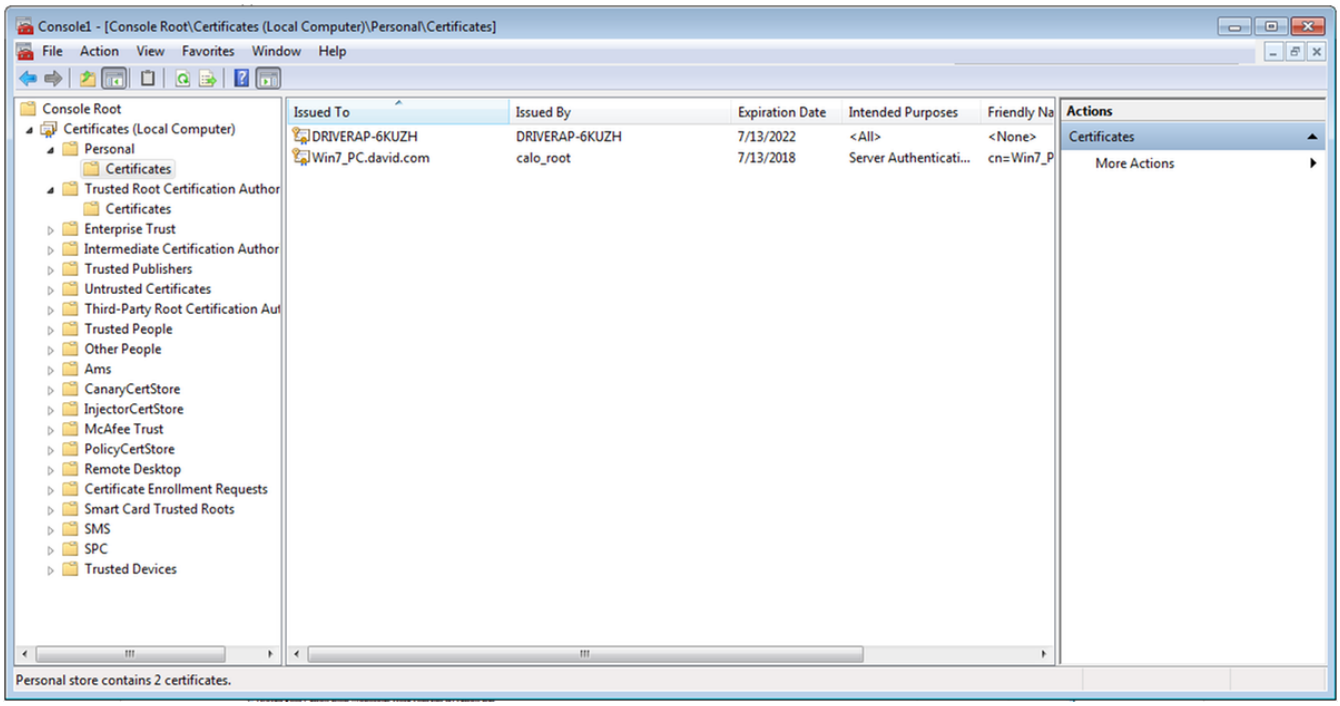


Étape 15. Sélectionnez **OK**. Vous verrez maintenant les certificats installés (le certificat CA et le certificat d'identité).



Étape 16. Faites glisser et déposez le certificat CA à partir de **Certificates (Local Computer)>Personal>Certificates** vers **Certificates (Local Computer)>Trusted Root Certification Authority>Certificates.**



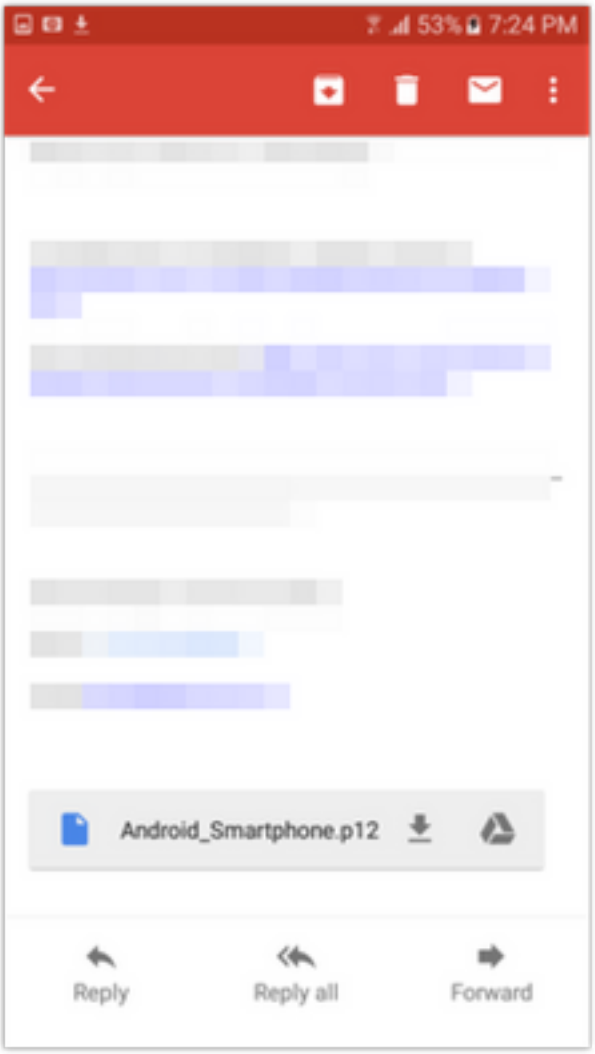


Comment installer le certificat d'identité sur votre appareil mobile Android

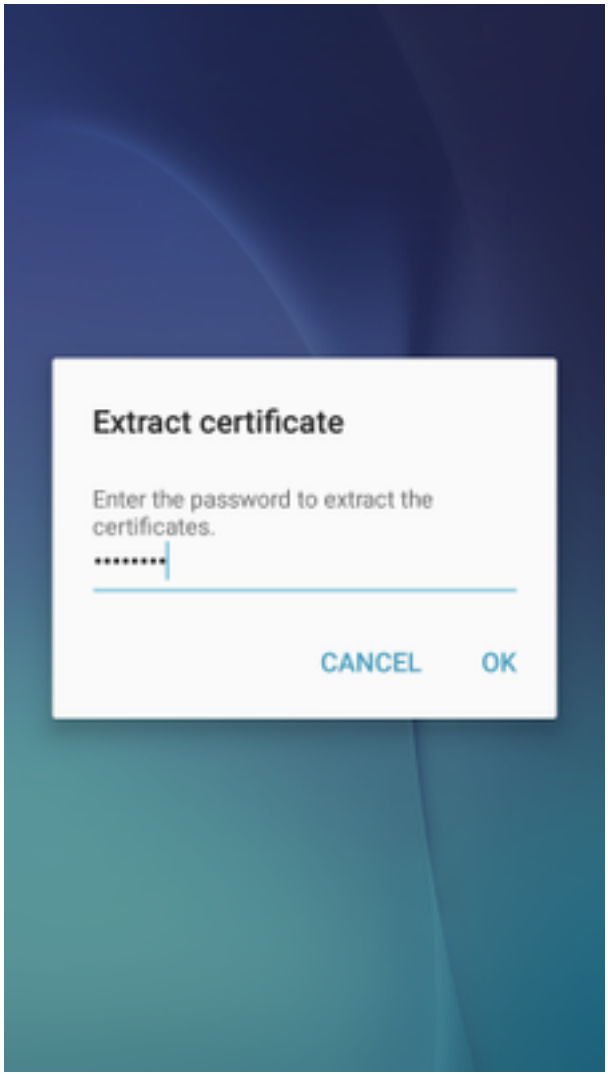
Note: Android prend en charge les fichiers de magasin de clés PKCS#12 avec l'extension .pfx ou .p12.

Note: Android prend uniquement en charge les certificats SSL X.509 encodés en DER.

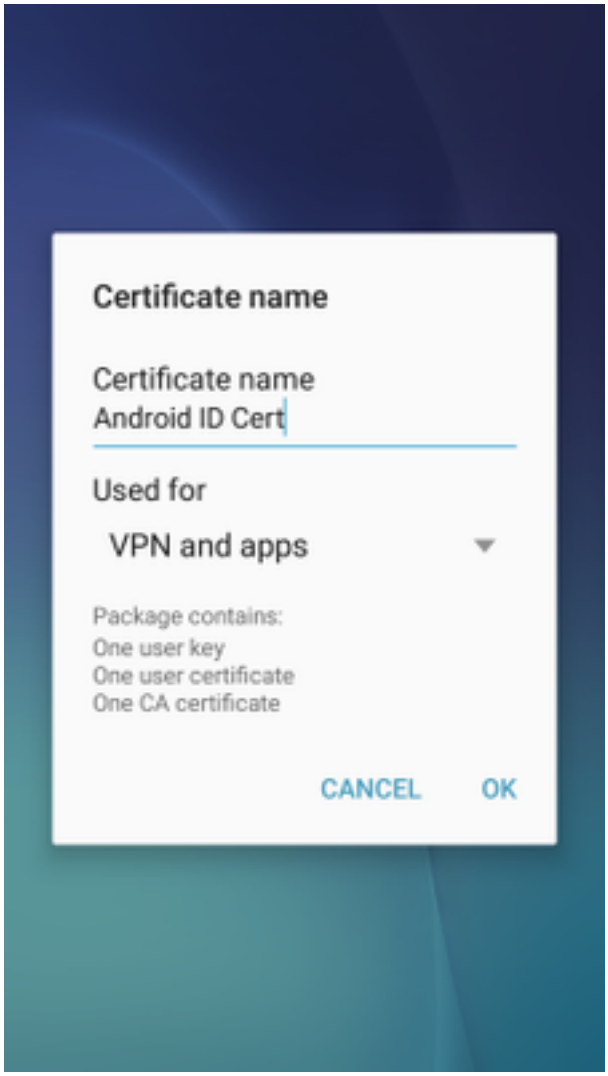
Étape 1. Après l'exportation du certificat client à partir du serveur AC IOS au format PKCS12 (.p12), envoyez le fichier au périphérique Android par e-mail. Une fois que vous l'avez, effleurez le nom du fichier pour démarrer l'installation automatique. (**Ne pas télécharger le fichier**)



Étape 2. Entrez le mot de passe utilisé pour exporter le certificat, dans cet exemple, le mot de passe est **cisco123**.

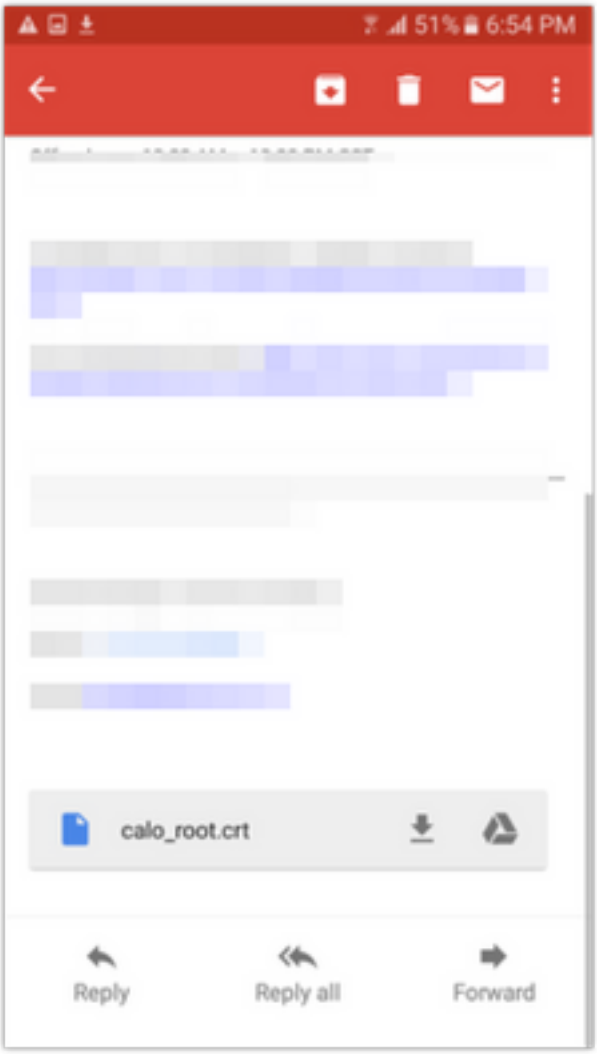


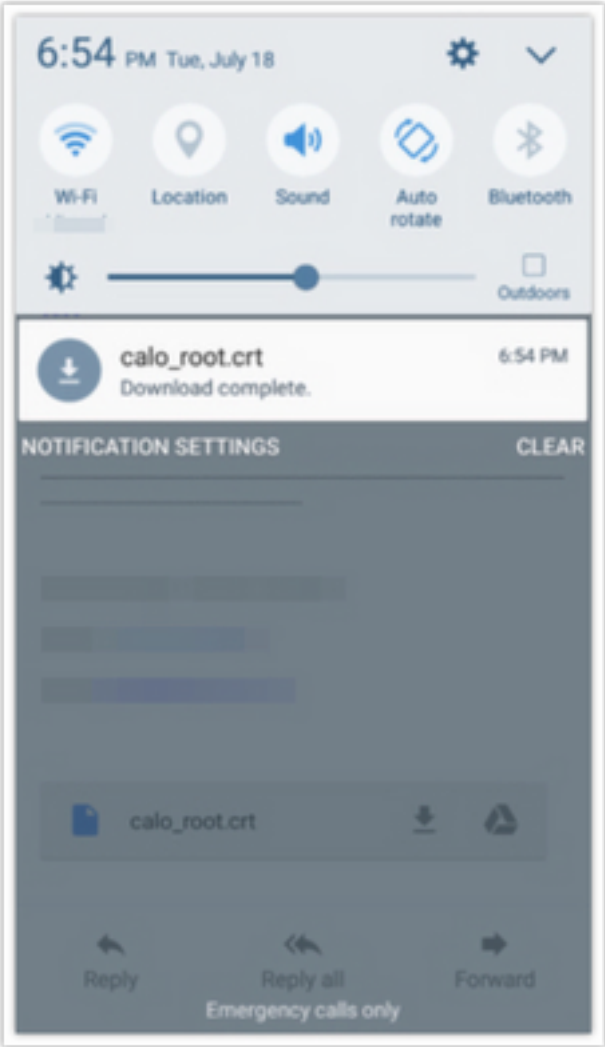
Étape 3. Sélectionnez **OK** et saisissez un **nom de certificat**. Il peut s'agir de n'importe quel mot, dans cet exemple, le nom est **Android ID Cert** .



