带Windows 7或Android VPN客户端的ASA IKEv2 RA VPN和证书身份验证配置

目录

简介

本文档介绍如何配置思科自适应安全设备(ASA)9.7.1版及更高版本，以允许Windows 7和Android本机（虚拟专用网络）VPN客户端使用互联网密钥交换协议(IKEv2)和证书作为身份验证方法建立（远程访问）RA VPN连接。

作者：David Rivera和Cesar Lopez Zamarripa，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 证书颁发机构 (CA)
- 公用密钥基础结构 (PKI)
- 在ASA上具有IKEv2的RA VPN
- Windows 7内置VPN客户端
- Android本地VPN客户端

使用的组件

本文档中的信息基于以下软件版本：

- CISCO1921/K9 - 15.5(3)M4a作为IOS CA服务器
- ASA5506X - 9.7(1)作为VPN头端
- Windows 7作为客户端计算机
- Galaxy J5 - Android 6.0.1作为移动客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

概述

以下步骤配置Windows 7和Android本机VPN客户端以连接到ASA头端：

配置证书颁发机构

CA允许在证书中嵌入所需的扩展密钥使用(EKU)。对于ASA头端，需要证书服务器身份验证EKU，而客户端证书需要客户端身份验证EKU。

可以使用多种CA服务器，例如：

- Cisco IOS CA服务器
- OpenSSL CA服务器
- Microsoft CA服务器
- 3第 交易方CA

此配置示例使用IOS CA服务器。

本节概述使CISCO1921/K9(版本15.5(3)M4a作为CA服务器工作的基本配置。

步骤1.确保设备和版本支持eku命令。

```
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
```

步骤2.在路由器上启用HTTP服务器。

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

步骤3.生成可导出的RSA密钥对。

```
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)
```

步骤4.配置信任点。

```
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>
```

注意：enrollment命令的IP地址是路由器为可到达接口配置的IP地址之一。

步骤5.验证信任点（获取CA证书）。

```
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.
```

步骤6.注册信任点（获取身份证书）。

```
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
```

步骤7.检验证书。

```
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
```

步骤8.以PKCS12格式将HeadEnd信任点导出到终端以获取身份证书。CA证书和私钥将添加到一个文件中。

```
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.
```

步骤9.在ASA上创建空信任点。

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

步骤 10导入PKCS12文件。

```
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
eC4Kbf1cmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/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
```

步骤11.检验证书信息。

```
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
```

生成客户端证书

步骤1.生成可导出的RSA密钥对。

```
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
```

步骤2.配置信任点。

```
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>
```

步骤3.对配置的信任点进行身份验证（获取CA证书）。

```
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.
```

步骤4.注册经过身份验证的信任点（获取身份证书）。

```
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
```

步骤5.检验证书信息。

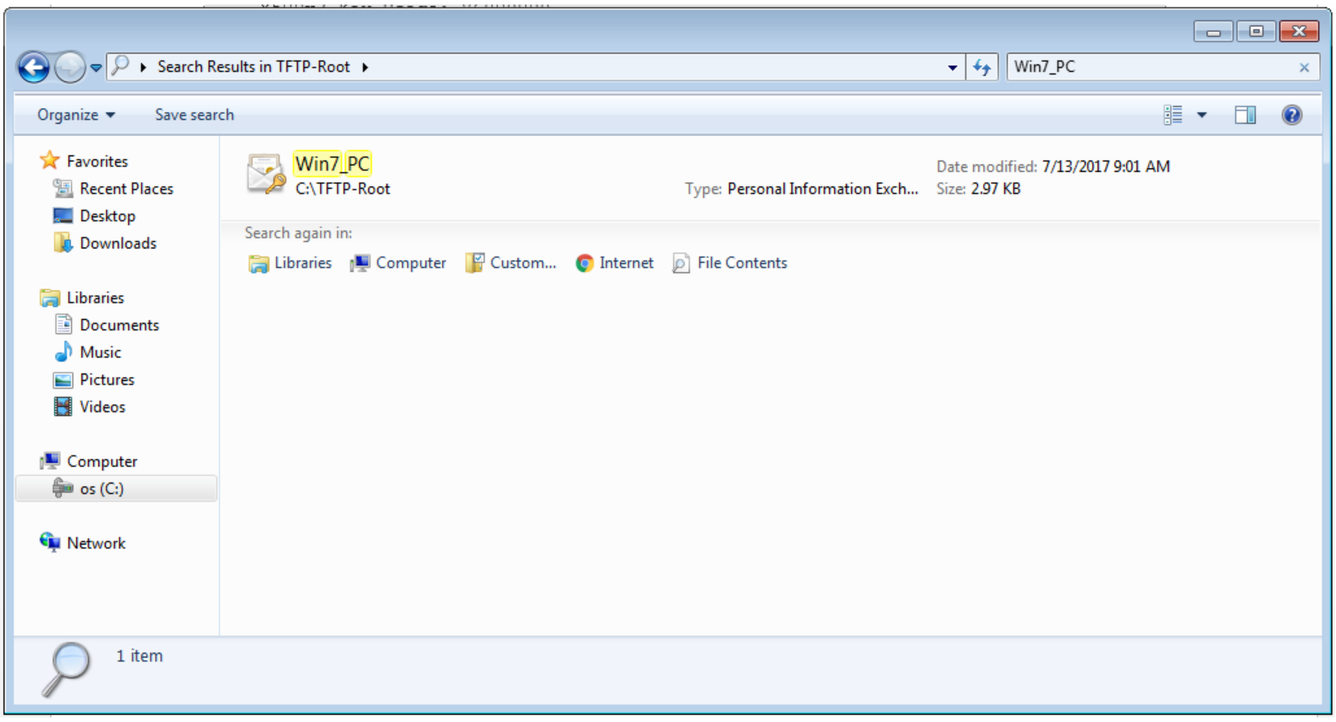
```
IOS-CA#show crypto pki certificates verbose <Win7_PC>
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 03
  Certificate Usage: General Purpose
  Issuer:
    cn=calo_root
  Subject:
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
    cn=Win7_PC.david.com
  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
```

在Windows 7客户端计算机上安装身份证书

步骤1.以PKCS12格式(.p12)将命名的Win7_PC信任点导出到FTP/TFTP服务器（安装在Windows 7计算机上），以在单个文件中获取身份证书、CA证书和私钥。

```
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.
```

这是导出文件在客户端计算机上的显示方式。



Win7_PC

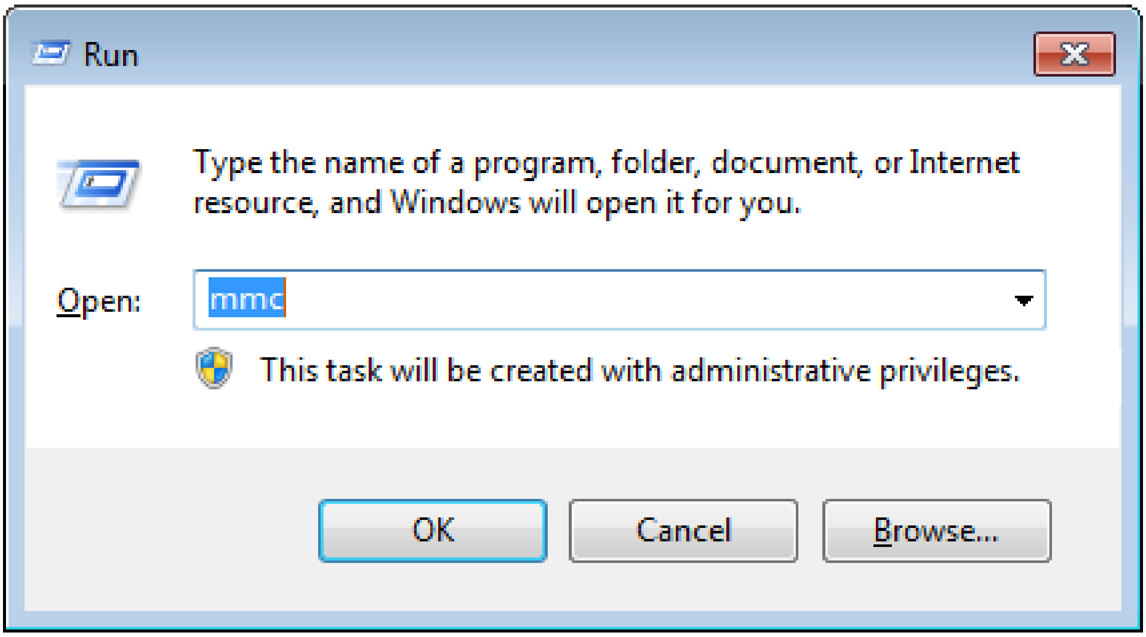
Win7_PC
C:\TFTP-Root

Type: Personal Information Exch...

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

Size: 2.97 KB

步骤2.按**Ctrl + R**并键入**mmc**以打开Microsoft管理控制台(MMC)。

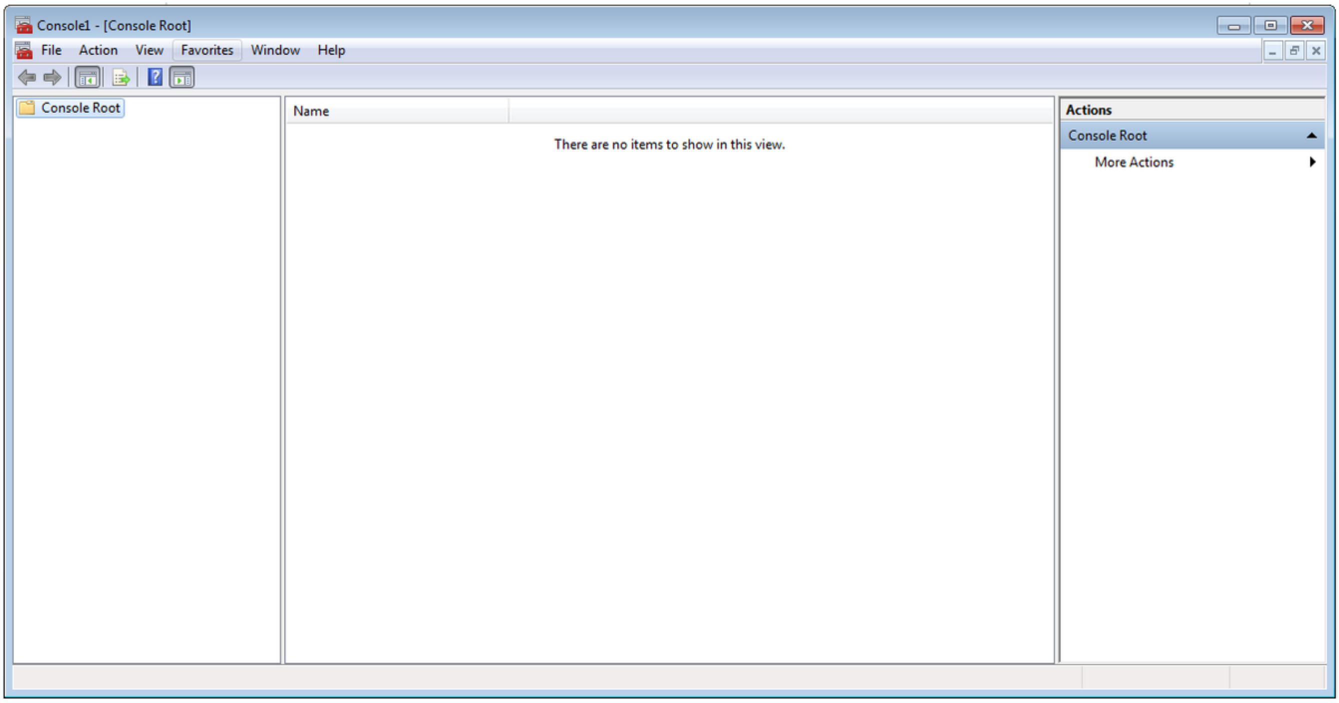


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

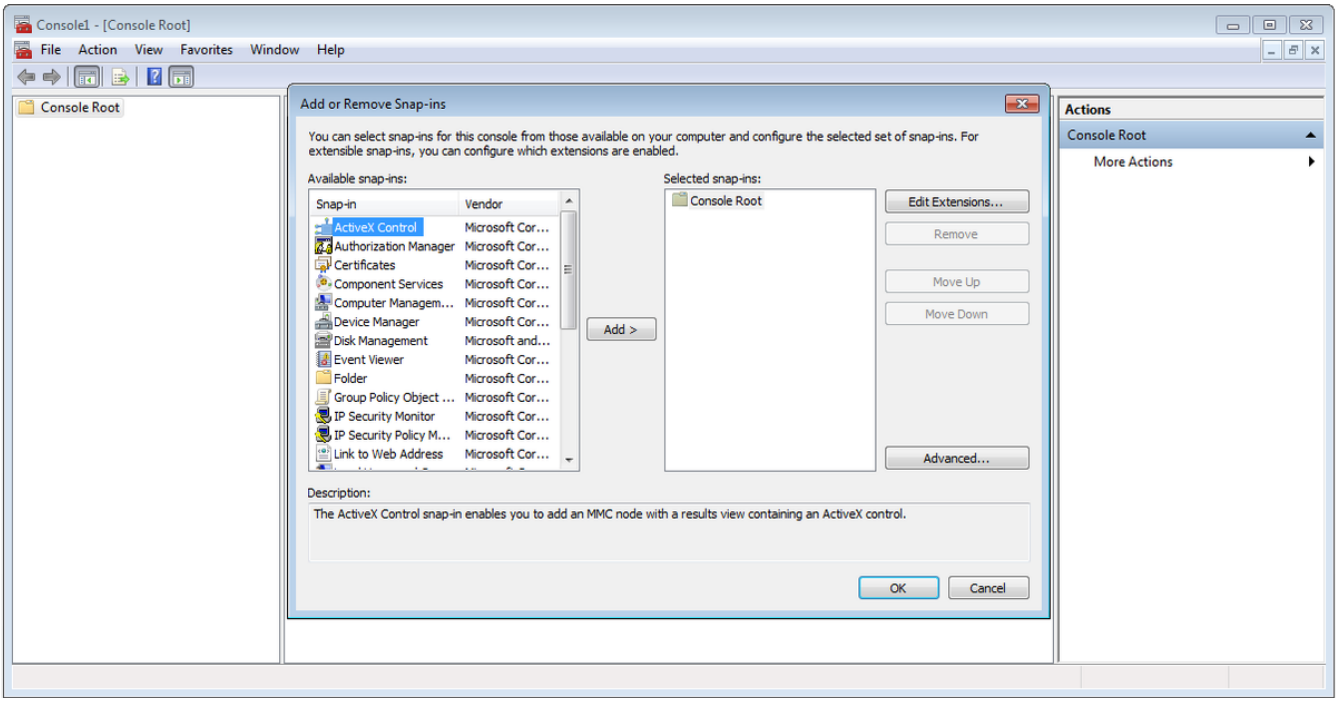
This task will be created with administrative privileges.