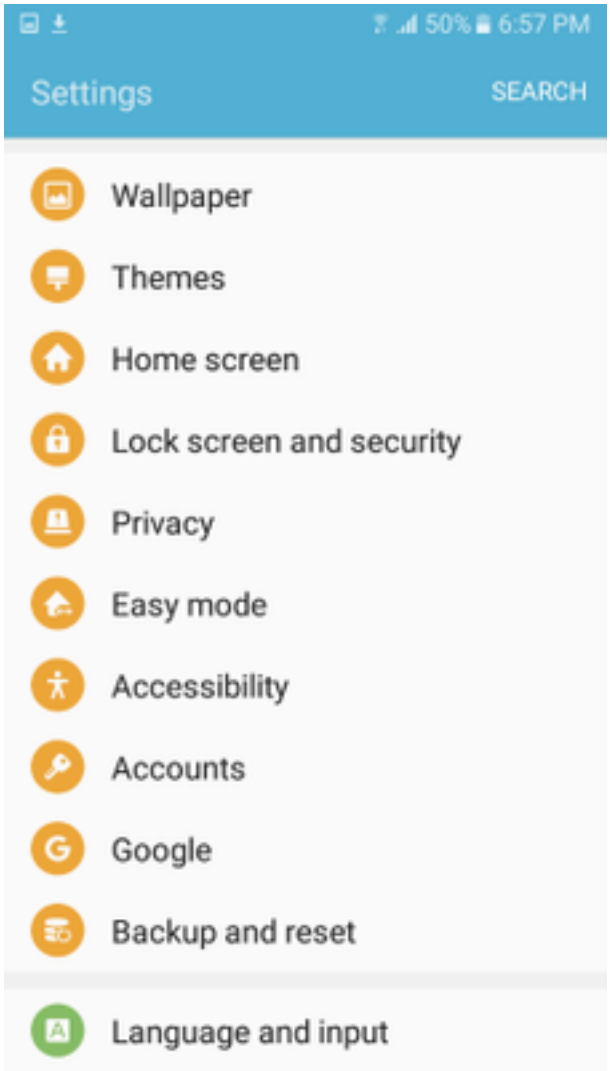
Étape 4. Sélectionnez **OK** et le message “ Android ID Cert installé ” s'affiche.

Étape 5. Afin d'installer le certificat d'autorité de certification, extrayez-le du serveur d'autorité de certification IOS au format base64 et enregistrez-le avec l'extension .crt. Envoyez le fichier à votre périphérique android par e-mail. Cette fois, vous devez télécharger le fichier en tapant sur la flèche située en regard du nom du fichier.


51% 6:54 PM
calo_root.crt
Reply
Reply all
Forward

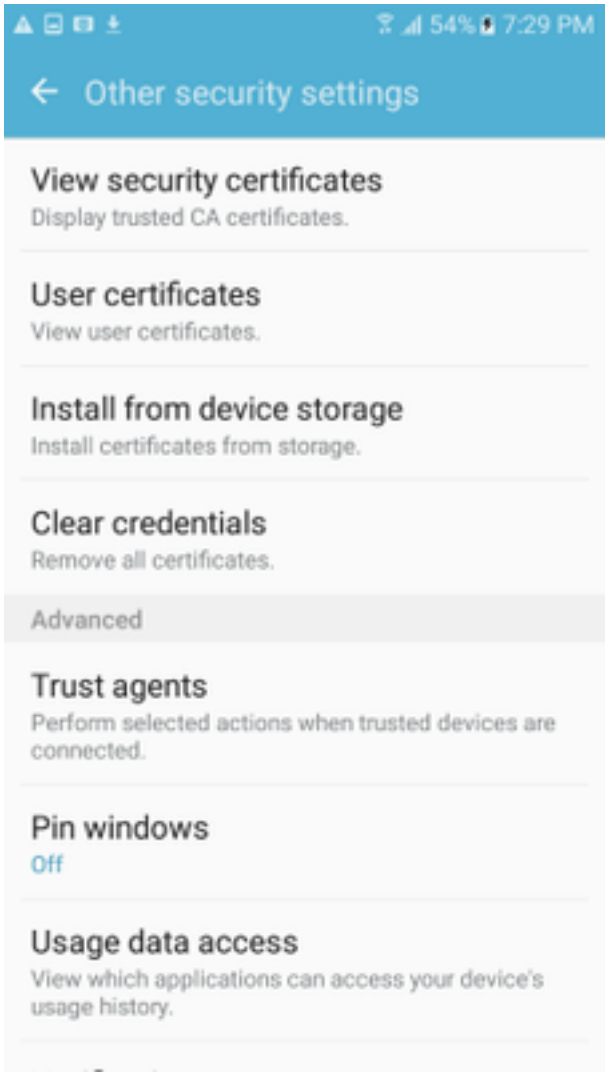


Étape 6. Accédez à **Paramètres** et **Verrouillage, écran et sécurité.**

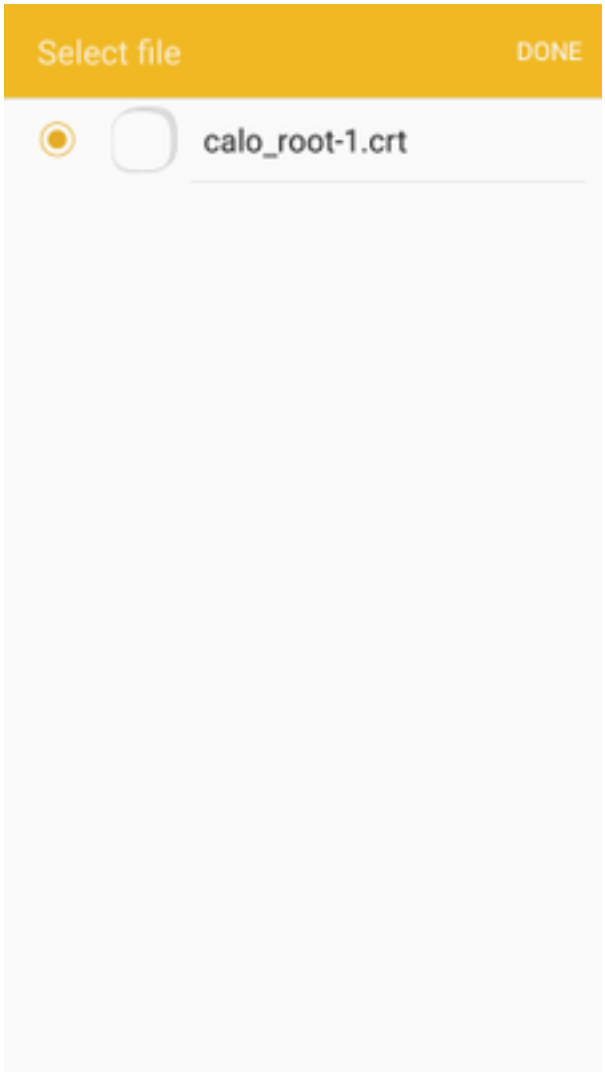


Étape 7. Sélectionnez **Autres paramètres de sécurité.**

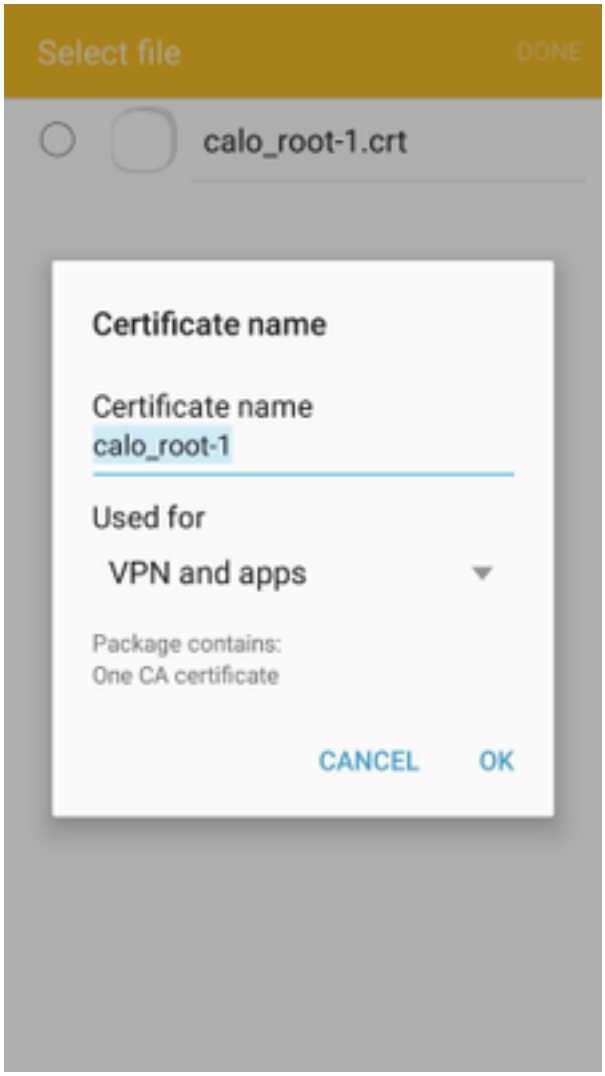
Étape 8. Accédez à **Installer à partir du stockage de périphérique.**



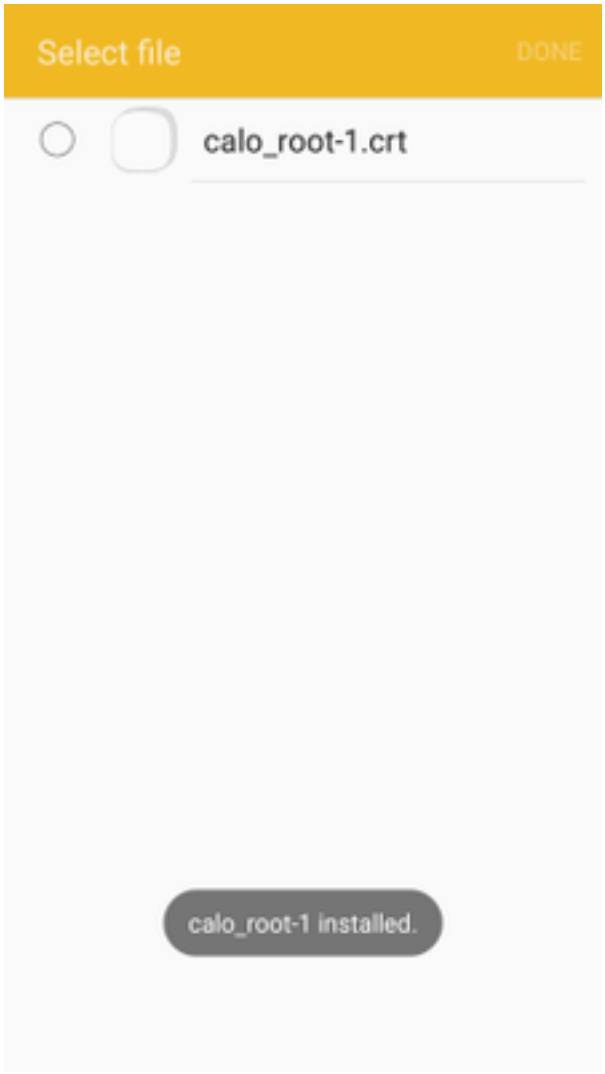
Étape 9. Sélectionnez le fichier .crt et appuyez sur **Terminé.**



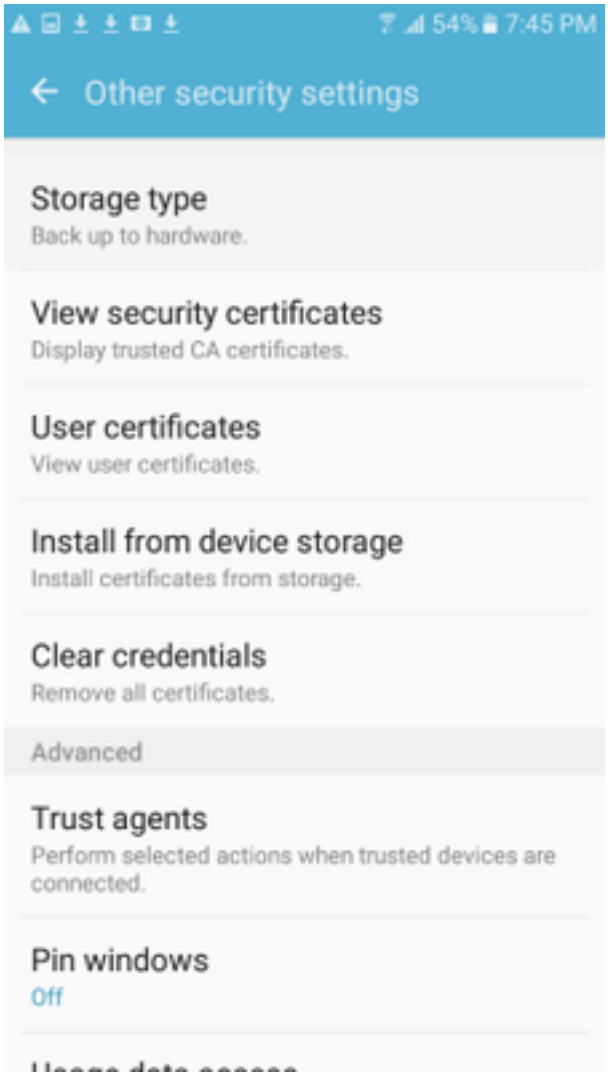
Étape 10. Entrez un **nom de certificat**. Il peut s'agir de n'importe quel mot, dans cet exemple, le nom est **calo_root-1**.



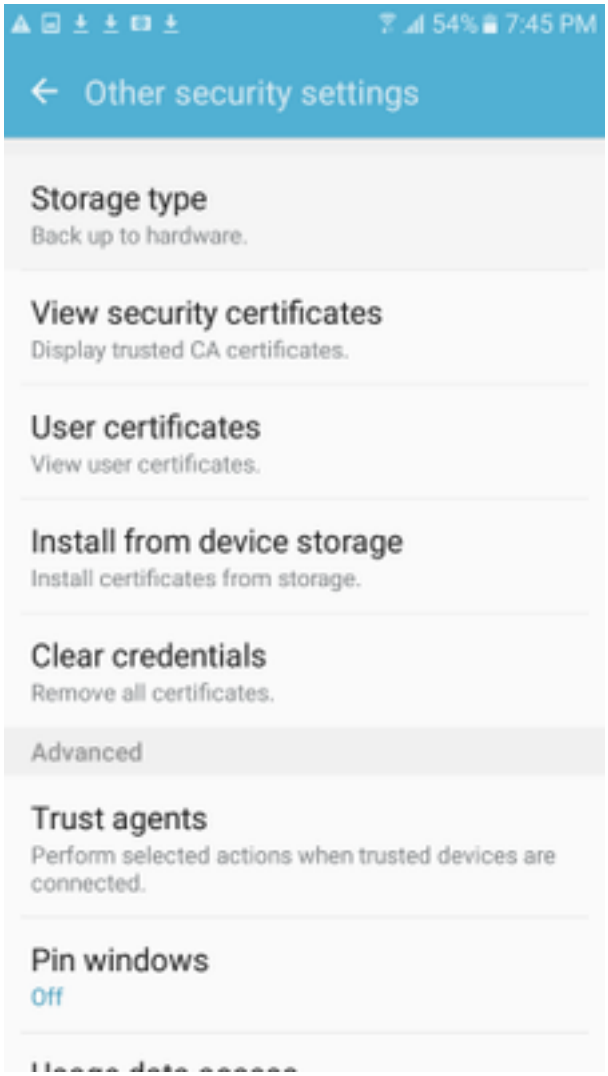
Étape 10. Sélectionnez **OK** et vous verrez le message “ calo_root-1 ” installé.