步骤3.选择**OK**。



There are no items to show in this view.

步骤4.导航至“文**件”>“添加/删除管理单元”**。



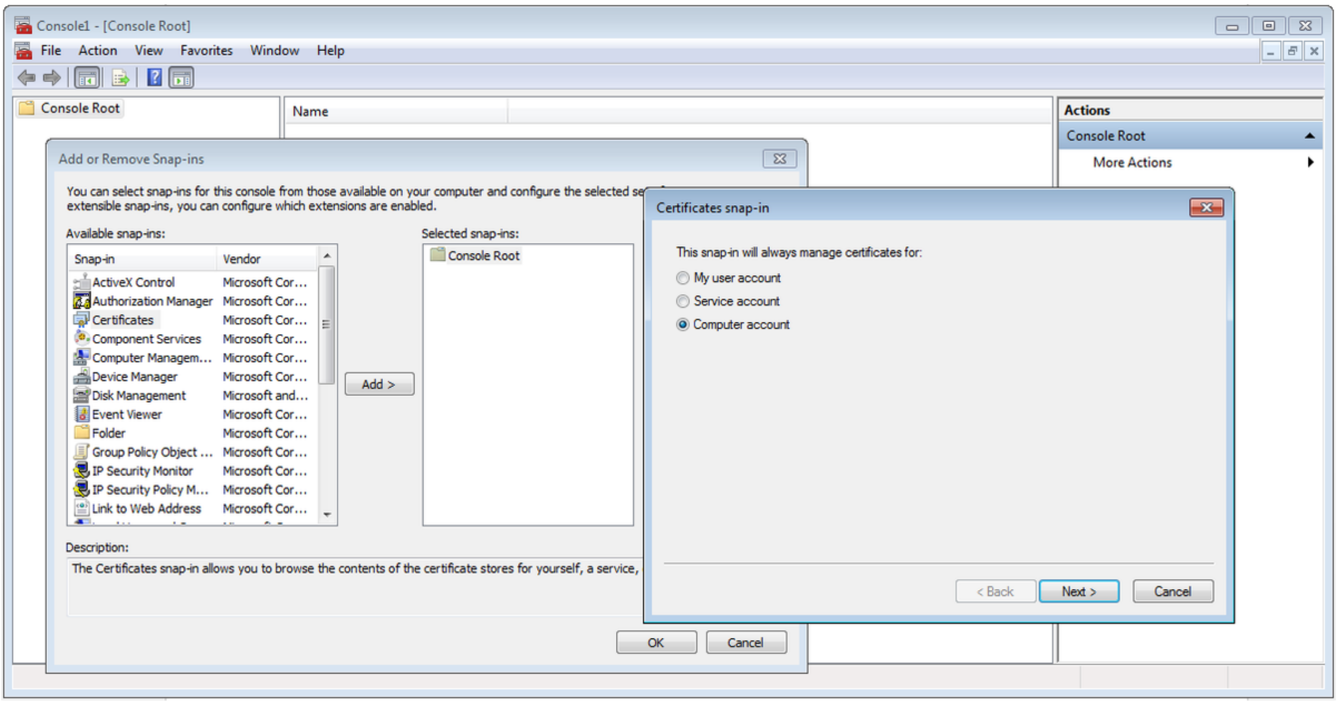
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

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...

Description:

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

步骤5.选择“证**书”>“添加”>“计算机帐户**”。



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,

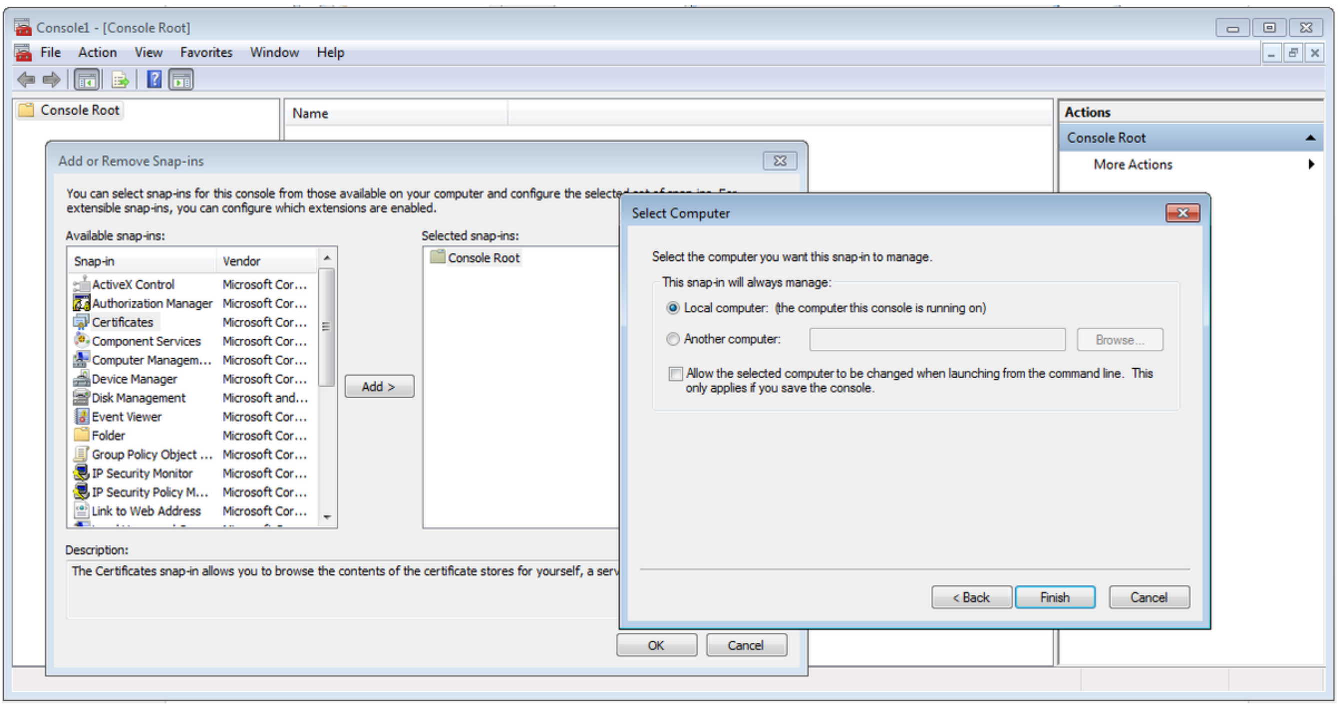
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

步骤6.选择“下一步”,



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 the computer you want this snap-in to manage.

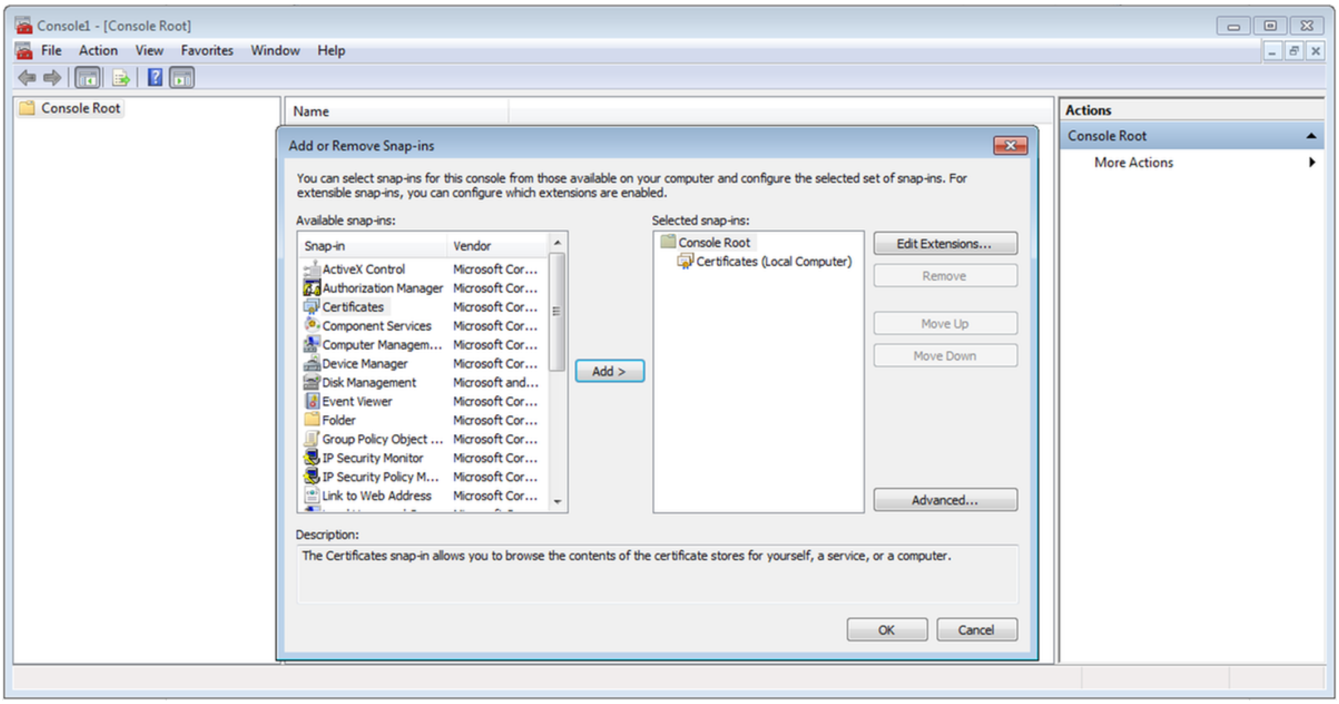
This snap-in will always manage:

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

○ Another computer:

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

步骤7.完成。



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.

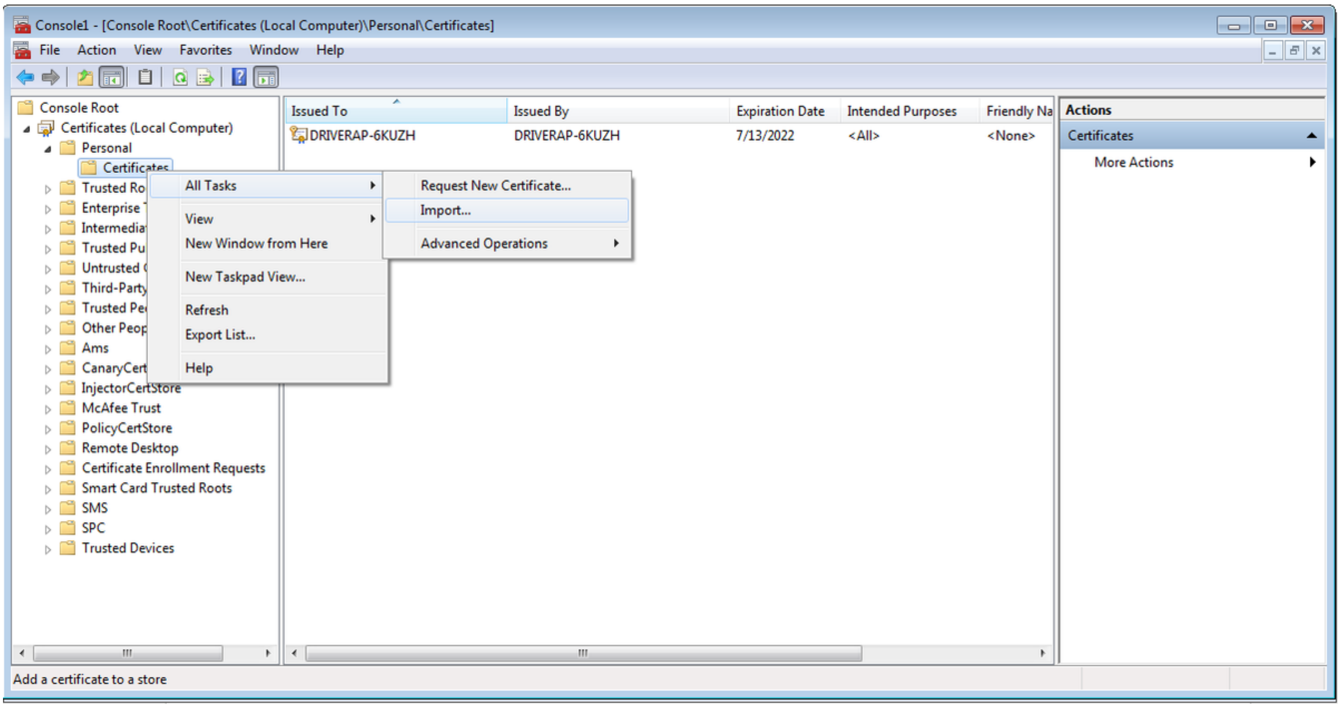
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft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

Description:

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

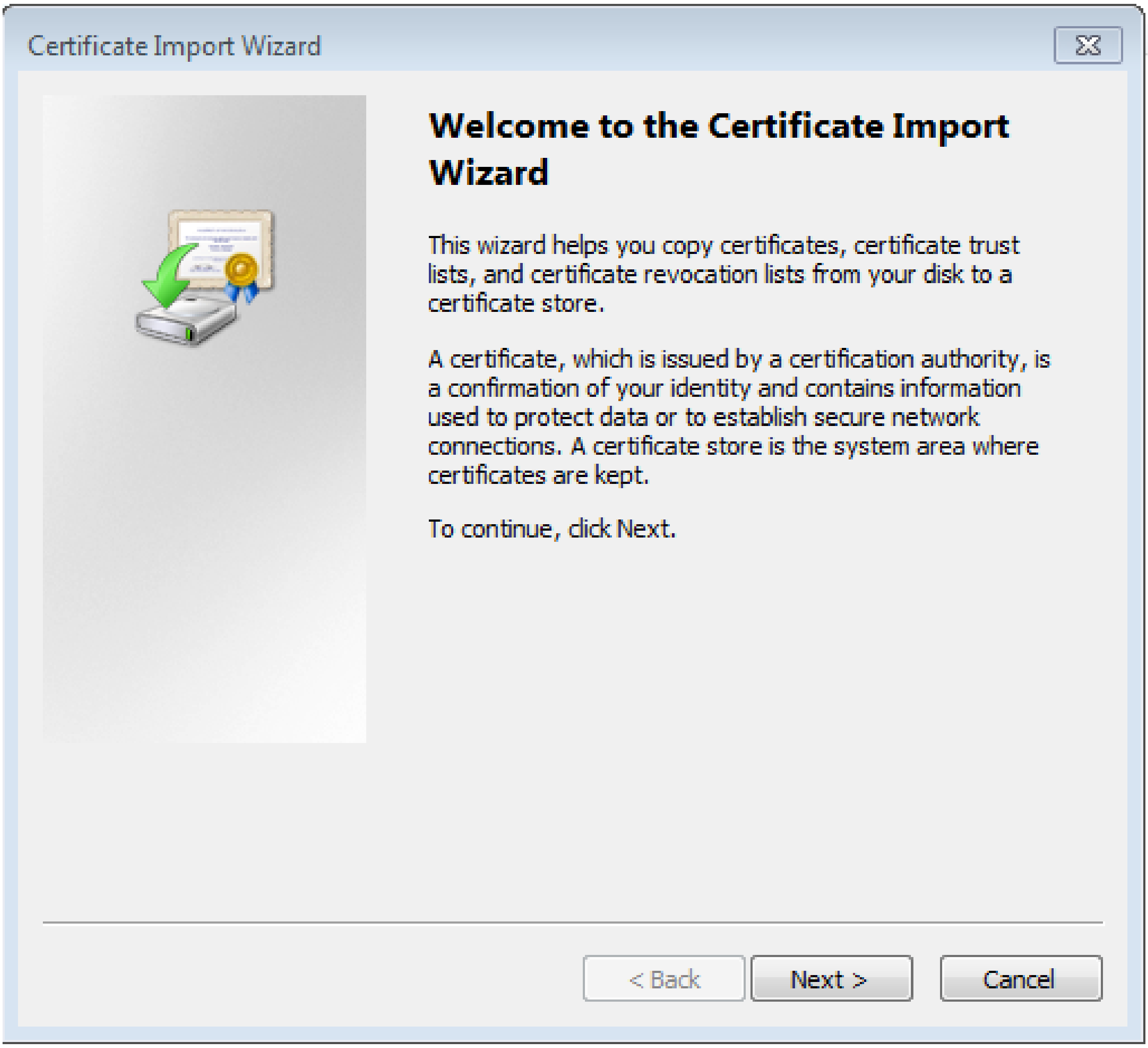
步骤8.选择**OK**。

步骤9.转到Certificates(Local Computer)**>Personal>Certificates，右键单击该文**件夹，然后导航到All Tasks**>Import**:



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



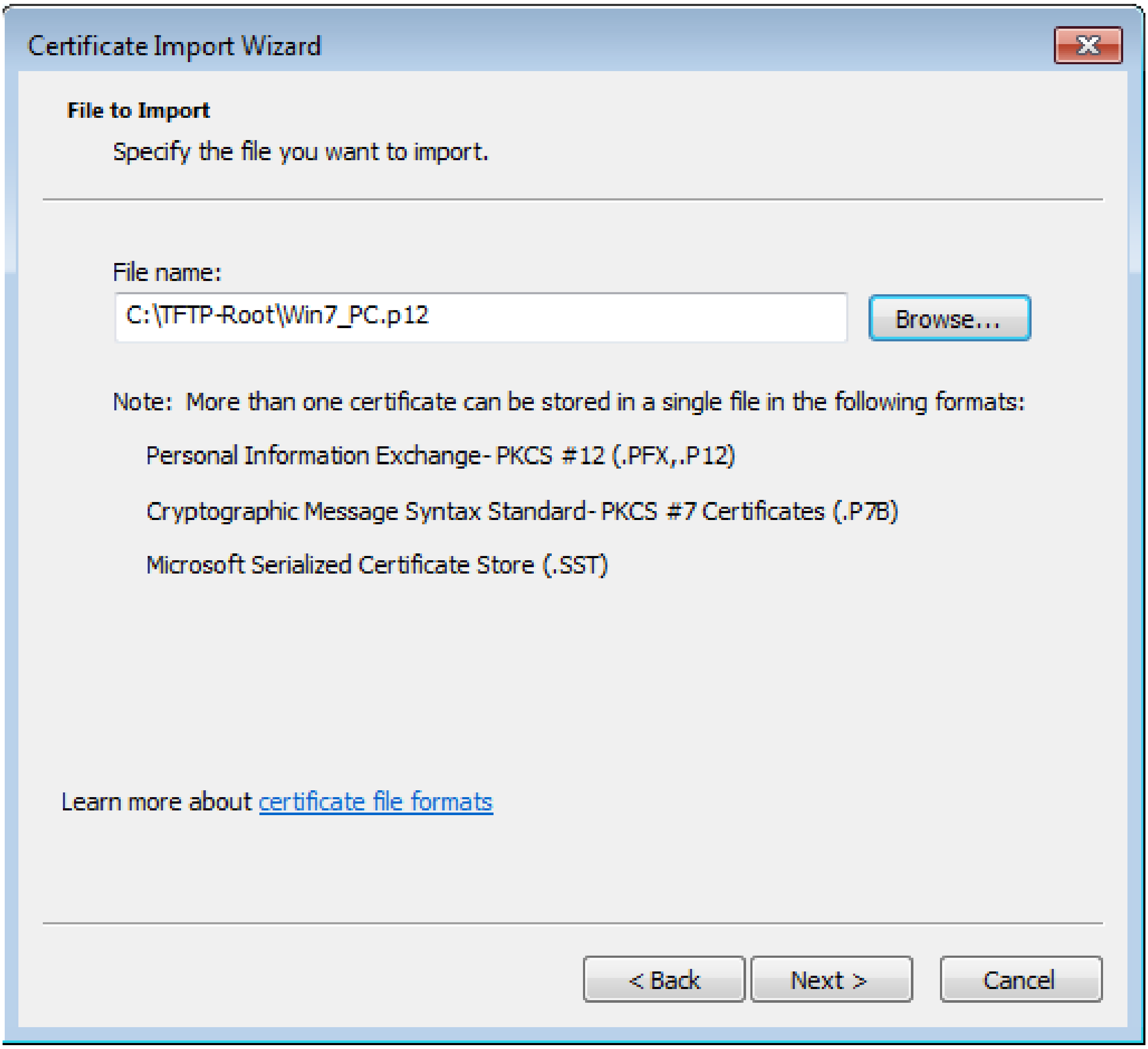
Welcome to the Certificate Import Wizard

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.

步骤10.单击“下**一步”**。指示PKCS12文件的存储路径。



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:

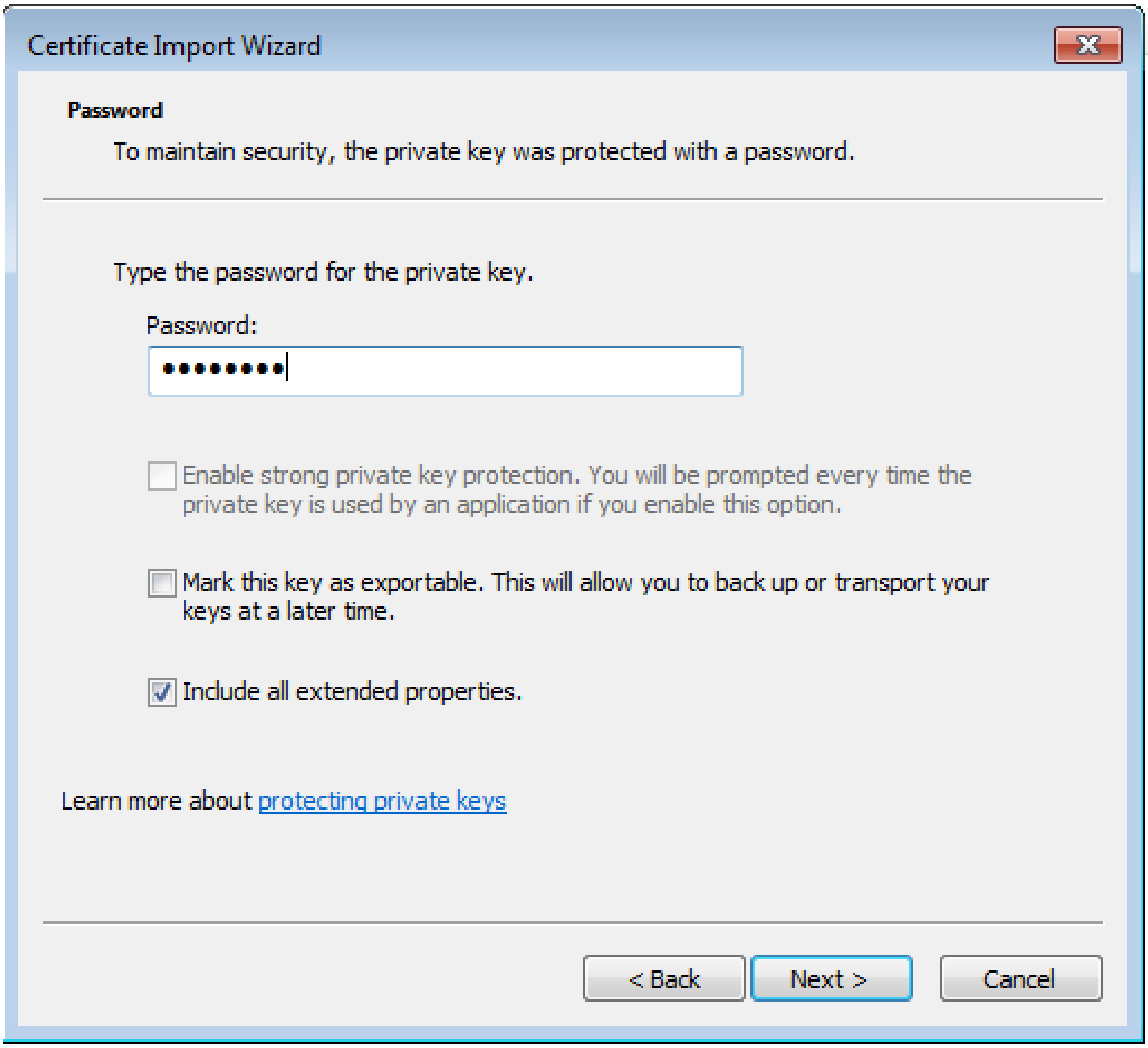
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

步骤11.再次选择**Next**，并键入*crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>*命令中输入的密码



Certificate Import Wizard

Password

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

Type the password for the private key.