Étape 11. Afin de vérifier que le certificat d'identité est installé, accédez à **Paramètres/Verrouiller l'écran et Sécurité/Autre > Paramètres de sécurité/Certificats d'utilisateur/onglet Système.**


54% 7:45 PM
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

Étape 12. Pour vérifier que le certificat d'autorité de certification est installé, accédez à **Paramètres/Verrouiller l'écran et sécurité/Autres paramètres de sécurité/Afficher les certificats de sécurité/onglet Utilisateur.**


54% 7:45 PM
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

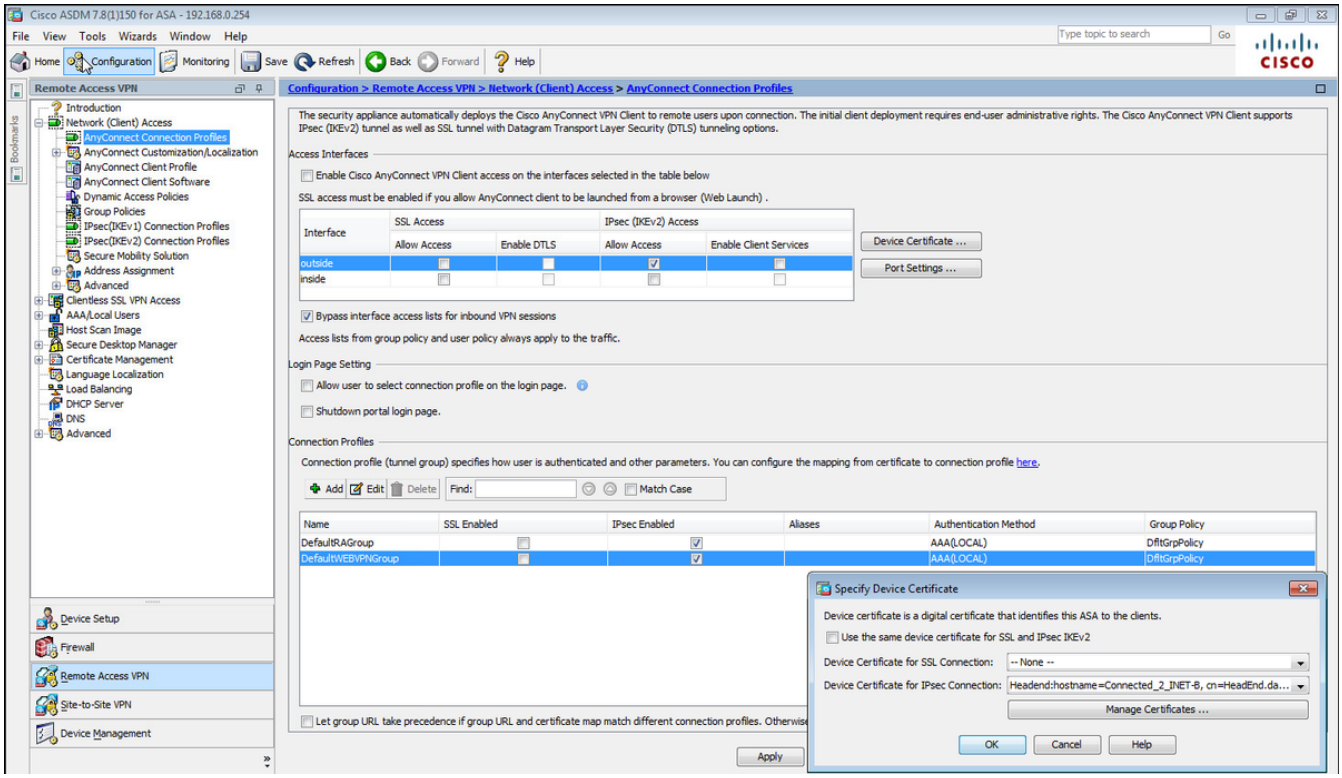
Configurer la tête de réseau ASA pour RA VPN avec IKEv2

Étape 1. Sur ASDM, accédez à **Configuration>Remote Access VPN > Network (client) Access> Anyconnect Connection Profiles**. Cochez la case **Accès IPSec (IKEv2), Autoriser l'accès** sur l'interface faisant face aux clients VPN (l'option **Activer les services client** n'est pas nécessaire).

Étape 2. Sélectionnez **Device Certificate** et supprimez la coche **Use the same device certificate for SSL and IPSec IKEv2**.

Étape 3. Sélectionnez le certificat de tête de réseau pour la connexion IPSec et sélectionnez Aucun pour la connexion SSL.

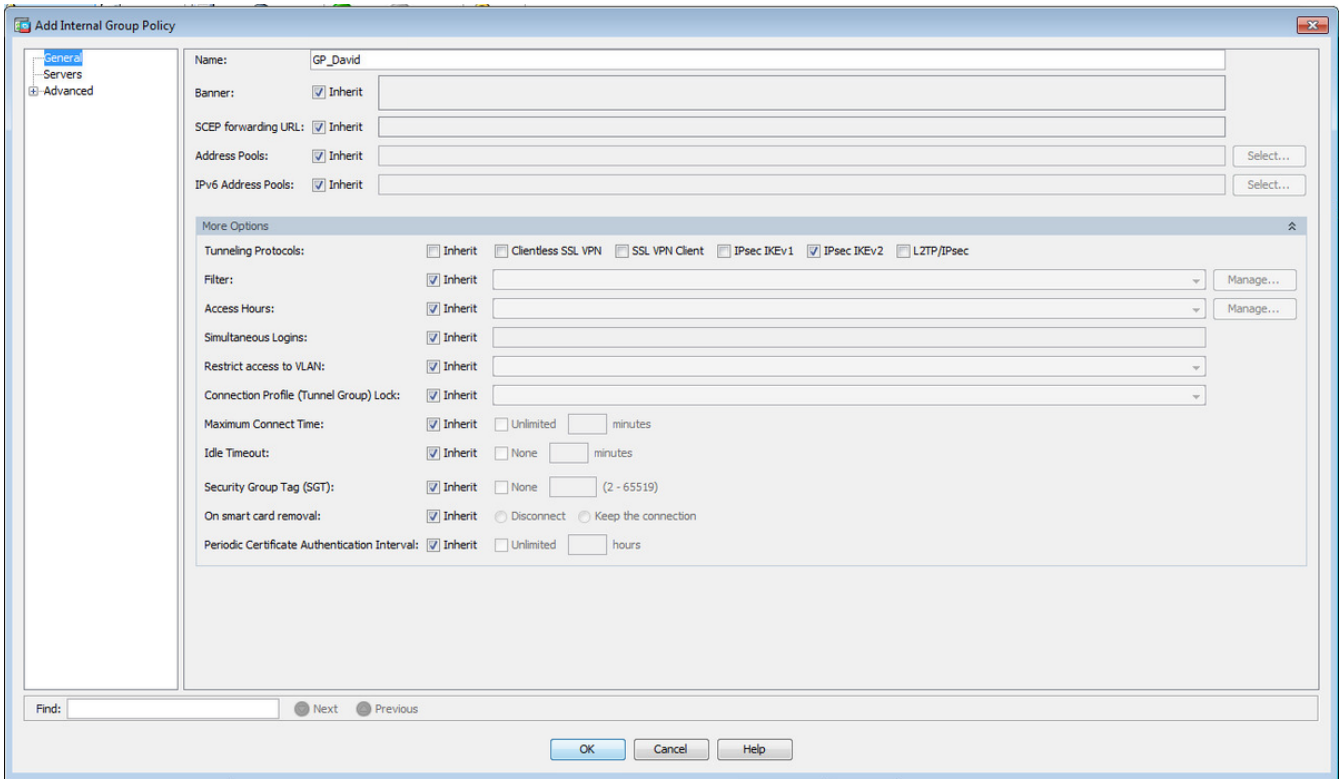
Cette option place la crypto ikev2, crypto ipsec, crypto dynamic-map et la configuration crypto map.



Voici l'aspect de la configuration sur l'interface de ligne de commande (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
```

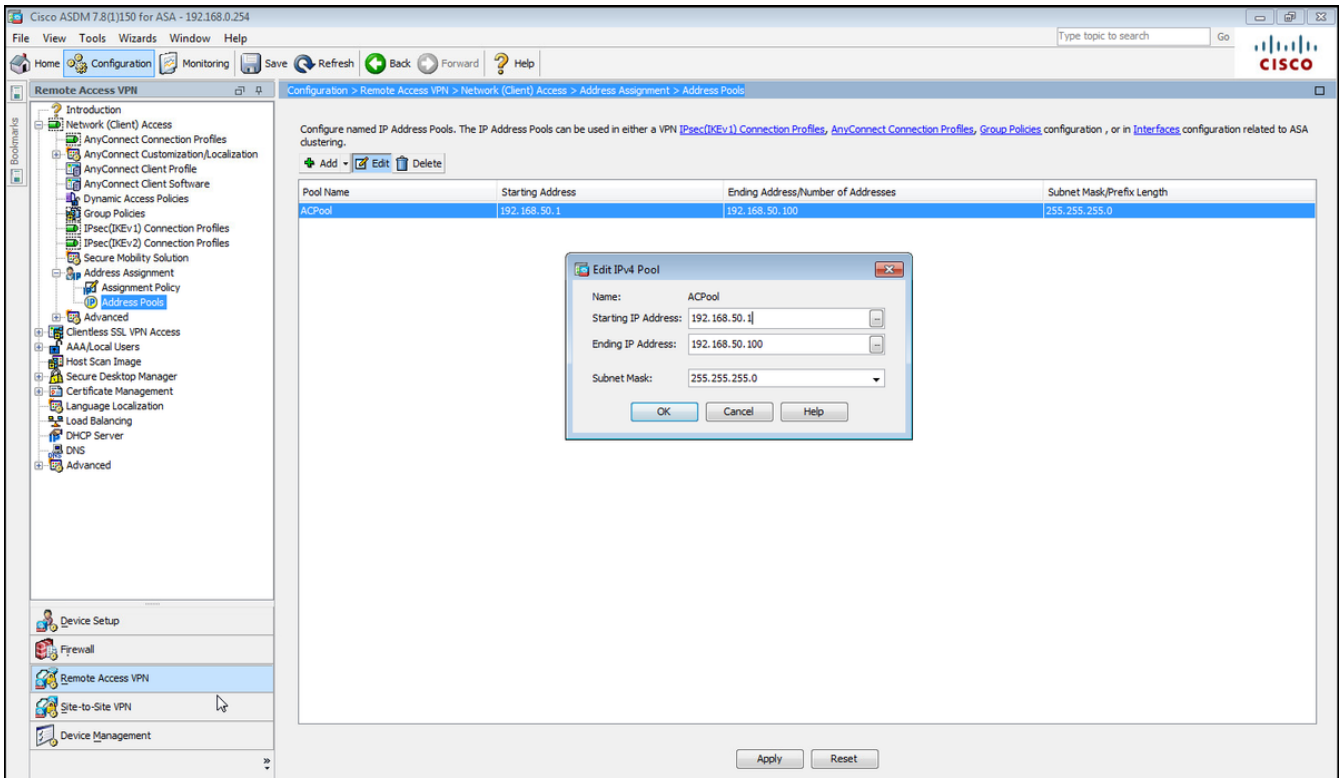
Étape 4. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** pour créer une stratégie de groupe



Sur CLI.

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

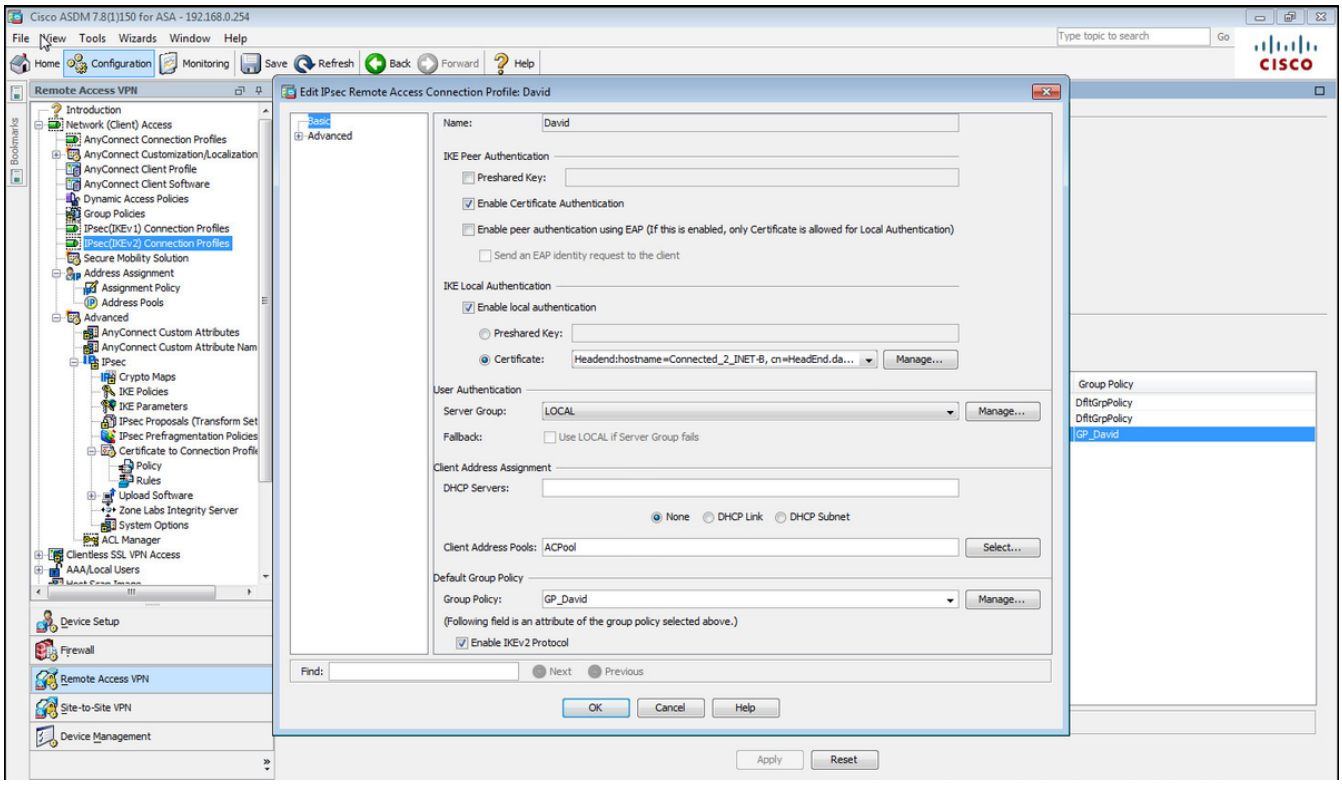
Étape 5. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Address Pools** et sélectionnez **Add** pour créer un pool IPv4.



Sur CLI.

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

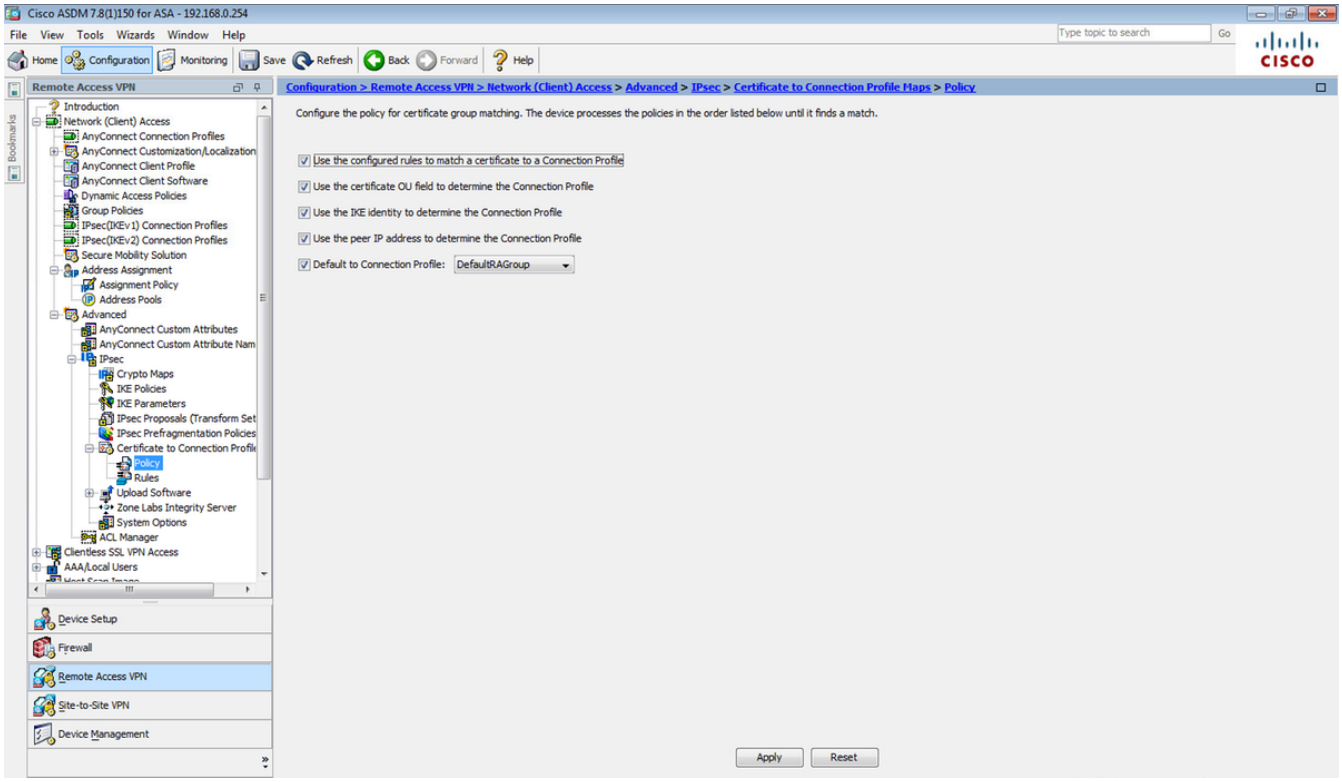
Étape 6. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles** et sélectionnez **Add** pour créer un nouveau groupe de tunnels.



Sur 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
```