Password:

●●●●●●●●●

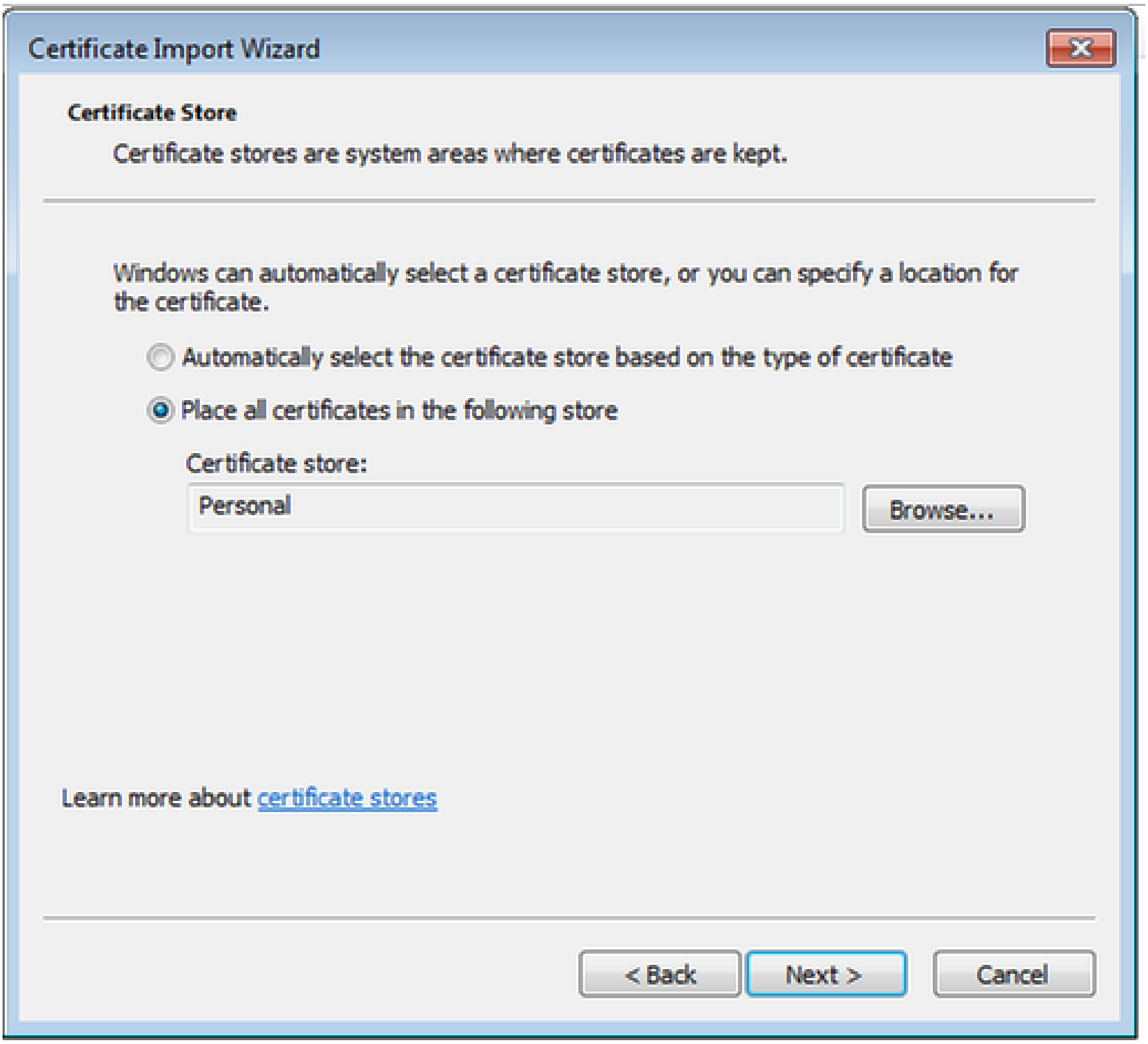
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ 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

步骤12.选择“下**一步**”。



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

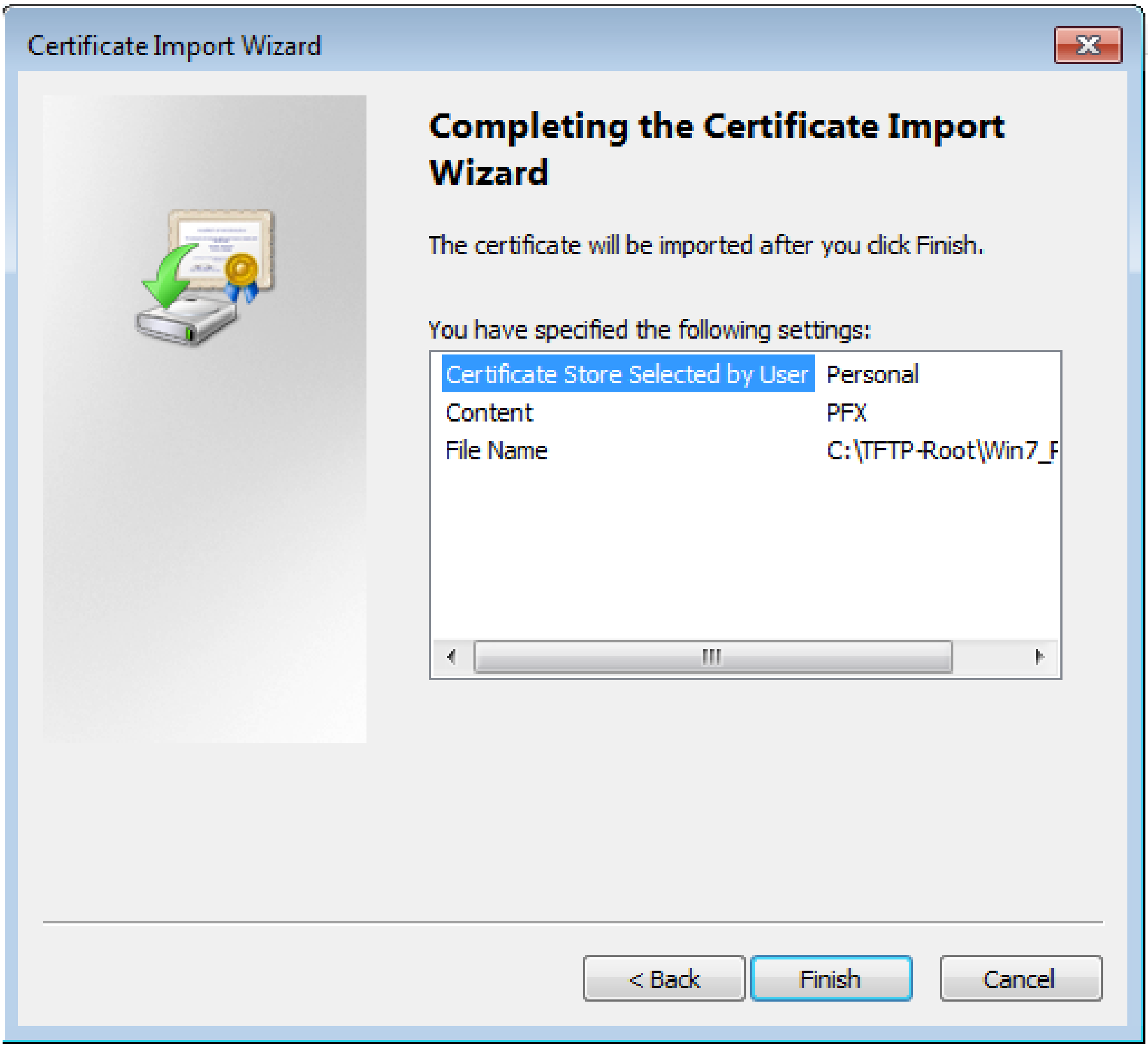
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store: Personal

步骤13.再选择Next。



Certificate Import Wizard

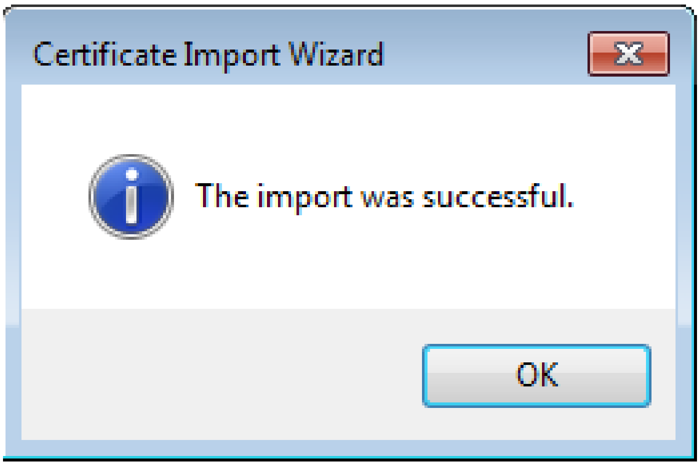
Completing the Certificate Import Wizard

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

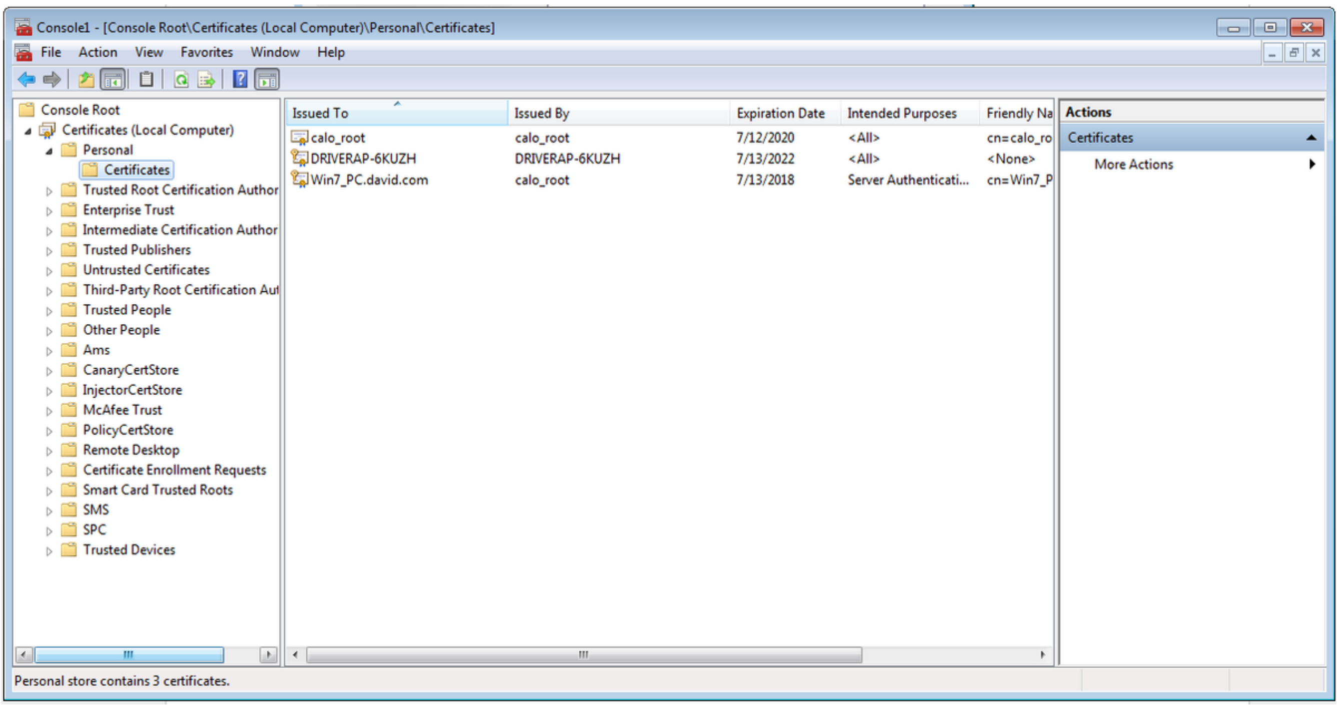
步骤14.选择“**完成**”。



Certificate Import Wizard

The import was successful.