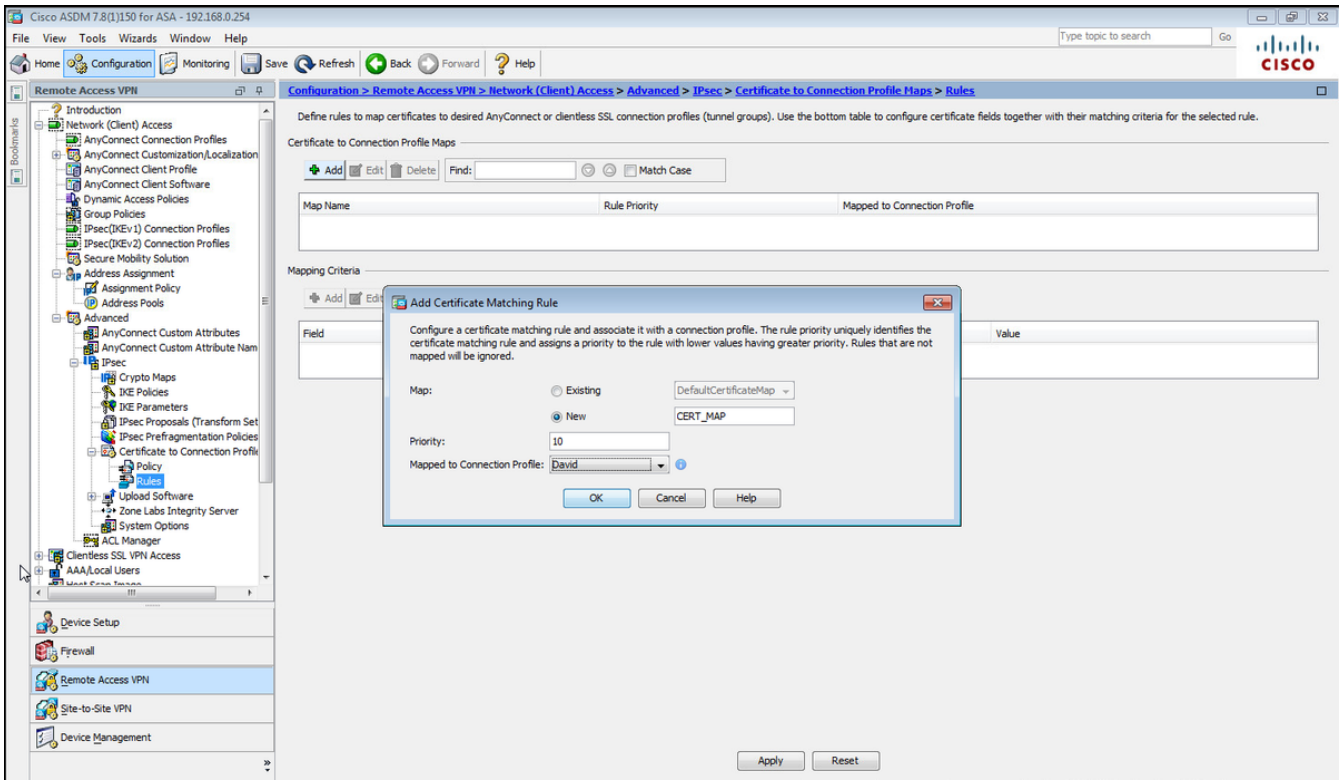
Étape 7. Naviguez jusqu'à **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy** et cochez la case **Used the configure rules to math a certificate to a Connection Profile**.



Sur CLI.

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

Étape 8. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules** et créez une nouvelle carte de certificat. Sélectionnez **Ajouter** et associez-le au groupe de tunnels. Dans cet exemple, le groupe de tunnels est nommé **David**.



Sur CLI.

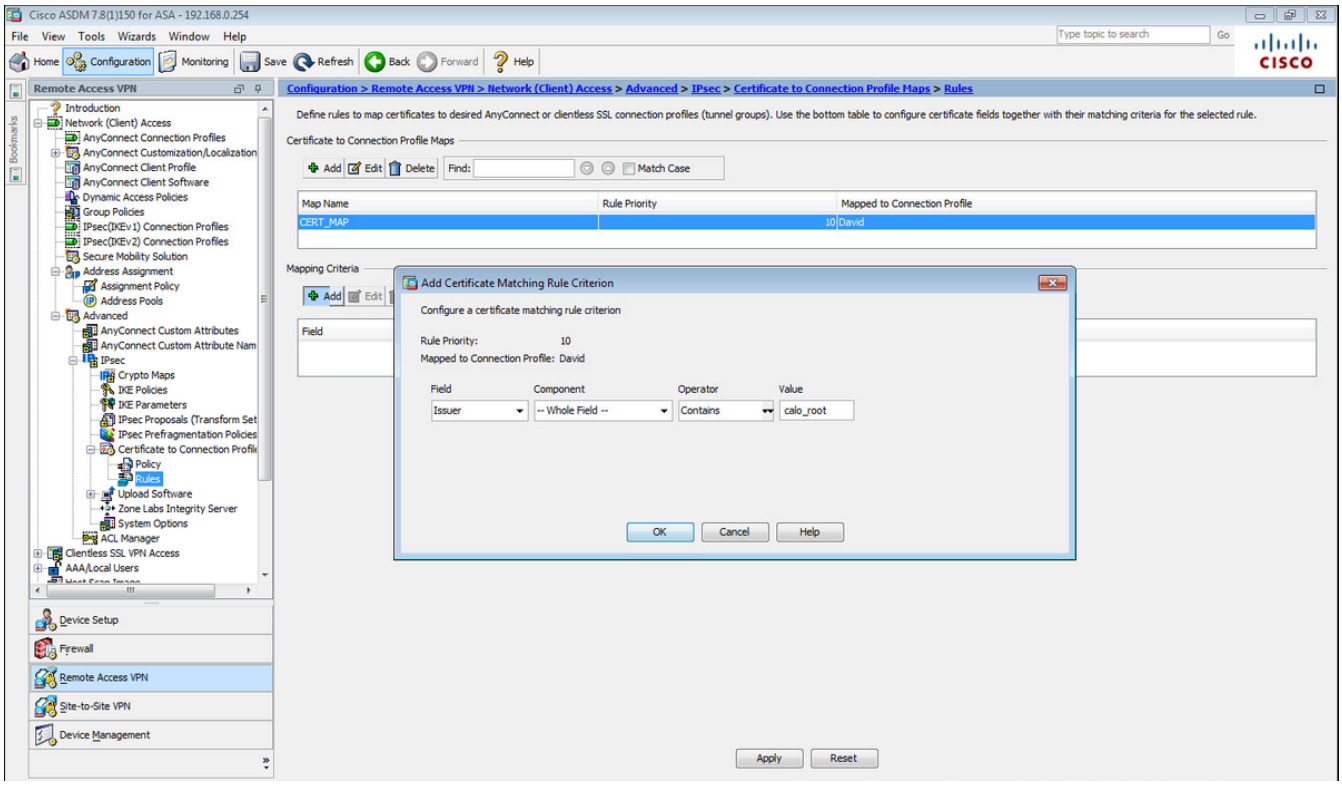
```
tunnel-group-map CERT_MAP 10 David
```

Étape 9. Sélectionnez **Ajouter** dans la section **Critères de mappage** et entrez ces valeurs.

Champ: Émetteur

Opérateur : Contient

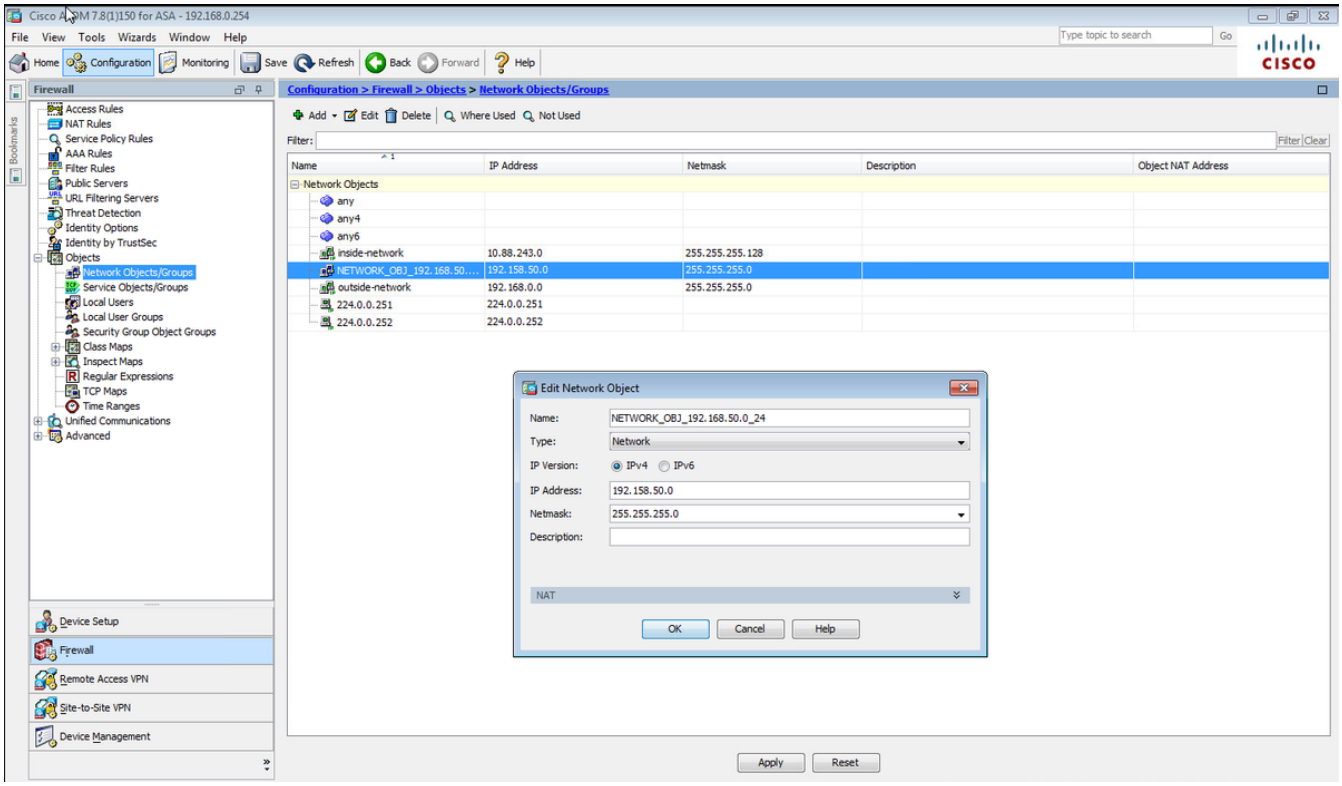
Valeur: racine_calo



Sur CLI.

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

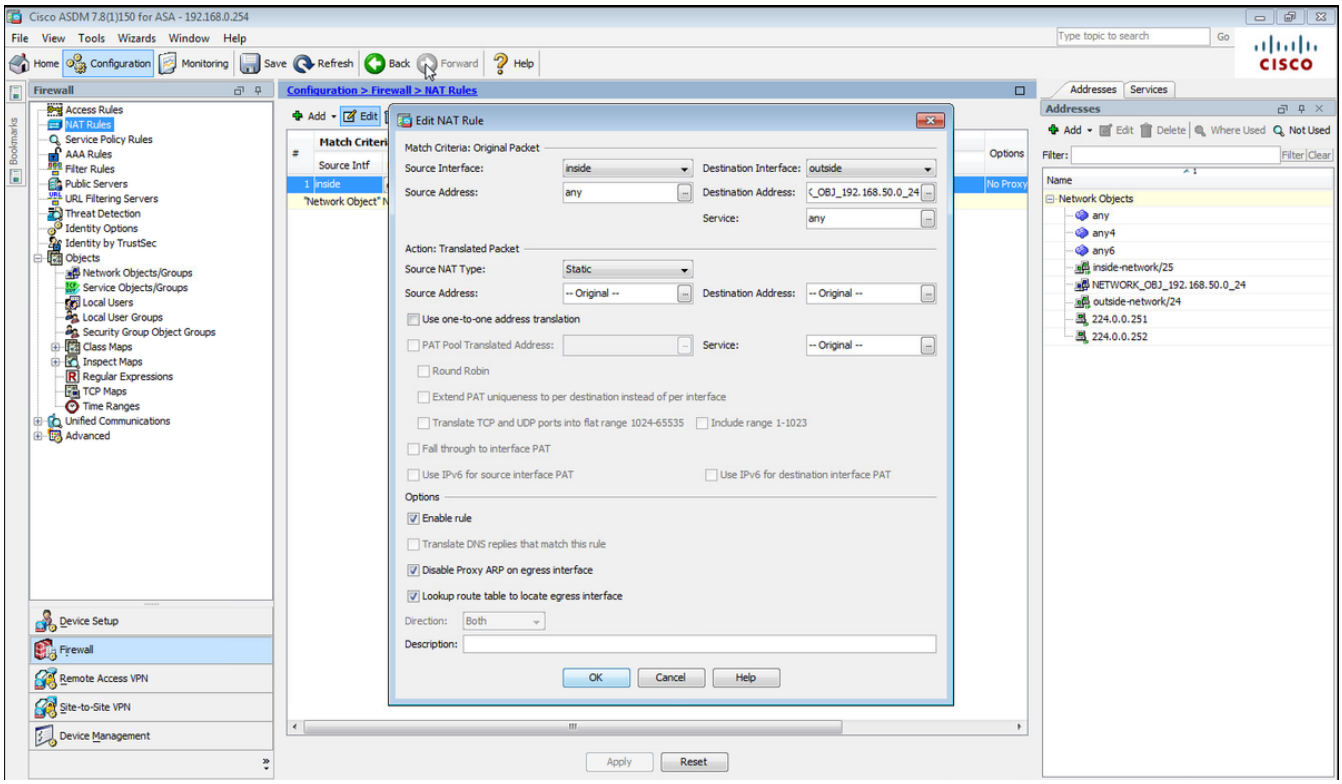
Étape 10. Créez un objet avec le réseau du pool d'adresses IP à utiliser afin d'ajouter une règle d'exemption NAT (Traduction d'adresses réseau) à **Configuration > Firewall > Objects > Network Objects/Groups> Add**.



Sur CLI.

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

Étape 11. Accédez à **Configuration > Firewall > NAT Rules** et sélectionnez **Add** pour créer la règle d'exemption NAT pour le trafic VPN RA.



Sur CLI.

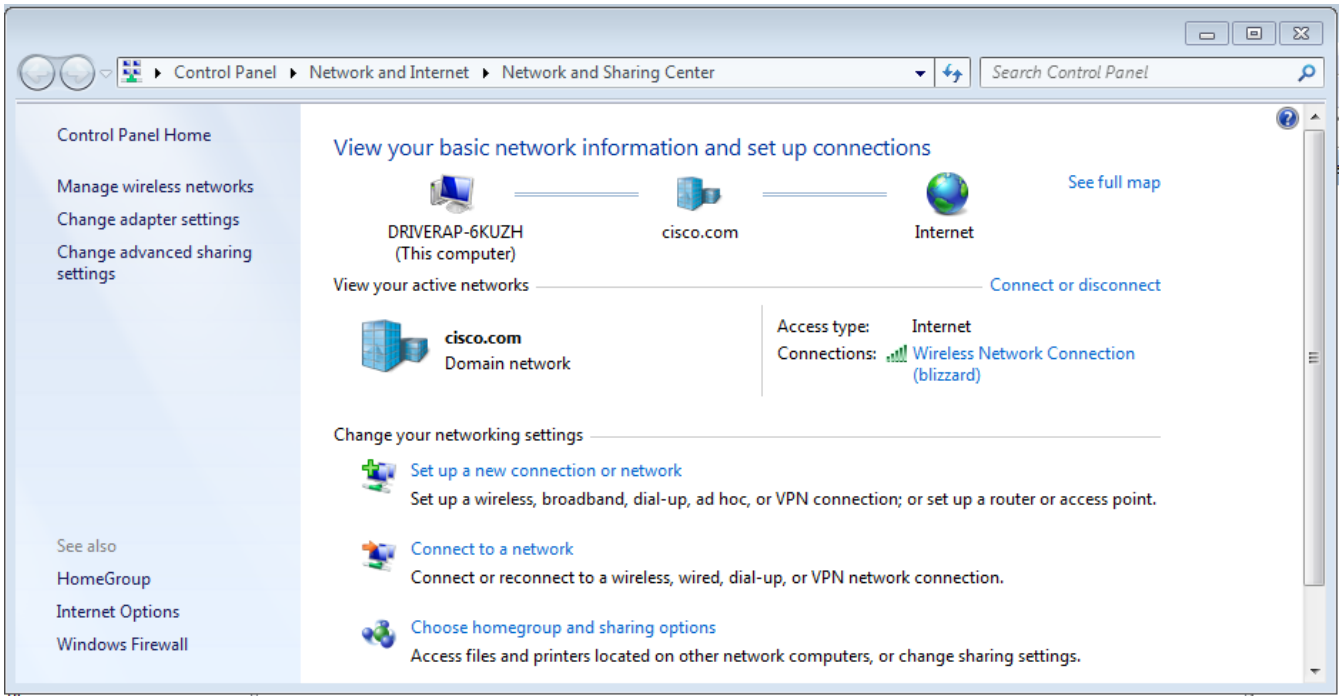
```
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup
```

Il s'agit de la configuration ASA complète utilisée pour cet exemple.

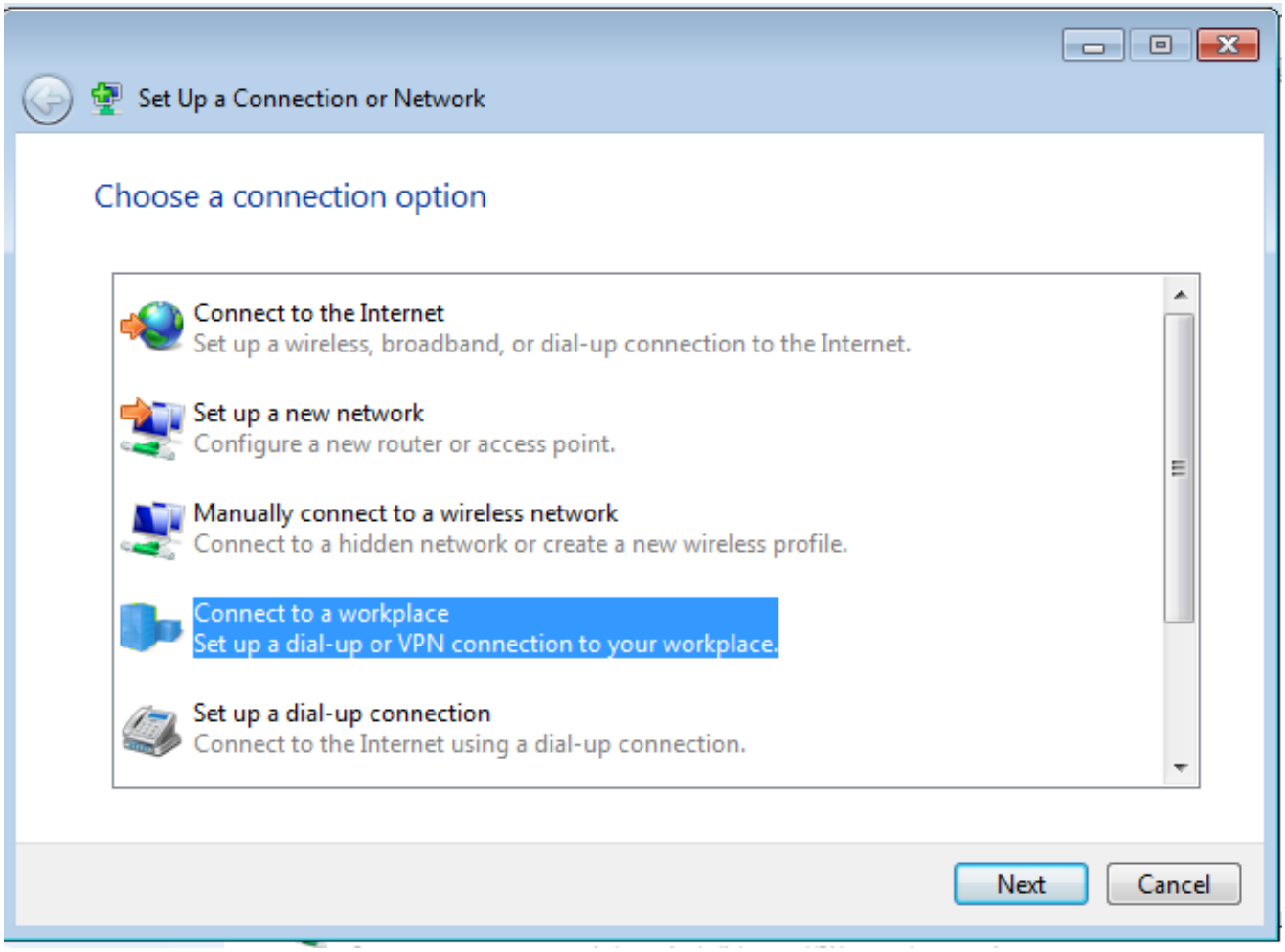
```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.88.243.108 255.255.255.128

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
```

Configurer le client intégré de Windows 7

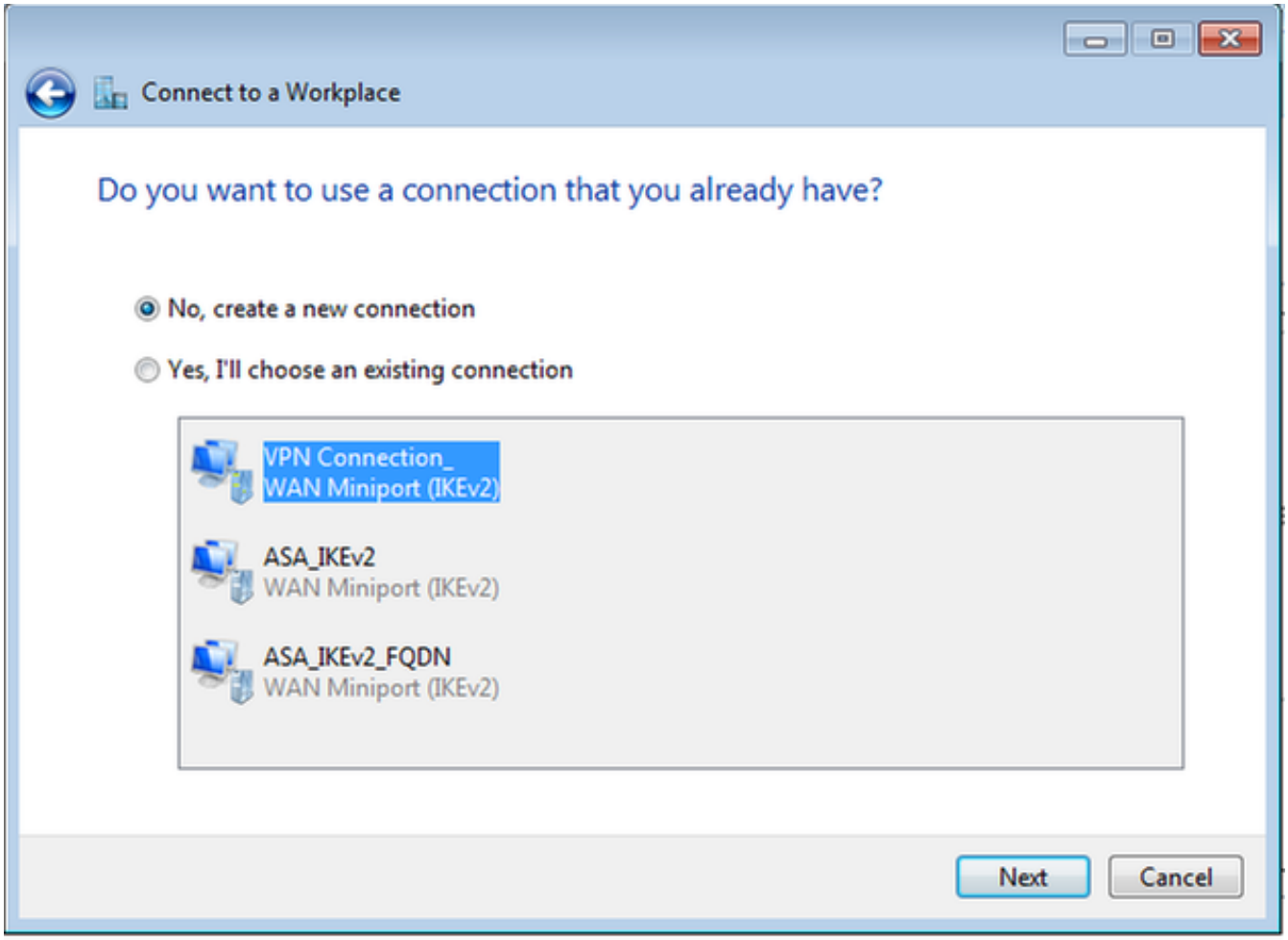
Étape 1. Accédez à **Panneau de configuration > Réseau et Internet > Centre Réseau et partage**.