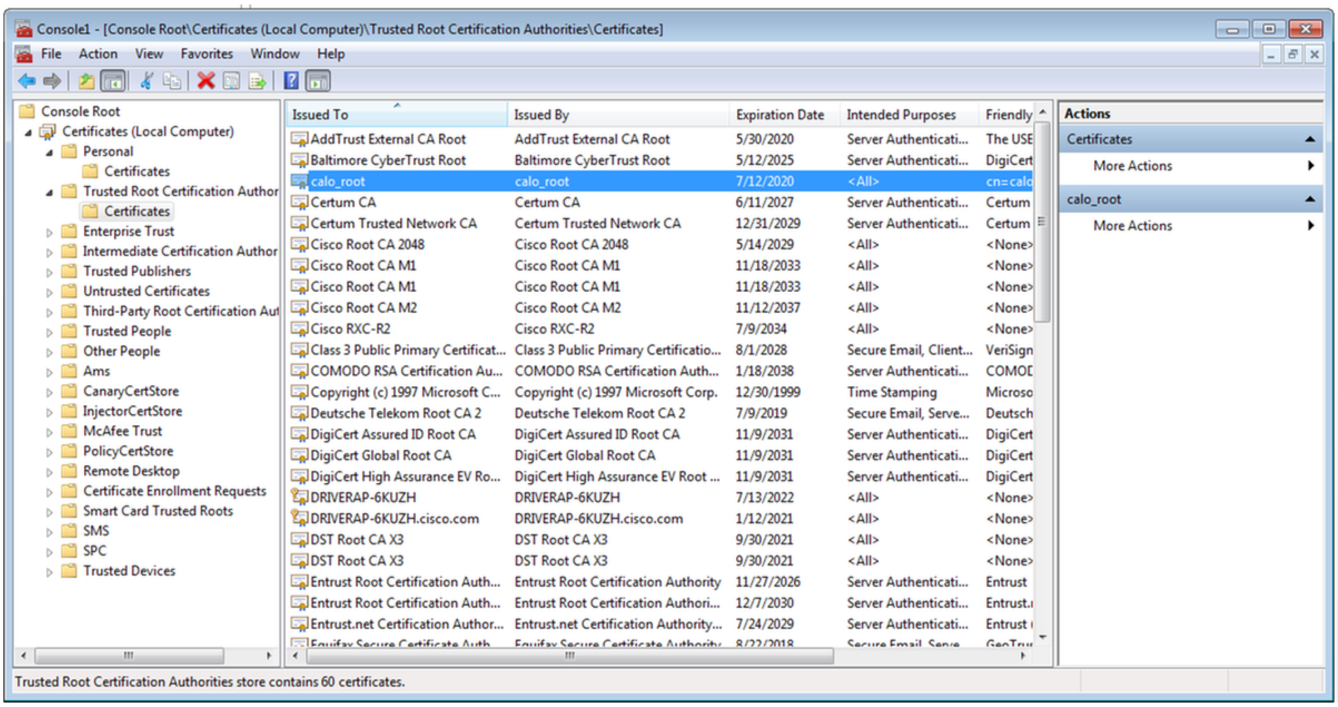
步骤15.选择**OK**。现在，您将看到安装的证书（CA证书和身份证书）。



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

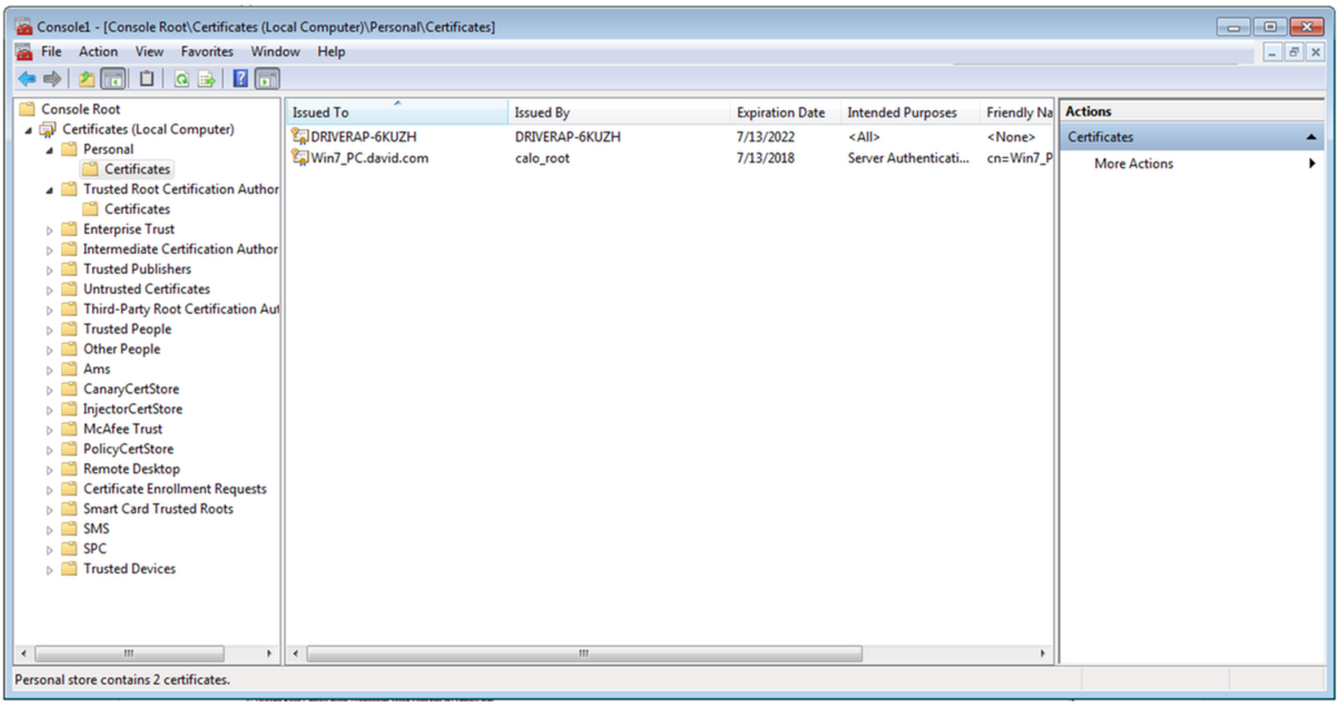
Personal store contains 3 certificates.

步骤16.将CA Certificate从Certificates(Local Computer)>Personal>Certificates拖放到**Certificates(Local Computer)> Trusted Root Certification Authority>Certificates。**



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.i
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	GeoTrus

Trusted Root Certification Authorities store contains 60 certificates.



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

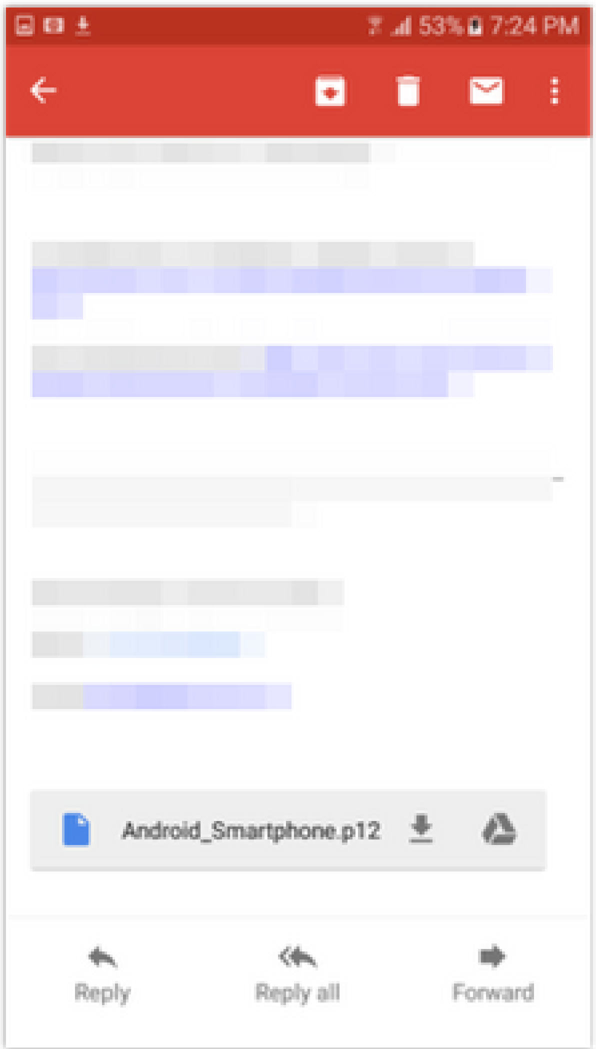
Personal store contains 2 certificates.

如何在Android移动设备上安装身份证书

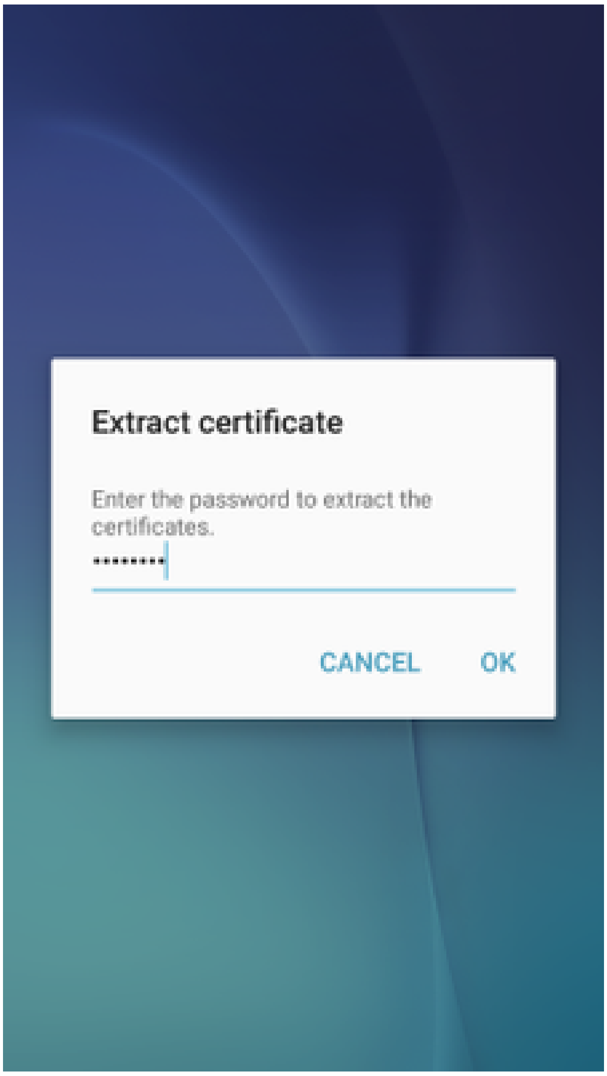
注意：Android支持扩展名为.pfx或.p12的PKCS#12密钥存储文件。

注意：Android仅支持DER编码的X.509 SSL证书。

步骤1.以PKCS12(.p12)格式从IOS CA服务器导出客户端证书后，通过电子邮件将文件发送到Android设备。一旦您在其中，轻触文件名称即可开始自动安装。(**不下载文件**)



步骤2.输入用于导出证书的密码，在本例中，密码为cisco123。

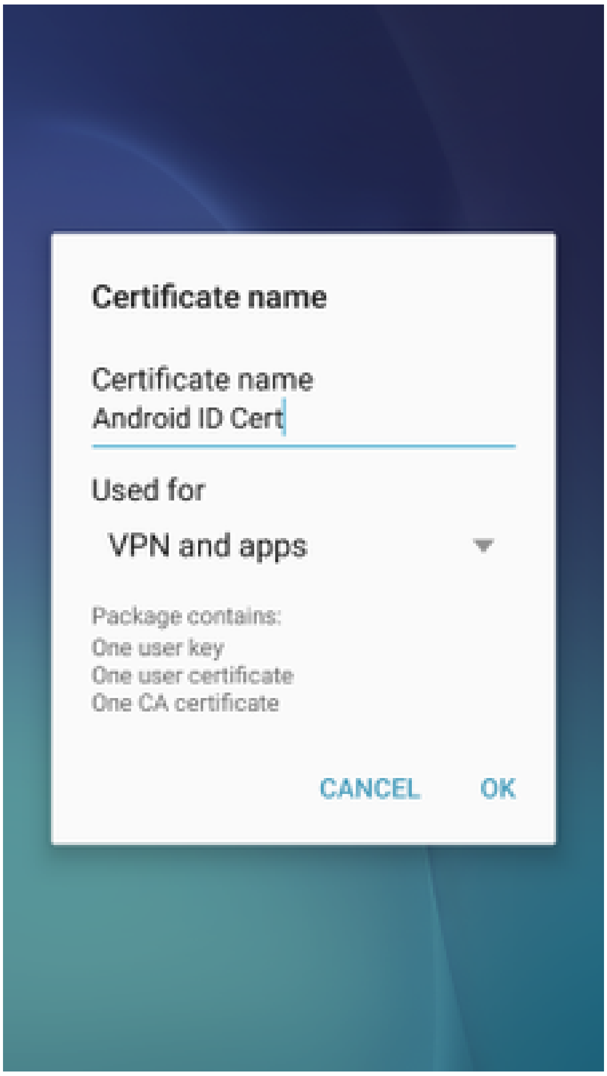


Extract certificate

Enter the password to extract the certificates.

****

步骤3.选择“**确定”**并输入证**书名称**。它可以是任意字，在本例中名称为**Android ID Cert**。



Certificate name

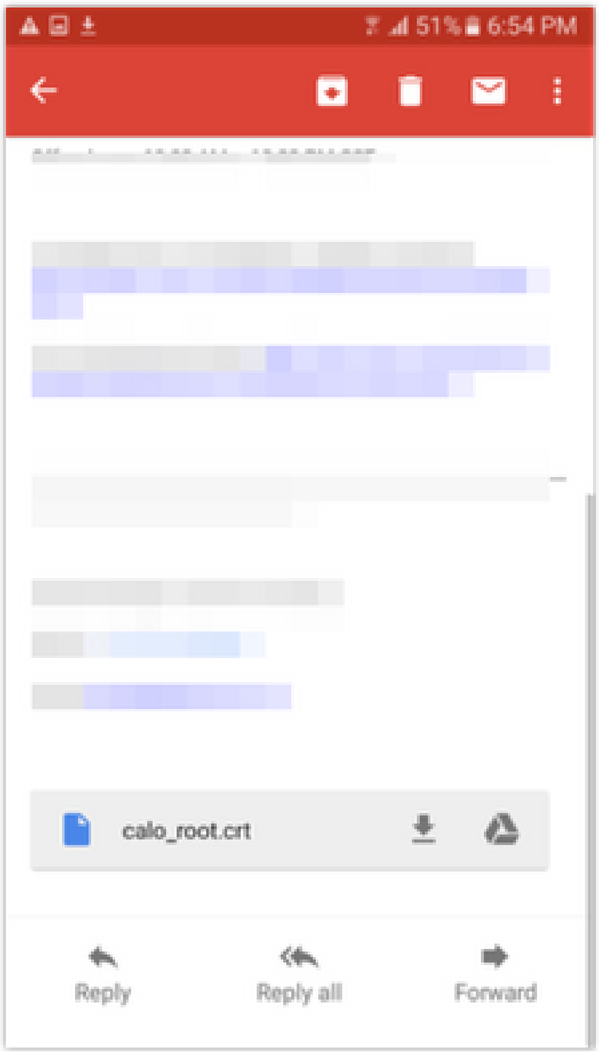
Certificate name
Android ID Cert

Used for
VPN and apps

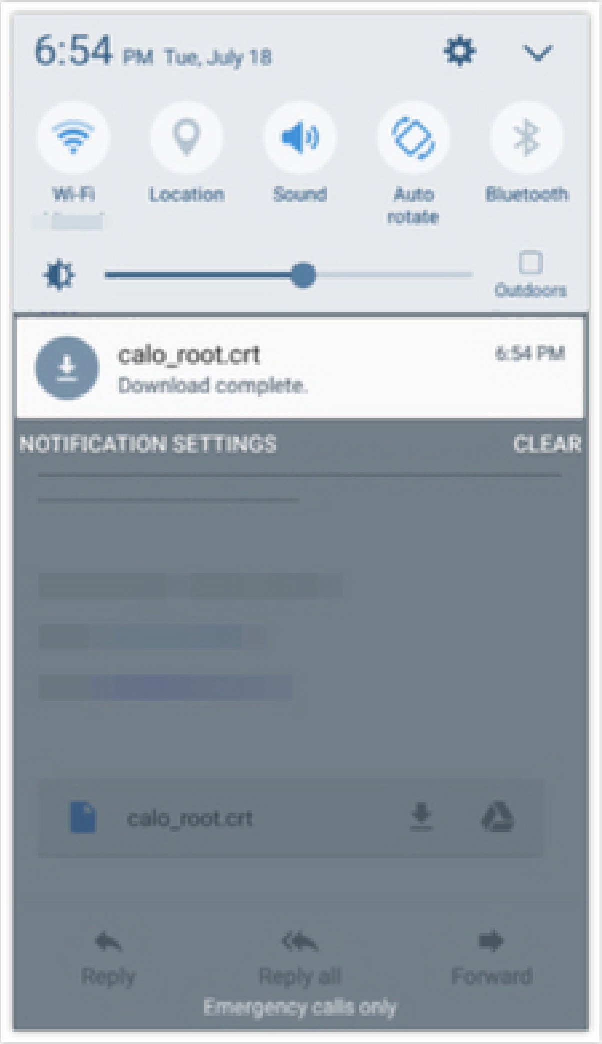
Package contains:
One user key
One user certificate
One CA certificate