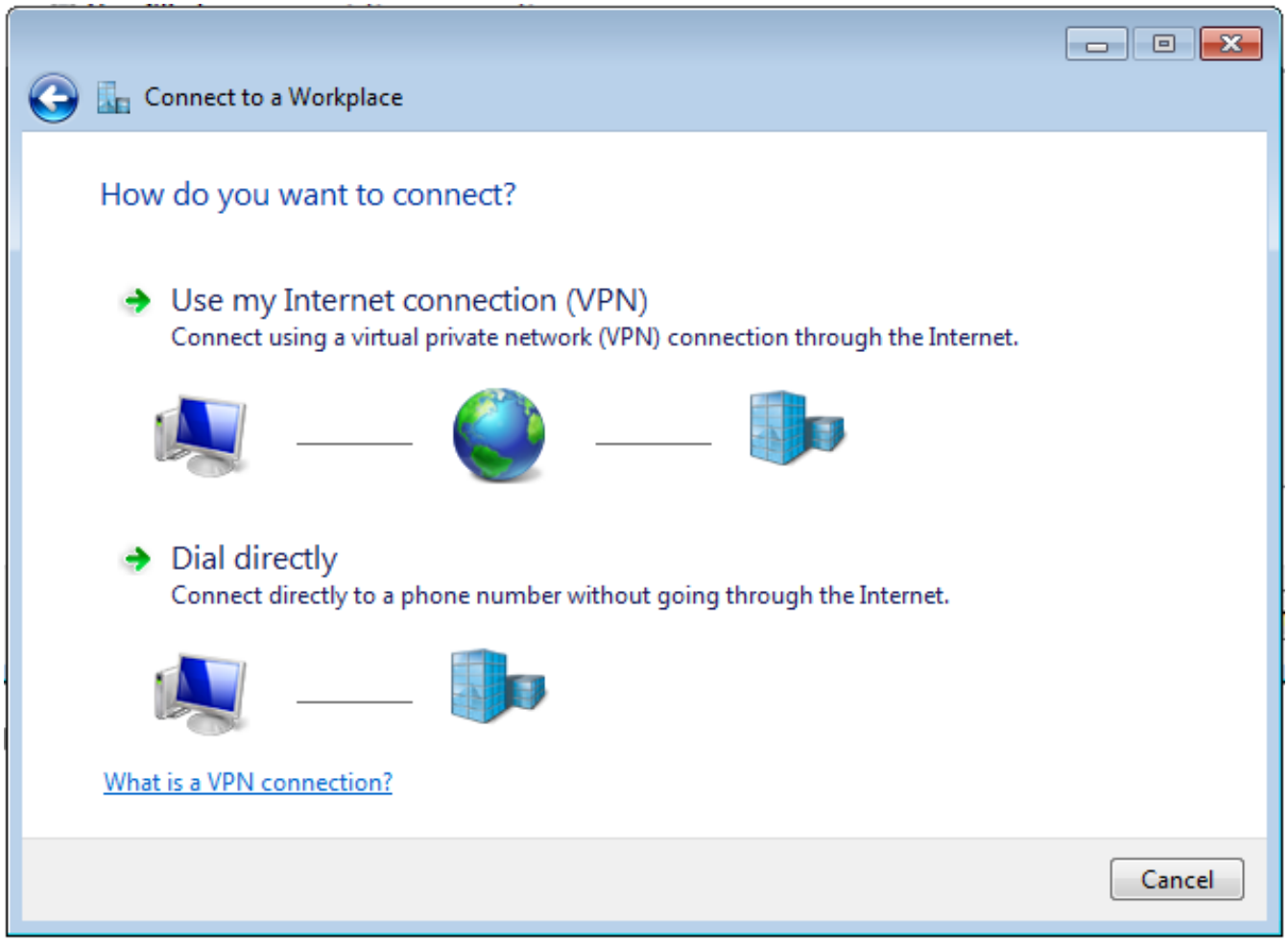
Étape 2. Sélectionnez **Configurer une nouvelle connexion ou un nouveau réseau**.



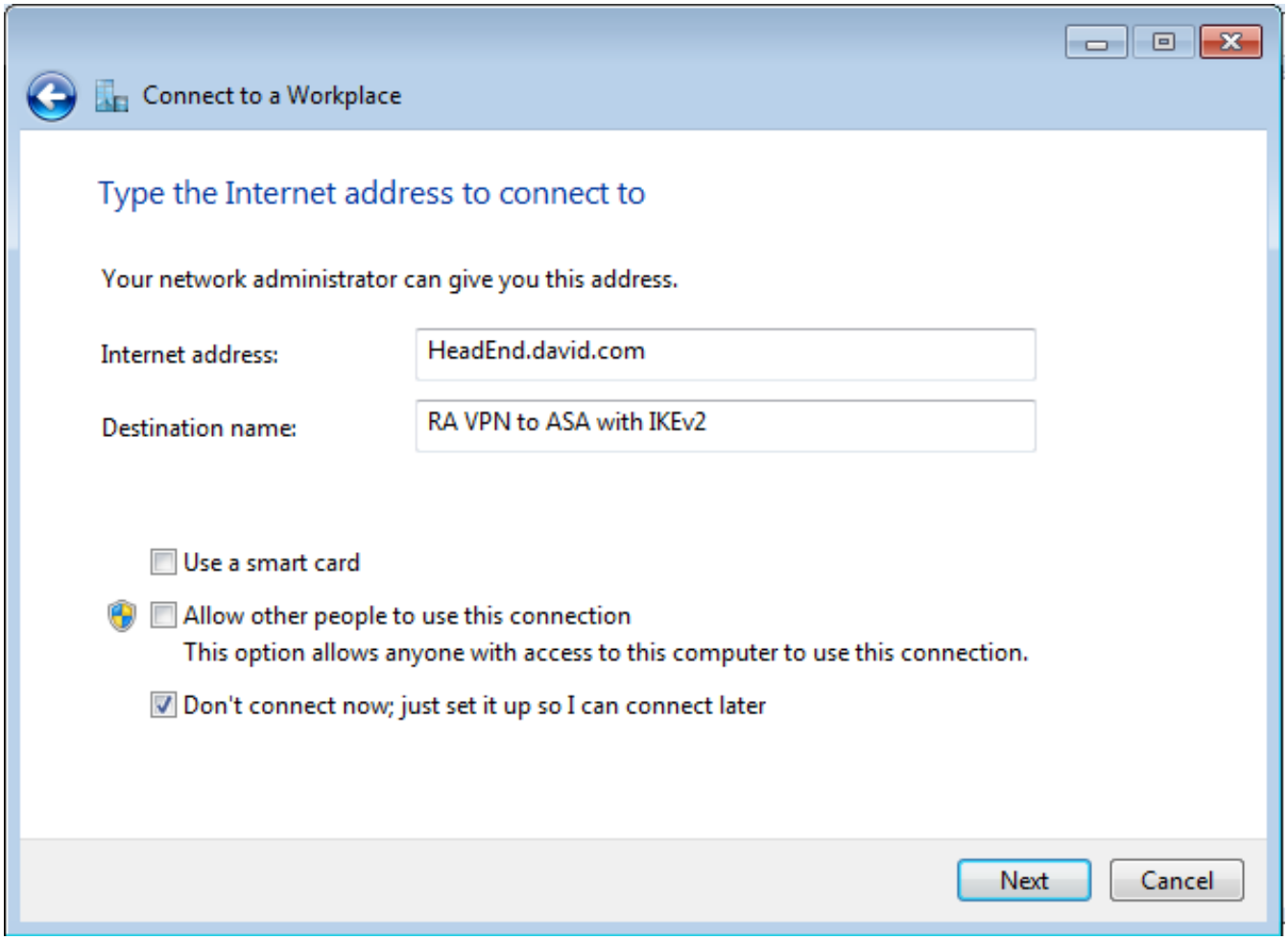
Étape 3. Sélectionnez **Se connecter à un lieu de travail** et **Suivant**.



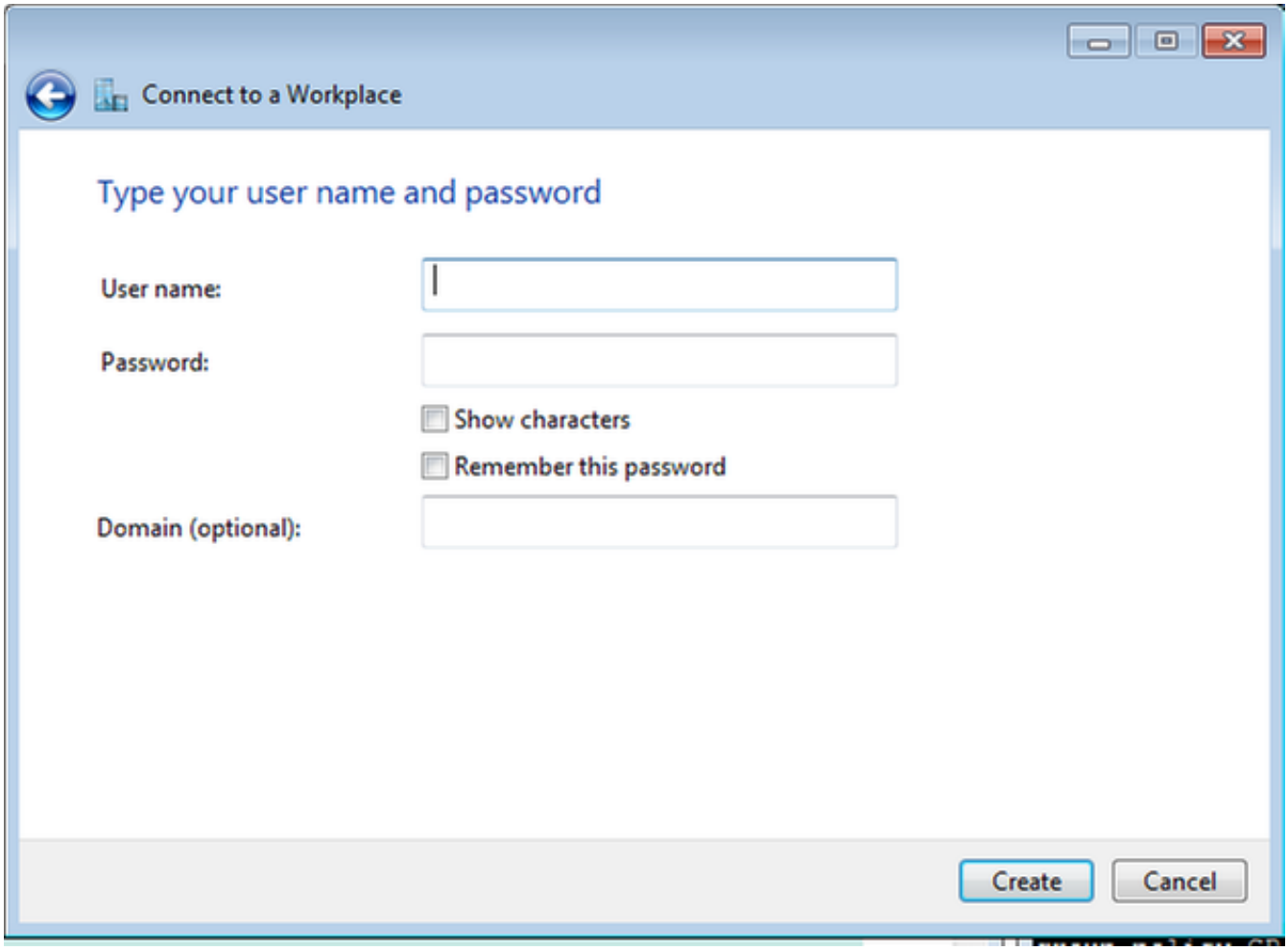
Étape 4. Sélectionnez **Non, créez une nouvelle connexion** et **Suivant**.



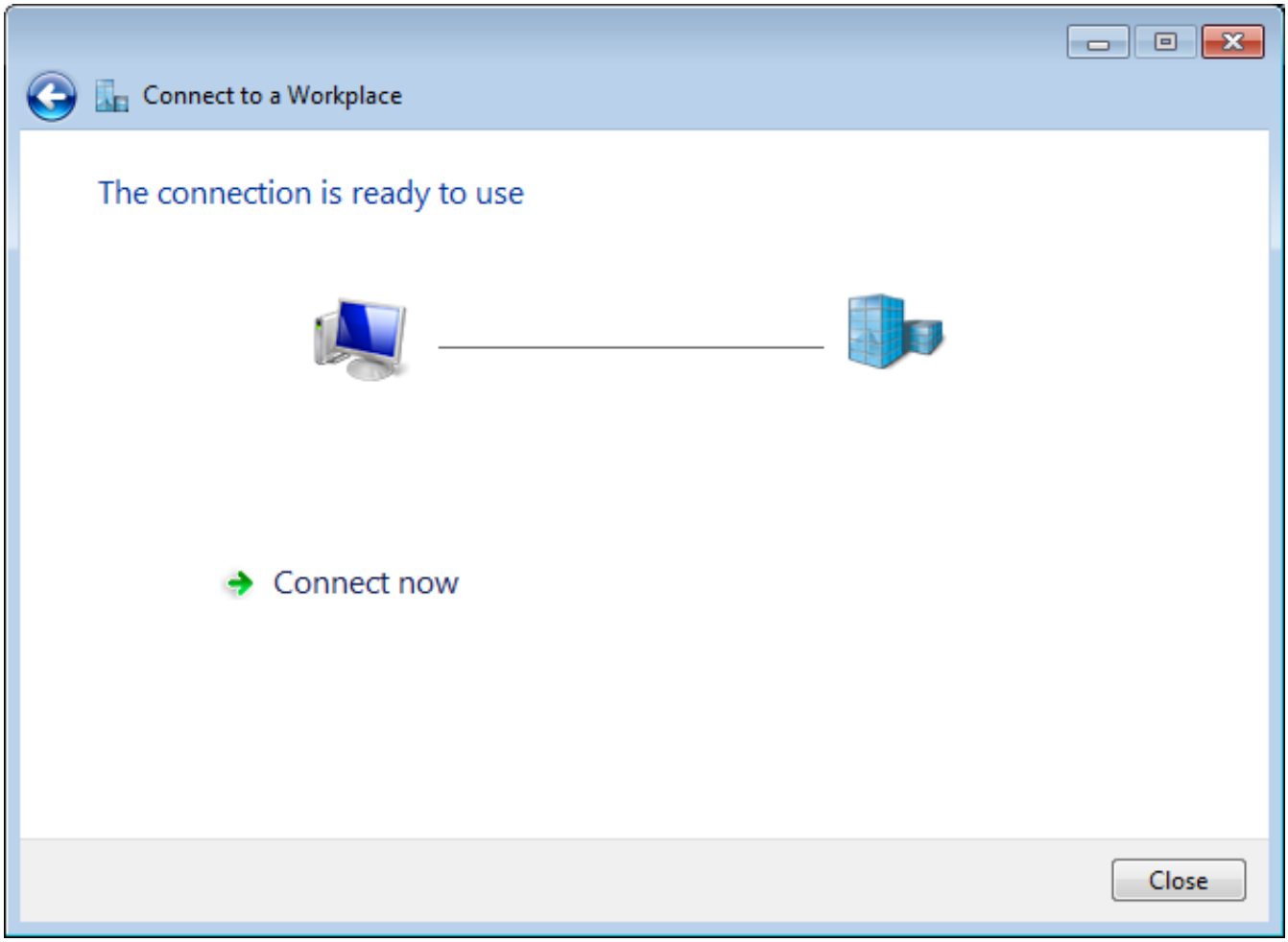
Étape 5. Sélectionnez **Utiliser ma connexion Internet (VPN)** et ajoutez la chaîne Nom commun (CN) du certificat HeadEnd dans le champ **Adresse Internet**. Dans le champ **Nom de la destination**, saisissez le nom de la connexion. Il peut s'agir de n'importe quelle chaîne. Assurez-vous de vérifier le **bouton Ne pas vous connecter maintenant ; il suffit de le configurer pour que je puisse me connecter plus tard** box.