步骤4.选择**OK**，并显示消息“Android ID Cert installed”。

步骤5.要安装CA证书，请以base64格式从IOS CA服务器中解压并用.crt扩展名保存。通过电子邮件将文件发送到您的android设备。这次，您需要通过在文件名称旁边的箭头上录音来下载文件。

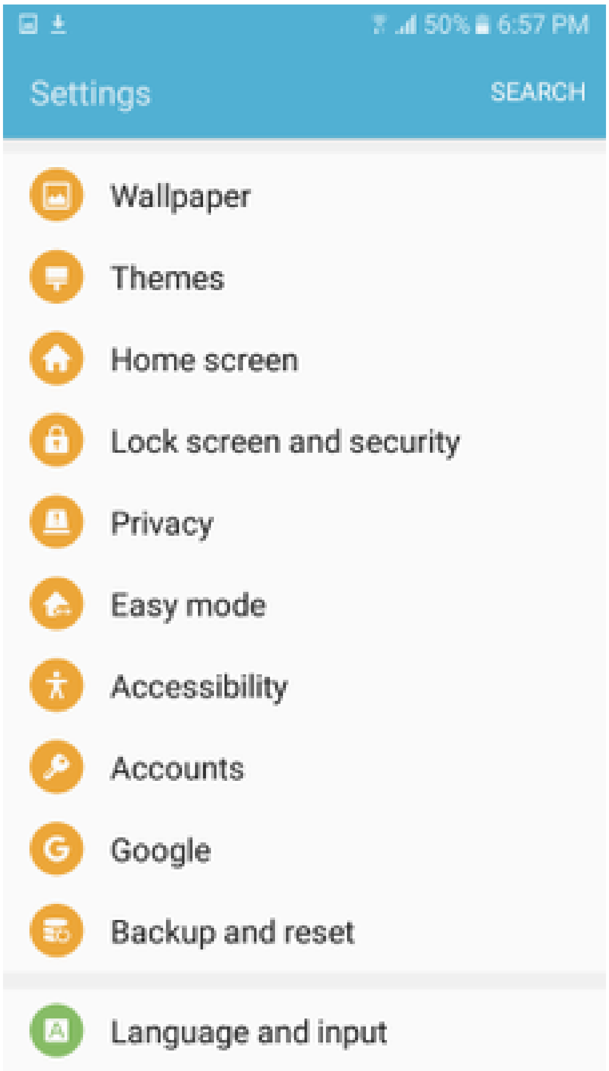


51% 6:54 PM
calo_root.crt
Reply
Reply all
Forward

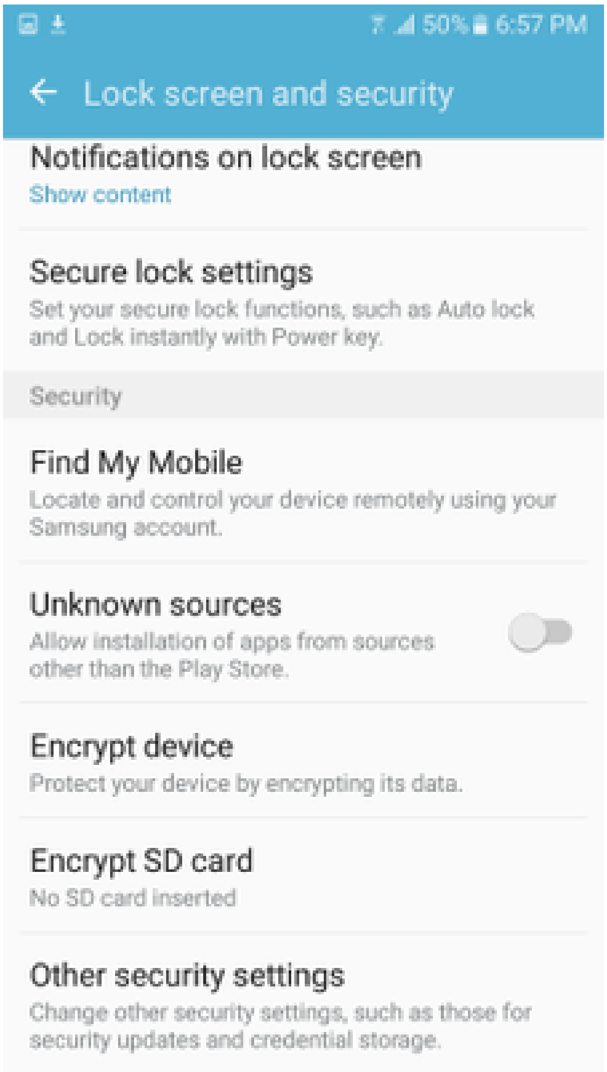


calo_root.crt 6:54 PM
Download complete.

步骤6.导航至“设**置”**和“**锁定”屏幕和安全性。**



步骤7.选择“其**他安全设置”。**



50% 6:57 PM

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.

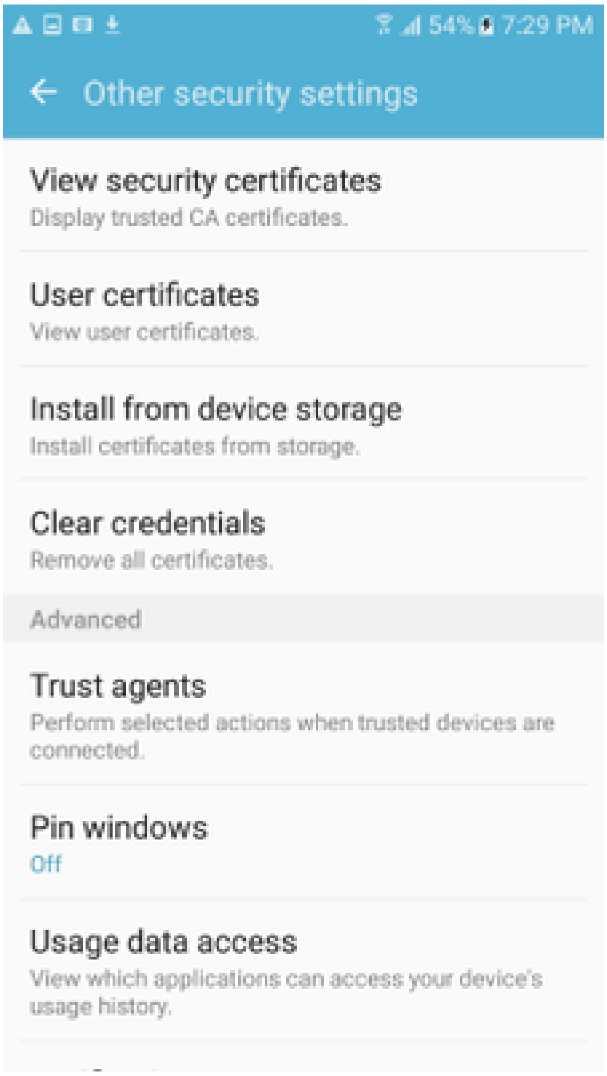
Unknown sources
Allow installation of apps from sources other than the Play Store.

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.

步骤8.导航至“从设**备存储安装”。**



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.

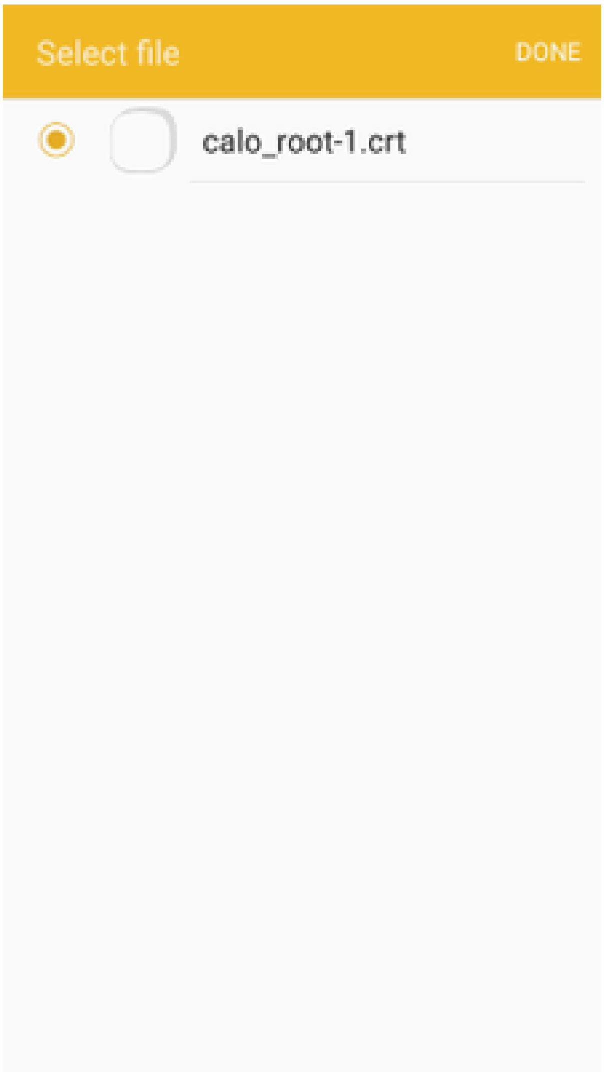
Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows
Off

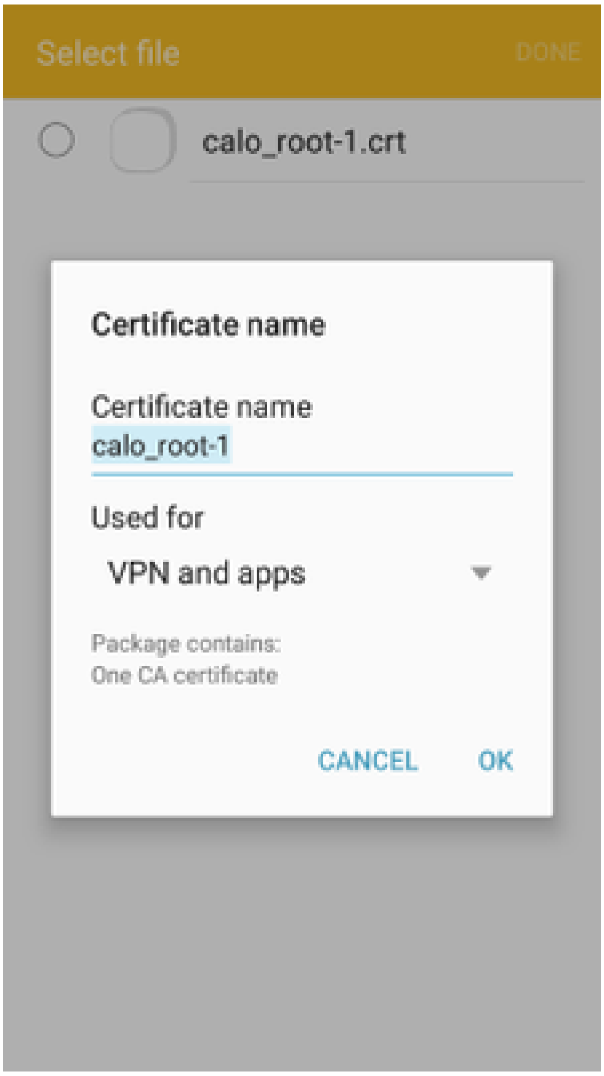
Usage data access
View which applications can access your device's usage history.