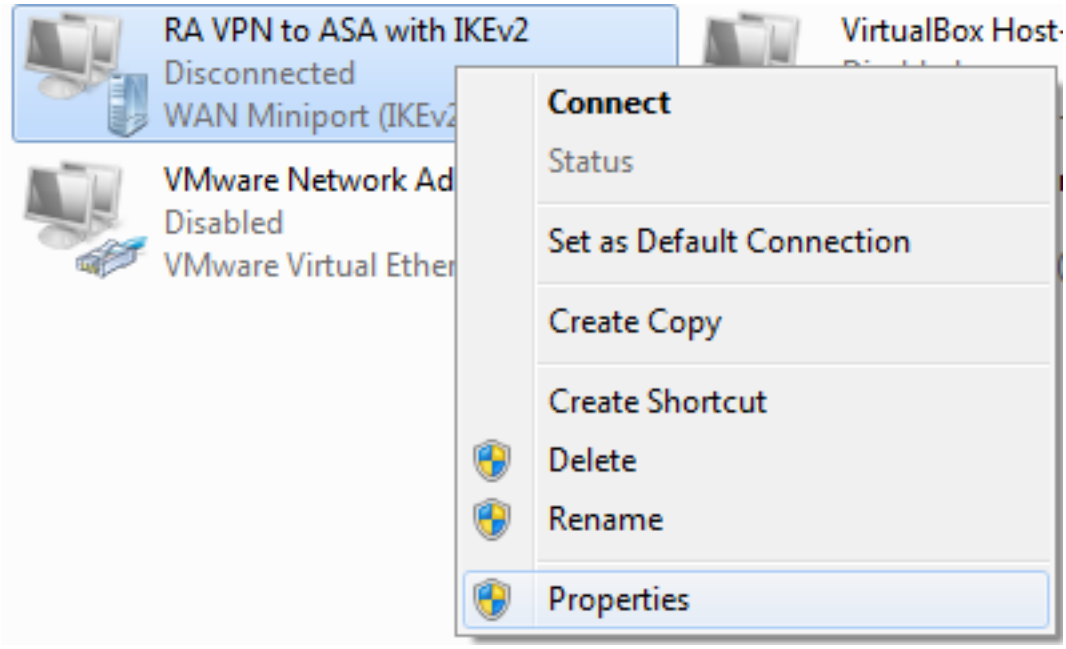
Étape 6. Sélectionnez **Suivant**.



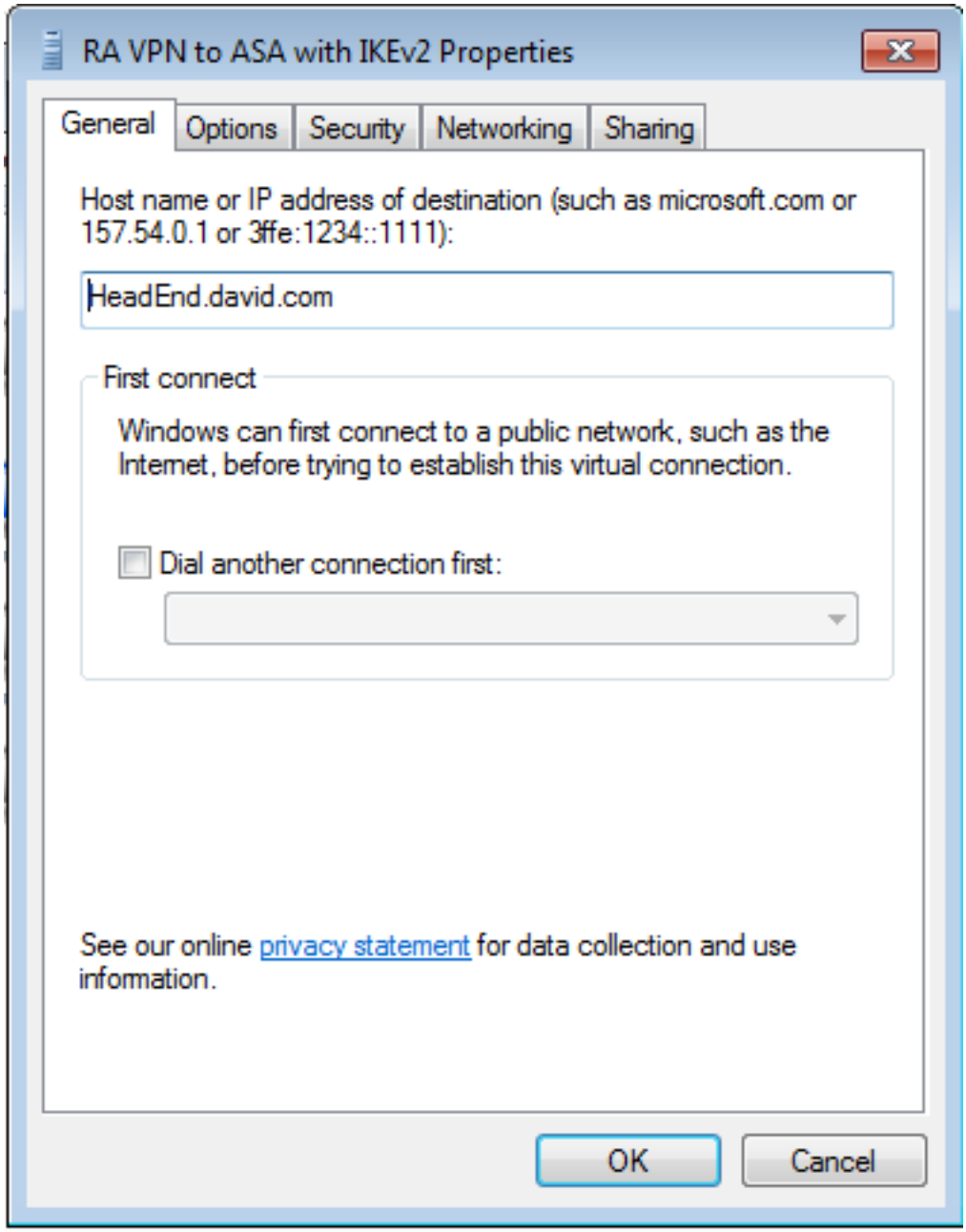
Étape 7. Sélectionnez **Créer**.



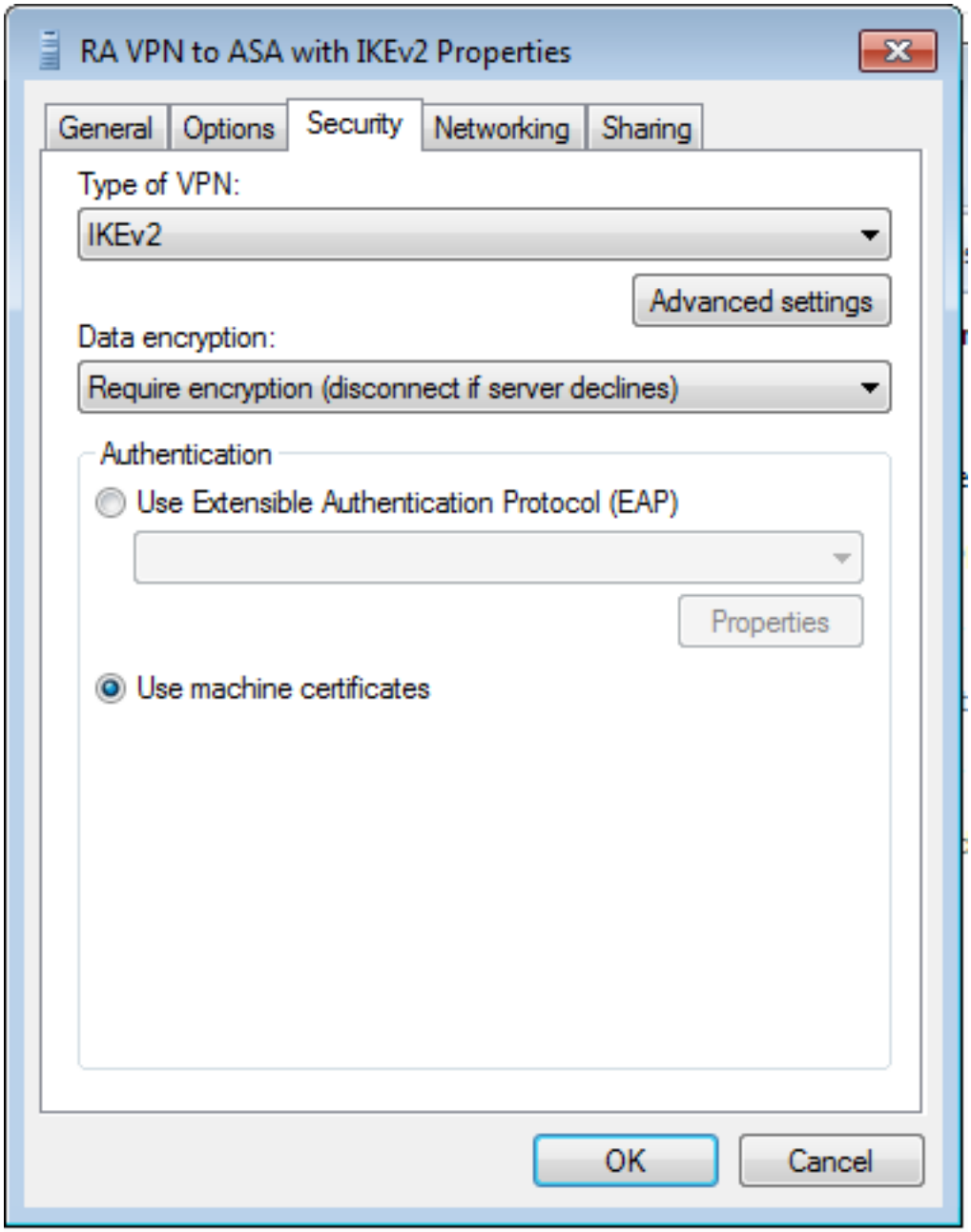
Étape 8. Sélectionnez **Fermer** et accédez à **Panneau de configuration > Réseau et Internet > Connexions réseau**. Sélectionnez la connexion réseau créée et cliquez dessus avec le bouton droit de la souris. Sélectionnez **Properties**.



Étape 9. Dans l'onglet **Général**, vous pouvez vérifier que le nom d'hôte approprié pour la tête de réseau est correct. Votre ordinateur va convertir ce nom en adresse IP ASA utilisée pour connecter les utilisateurs VPN d'accès distant.



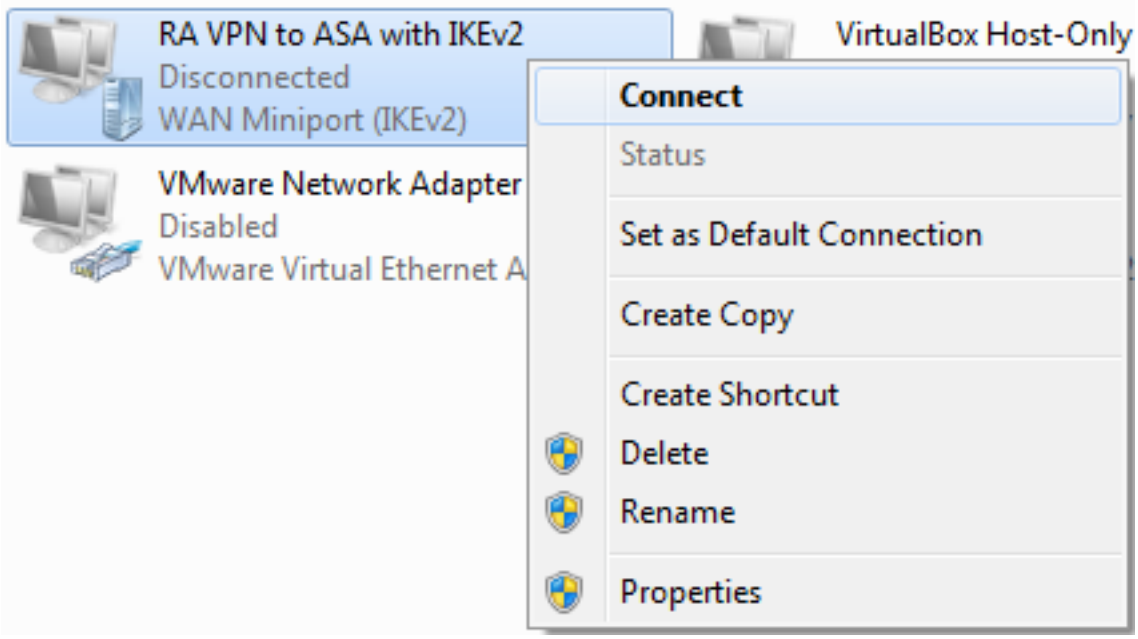
Étape 10. Accédez à l'onglet **Sécurité** et sélectionnez **IKEv2** comme **type de VPN**. Dans la section **Authentification**, sélectionnez **Utiliser les certificats de machine**.



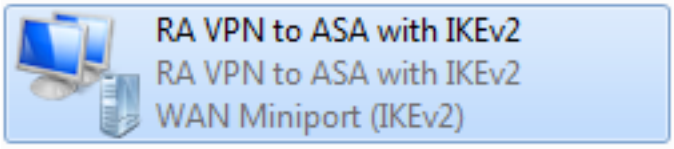
Étape 11. Sélectionnez **OK** et accédez à **C:\Windows\System32\drivers\etc**. Ouvrez le fichier **hosts** à l'aide d'un éditeur de texte. Configurez une entrée pour résoudre le nom de domaine complet (FQDN) configuré dans la connexion réseau à l'adresse IP de votre tête de réseau ASA (dans cet exemple, l'interface externe).

```
# 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
```

Étape 12. Revenez au **Panneau de configuration > Réseau et Internet > Connexions réseau**. Sélectionnez la connexion réseau que vous avez créée. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Connect.**



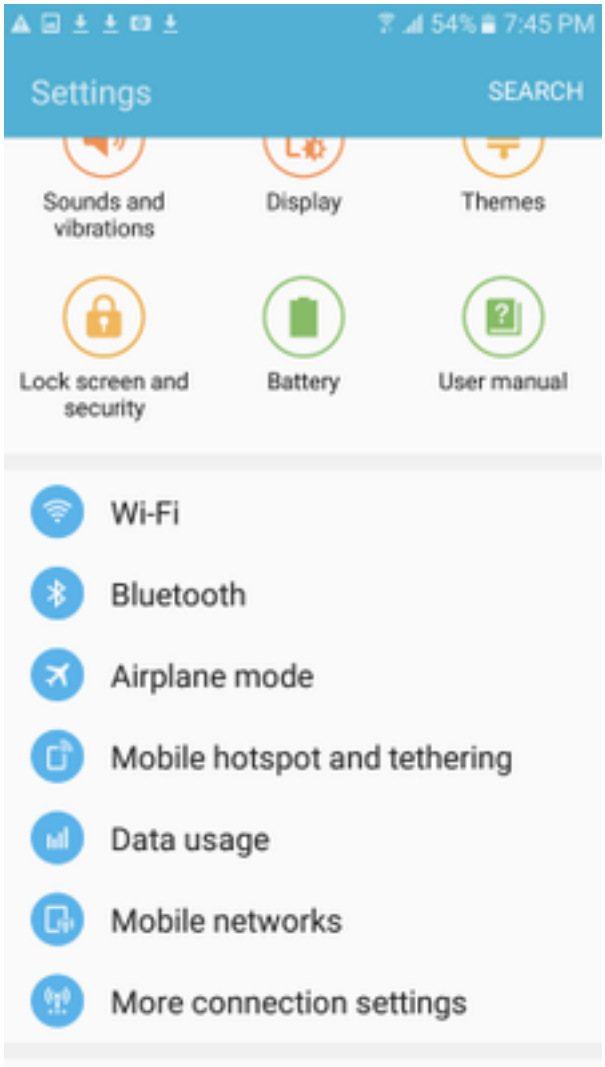
Étape 13. L'état de la connexion réseau passe de Disconnected à Connecting, puis à Connected. Enfin, le nom que vous avez spécifié pour la connexion réseau s'affiche.



L'ordinateur est connecté à la tête de réseau VPN à ce stade.

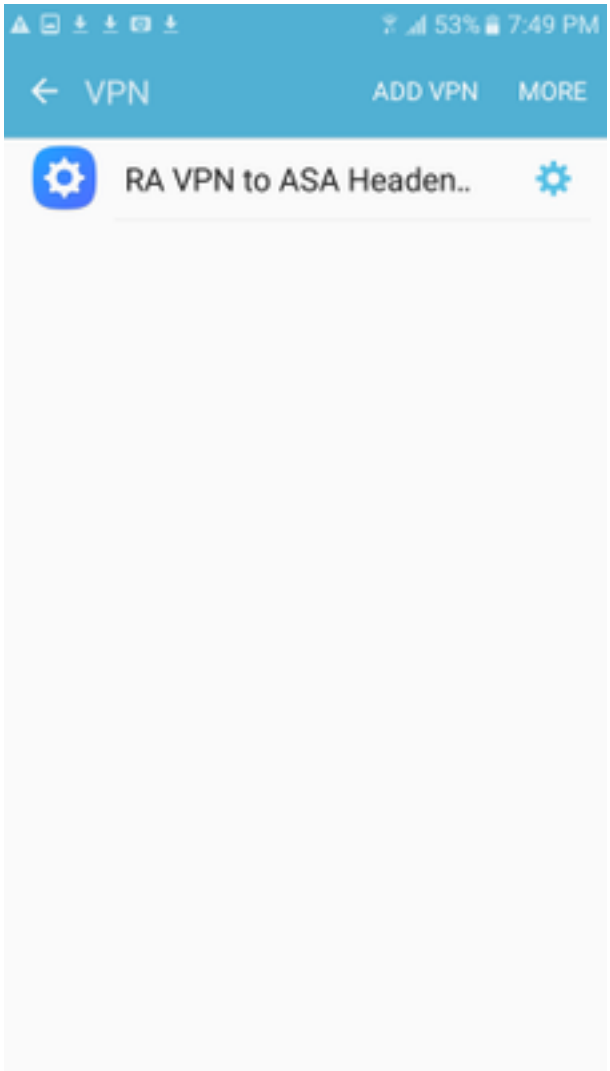
Configurer le client VPN natif Android

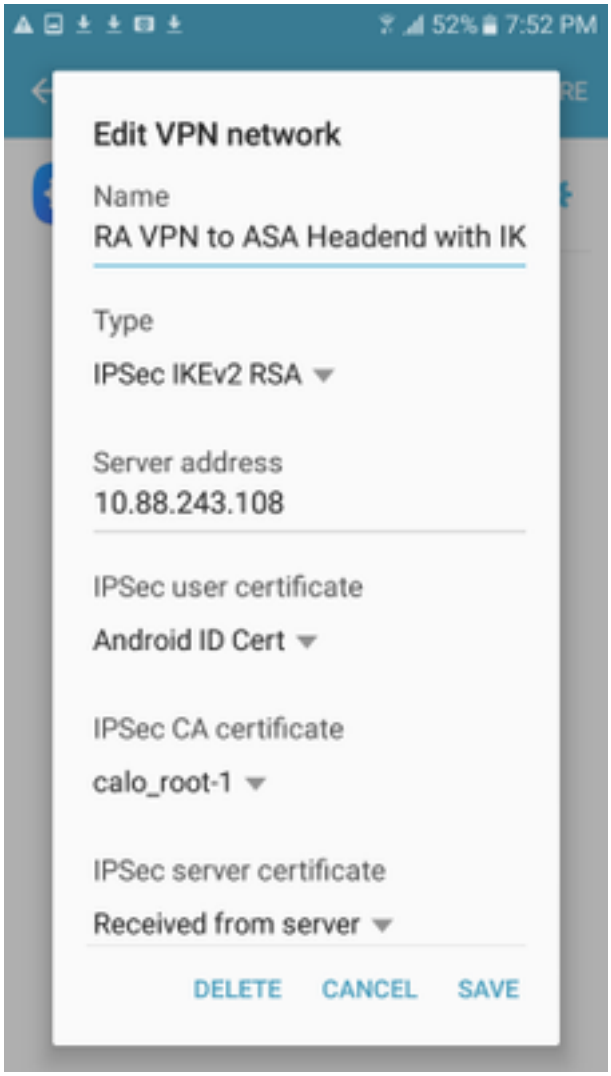
Étape 1. Accédez à **Paramètres >Autres paramètres de connexion**



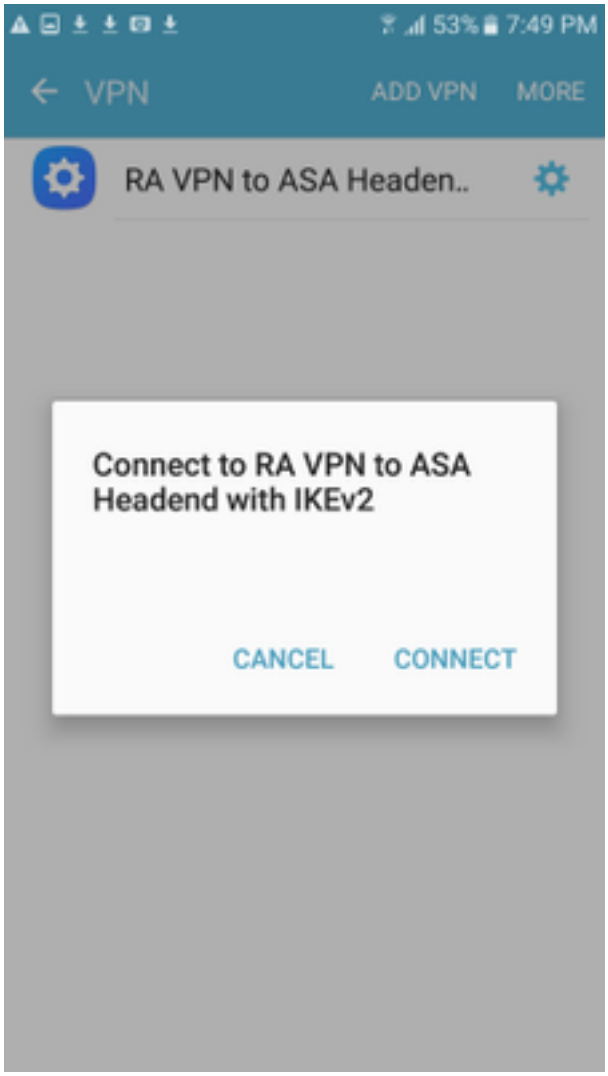
Étape 2. Sélectionner **VPN**

Étape 3. Sélectionnez **Add VPN**. Si la connexion est déjà créée comme dans cet exemple, effleurez l'icône du moteur pour la modifier. Spécifiez IPSec IKEv2 RSA dans le champ **Type**. L'**adresse du serveur** est l'adresse IP de l'interface ASA IKEv2 activée. Pour le **certificat d'utilisateur IPSec** et le **certificat d'autorité de certification IPSec**, sélectionnez les certificats installés en cliquant sur dans les menus déroulants. Laissez le **certificat du serveur IPSec** avec l'option par défaut, Received from server.

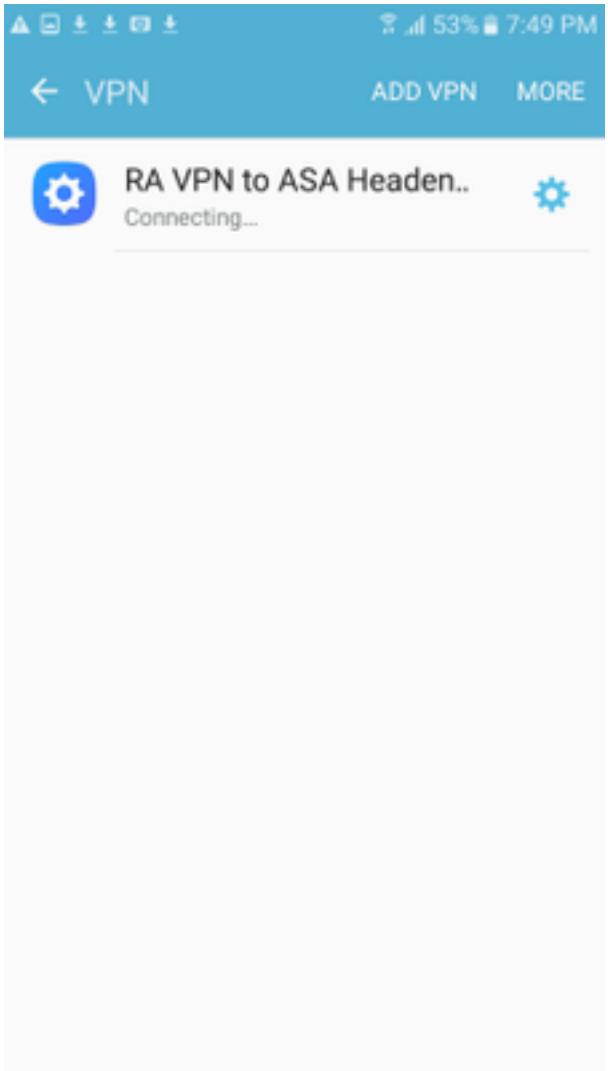

53% 7:49 PM
VPN
ADD VPN
MORE
RA VPN to ASA Headen..

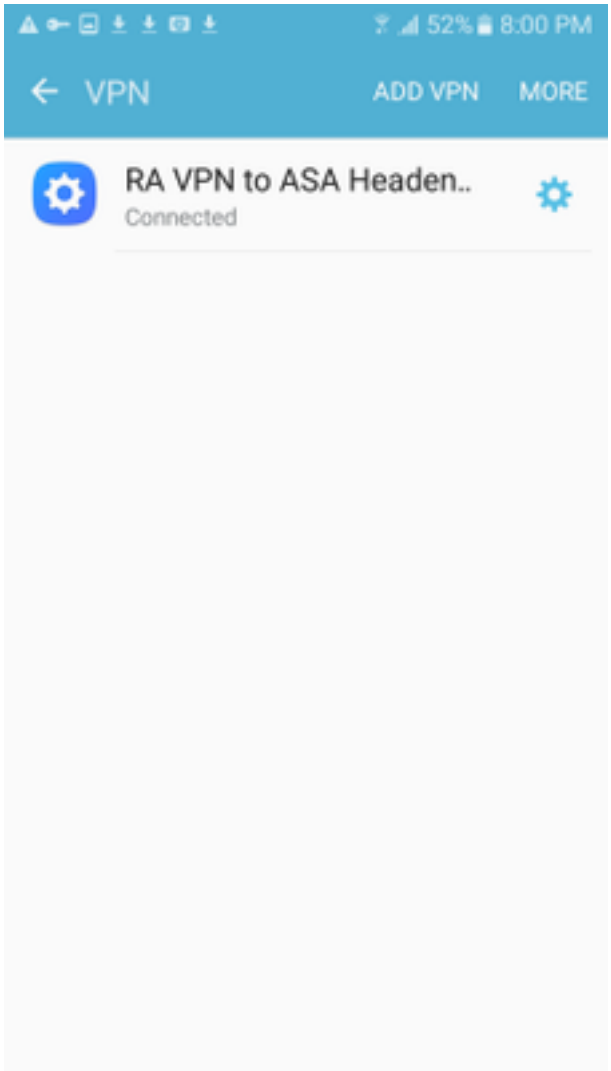


Étape 4. Sélectionnez **Enregistrer** puis effleurez le nom de la nouvelle connexion VPN.

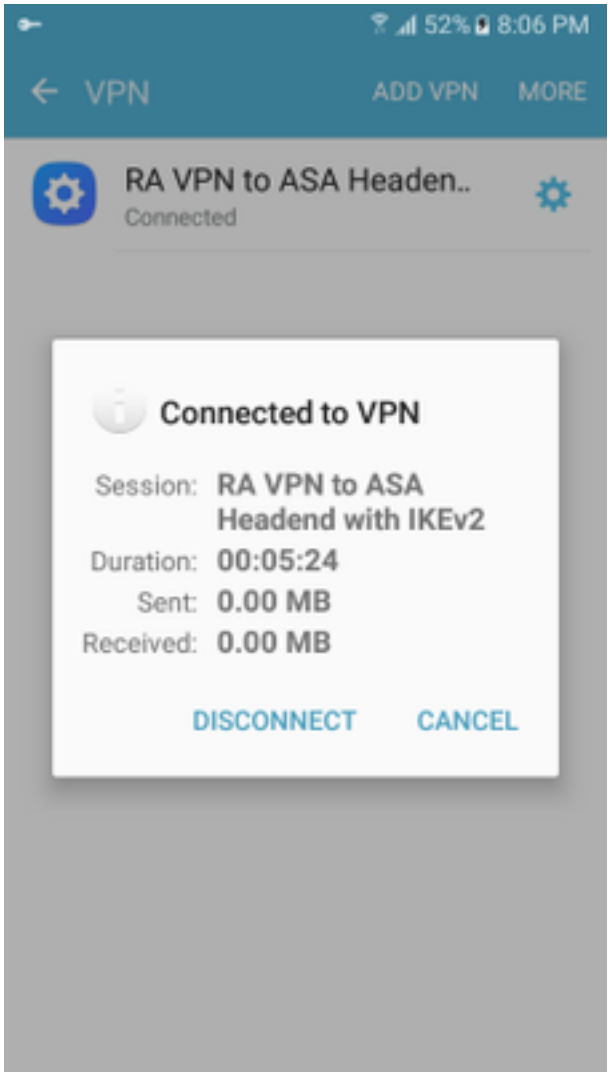


Étape 5. Sélectionnez **Connect.**


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



Étape 6. Tapez une nouvelle fois la connexion VPN pour vérifier l'état. Il s'affiche maintenant sous la forme **Connected**.



Vérification

Commandes de vérification sur la tête de réseau 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
2119549341    10.88.243.108/4500   10.152.206.175/4500      READY    RESPONDER      Encr: AES-
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
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

> **Note**: Référez-vous à Informations importantes sur les commandes de débogage avant d'utiliser les commandes debugcommand.

> **Attention** : Sur ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, la verbosité des débogages augmente. Faites ceci avec prudence, en particulier dans les environnements de production.

- **Debug crypto ikev2 protocol 15**
- **Debug crypto ikev2 platform 15**
- **Debug crypto ca 255**