步骤9.选择.crt文件，然后轻触“完成”。



◉ calo_root-1.crt

步骤10.输入证**书名称**。它可以是任意字，在本例中，名称**为calo_root-1**。



○ calo_root-1.crt

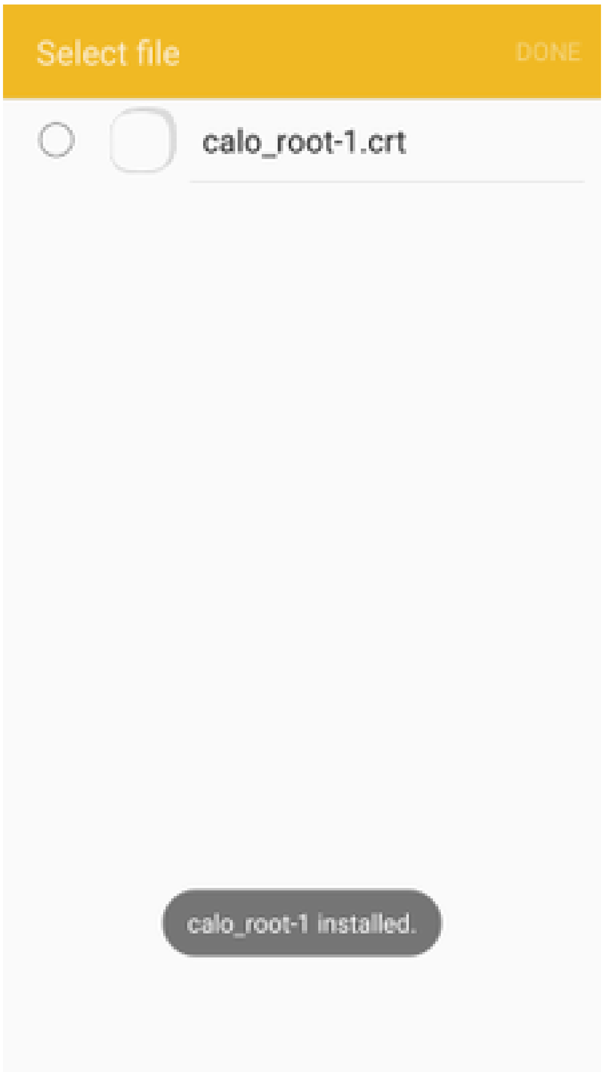
Certificate name

Certificate name
calo_root-1

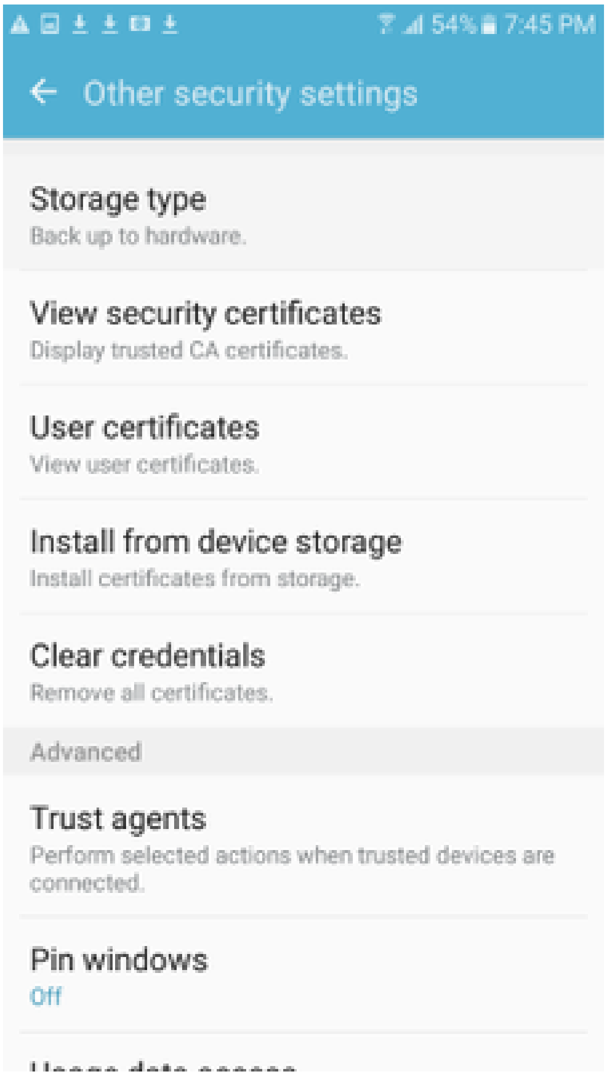
Used for
VPN and apps

Package contains:
One CA certificate

步骤10.选择**OK**，您将看到消息“calo_root-1 installed”。



步骤11.要验证身份证书是否已安装，请导航至**设置/锁定屏幕和安全/其他>安全设置/用户证书/系统选项卡。**



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.

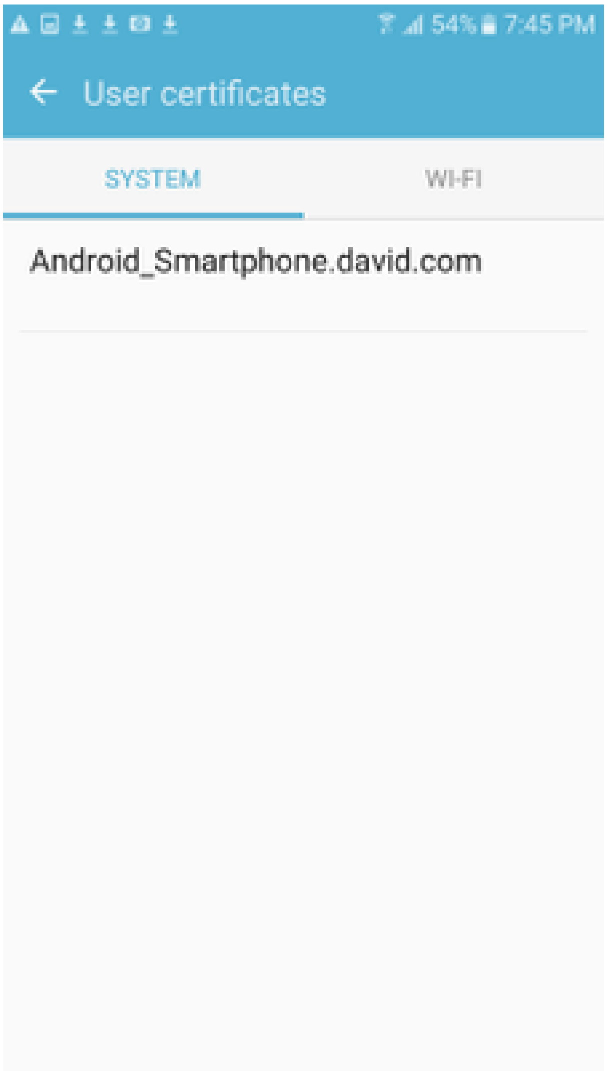
Clear credentials
Remove all certificates.

Advanced

Trust agents
Perform selected actions when trusted devices are connected.

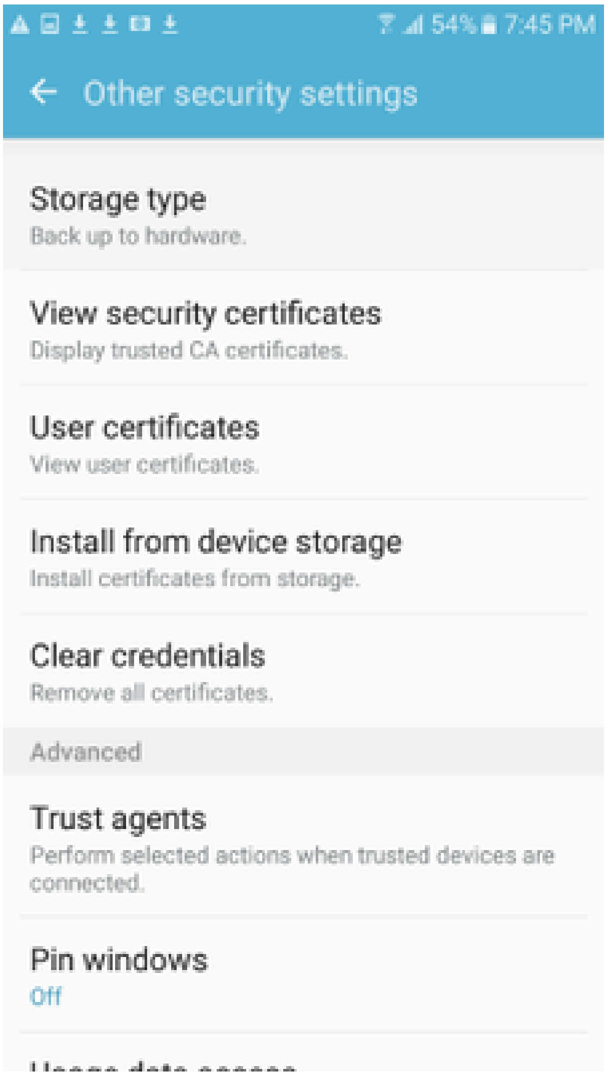
Pin windows
Off

Usage data access



Android_Smartphone.david.com

步骤12.要验证CA证书是否已安装，请导航至**Settings/Lock屏幕和安全/其他安全设置/查看安全证书/User选项卡。**



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.

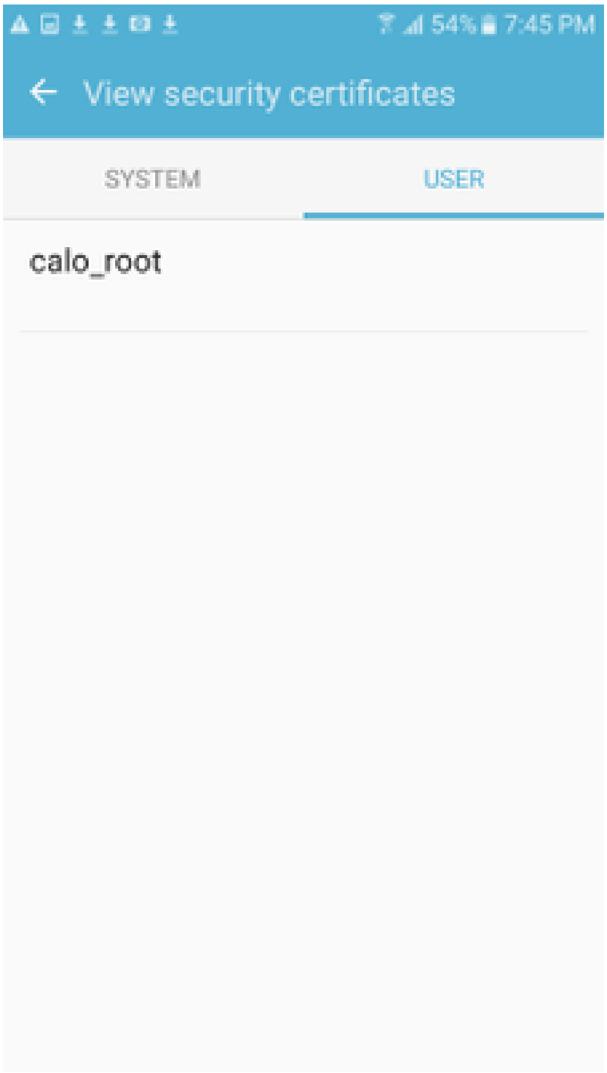
Clear credentials
Remove all certificates.

Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows
Off

Usage data access



calo_root

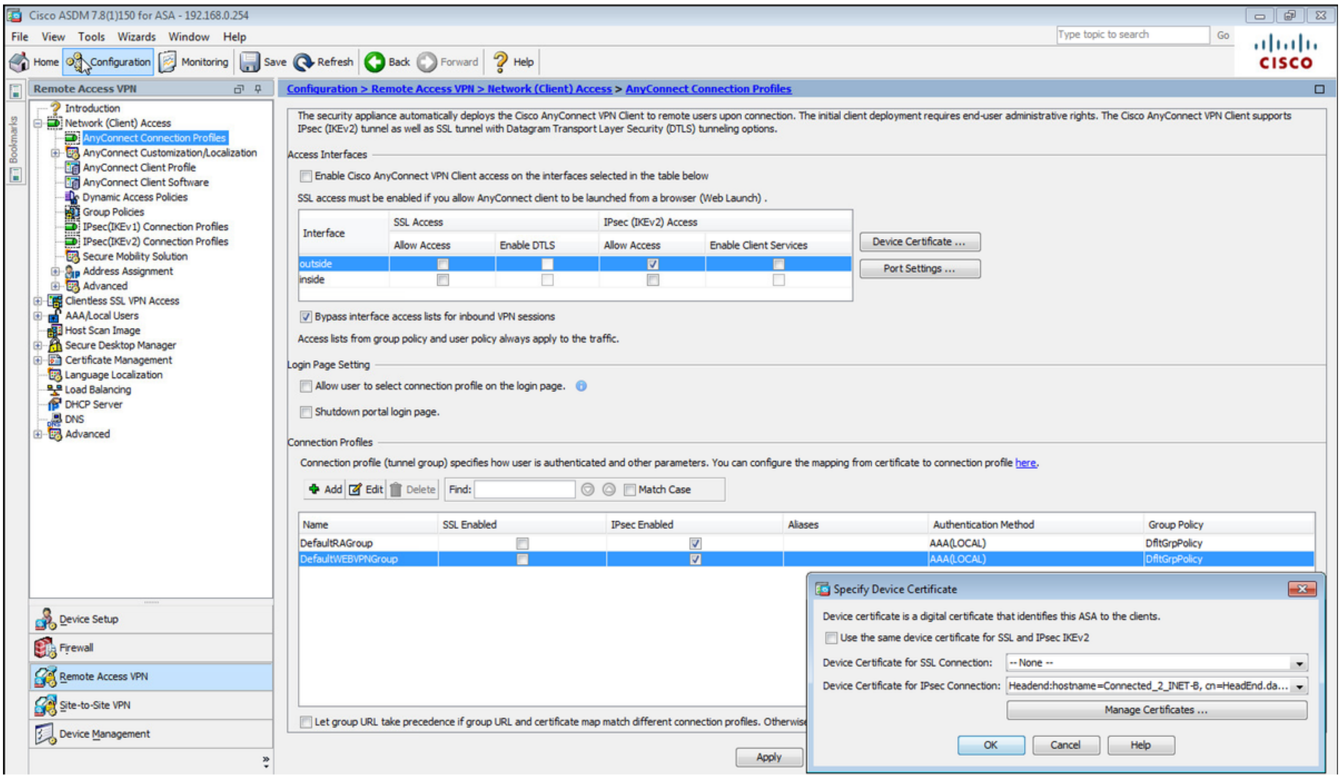
使用IKEv2为RA VPN配置ASA头端

步骤1.在ASDM上，导航至**Configuration>Remote Access VPN > Network(client)Access> Anyconnect Connection Profiles**。选中面**向VPN客户端的接口上的IPSec(IKEv2)访问、允许访问框(不必要选择启用客**户端服务选项)。

步骤2.选择**Device Certificate(设备证**书)并从Use the same device certificate for SSL and IPSec IKEv2(对SSL和IPSec IKEv2使**用同一设备证书)中删除检查标记。**

步骤3.为IPSec连接选择头端证书，并为SSL连接选择 — None —。

此选项将加密ikev2、加密IPSec、加密动态映射和加密映射配置置于适当位置。



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	□	□	□	□

☑ 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.

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. Otherwis

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

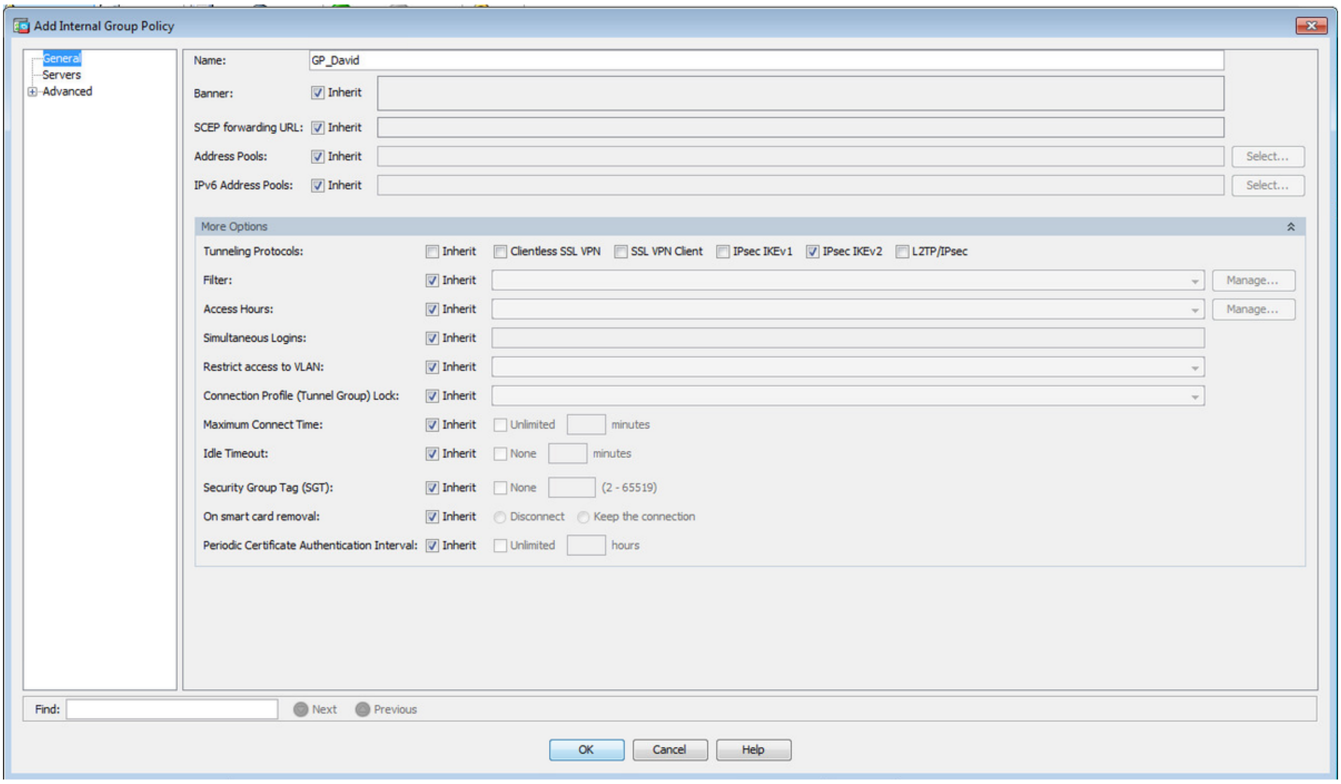
Device Certificate for SSL Connection: -- None --

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

这是配置在命令行界面(CLI)上的显示方式。

```
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
```

步骤4.导航至Configuration > Remote Access VPN > Network(Client)Access > Group Policies以创建组策略



Add Internal Group Policy

- General
- Servers
- Advanced

Name: GP_David

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 ☑ IPsec IKEv2 □ L2TP/IPsec

Filter: ☑ Inherit

Access Hours: ☑ Inherit

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)

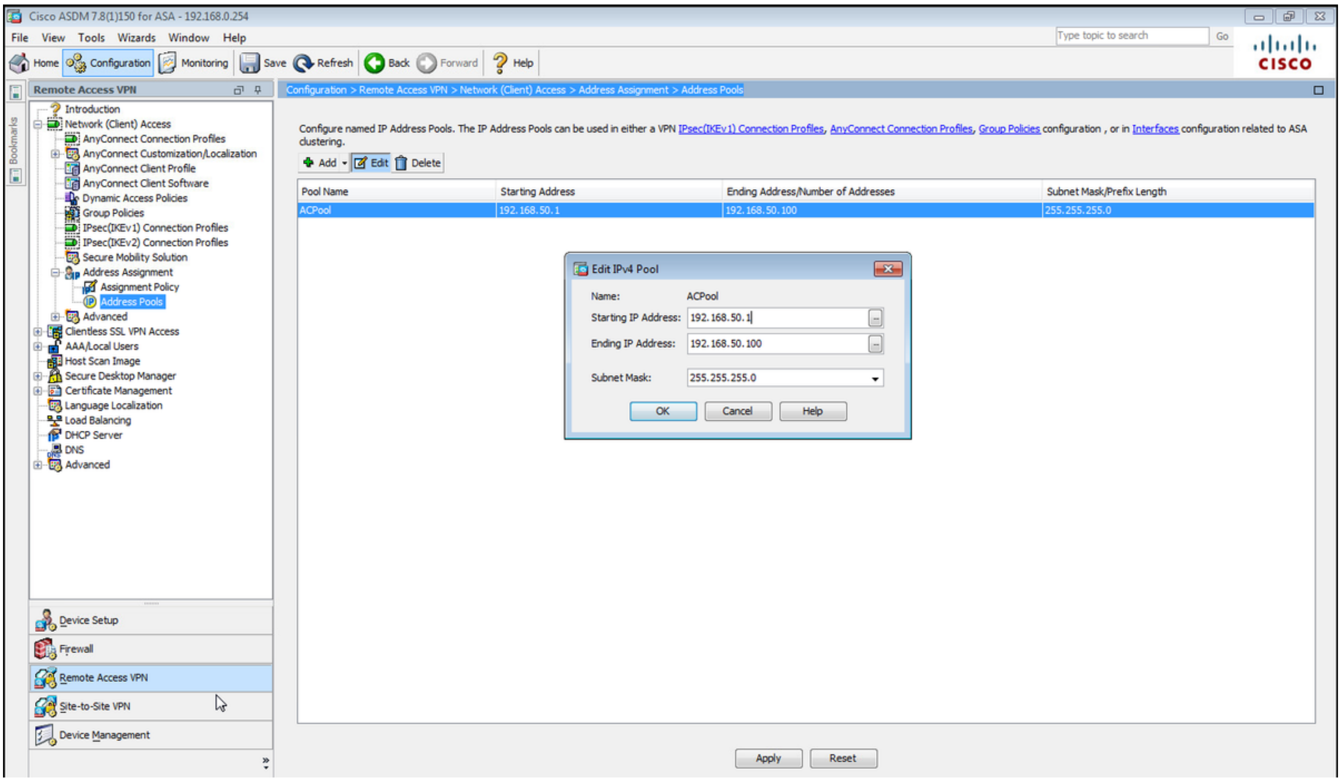
On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Periodic Certificate Authentication Interval: ☑ Inherit □ Unlimited hours

在CLI上。

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

步骤5.导航至**Configuration > Remote Access VPN > Network(Client)Access > Address Pools**，然后选择Add以创建IPv4池。



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

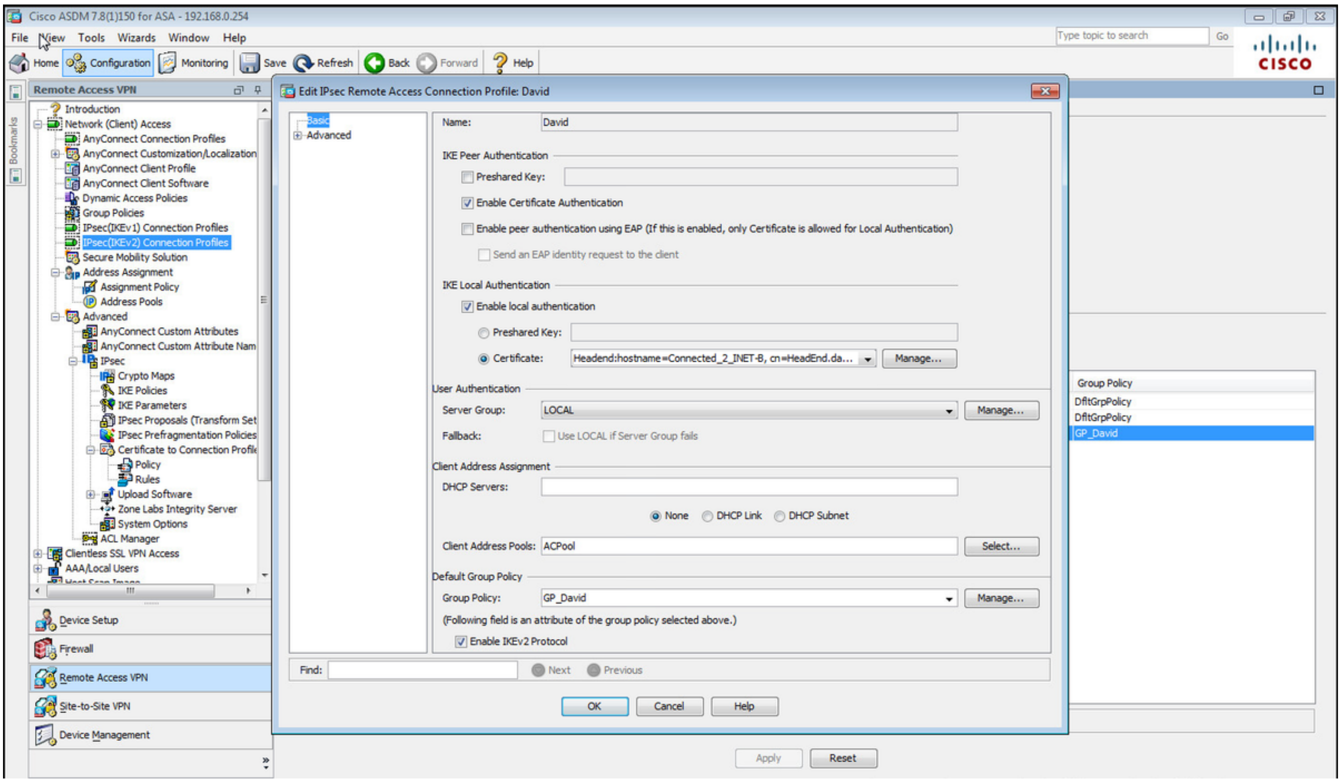
Ending IP Address: 192.168.50.100

Subnet Mask: 255.255.255.0

在CLI上。

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

步骤6.导航至Configuration > Remote Access VPN > Network(Client)Access > IPSec(IKEv2)Connection Profiles，然后选择Add以创建新隧道组。



Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254
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 Profile
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
Group Policy
DfltGrpPolicy
DfltGrpPolicy
GP_David
Apply
Reset

Edit IPsec Remote Access Connection Profile: David

Basic
Advanced

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... Manage...

User Authentication

Server Group: LOCAL Manage...

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: ACPool Select...

Default Group Policy

Group Policy: GP_David Manage...

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

☑ Enable IKEv2 Protocol

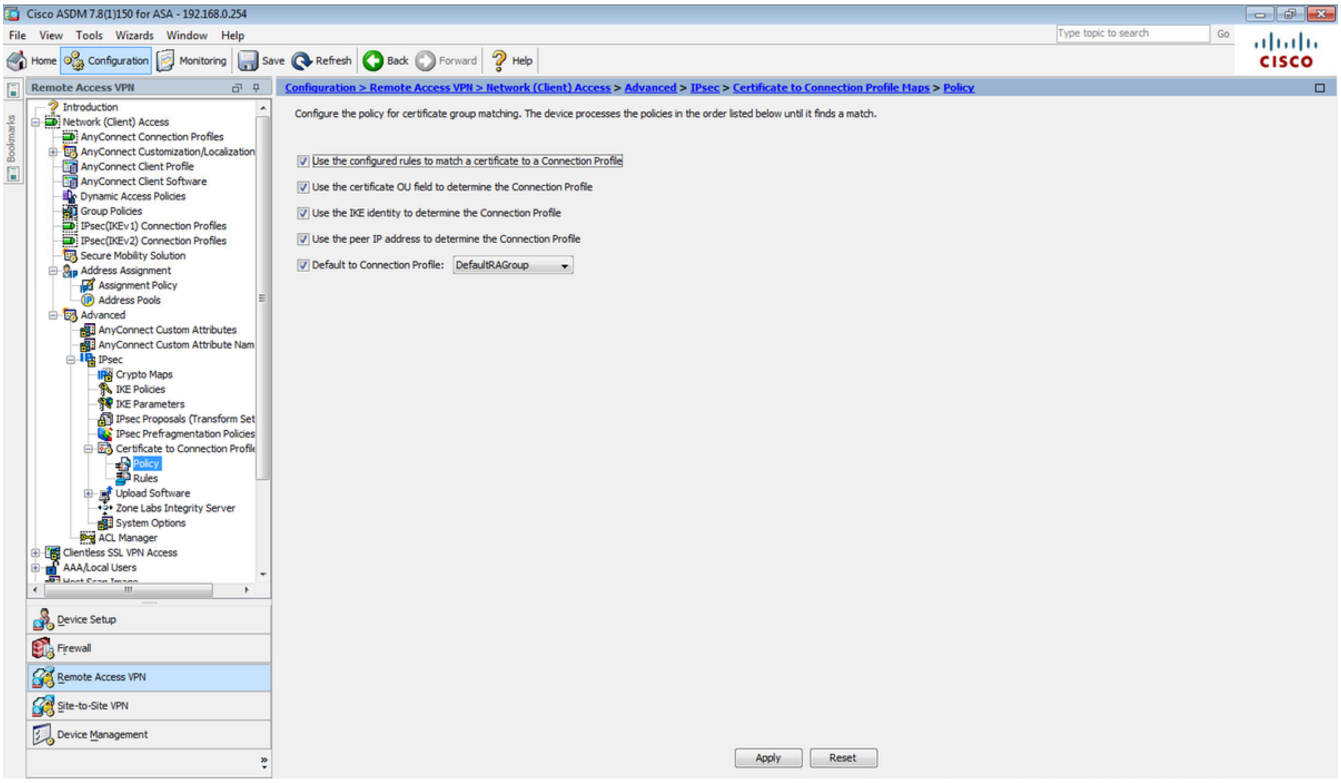
Find: Next Previous

OK Cancel Help

在CLI上。

```
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
```

步骤7.导航至Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy，并选中Used the configured rules to math a certificate to a Connection Profile框。



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 > 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

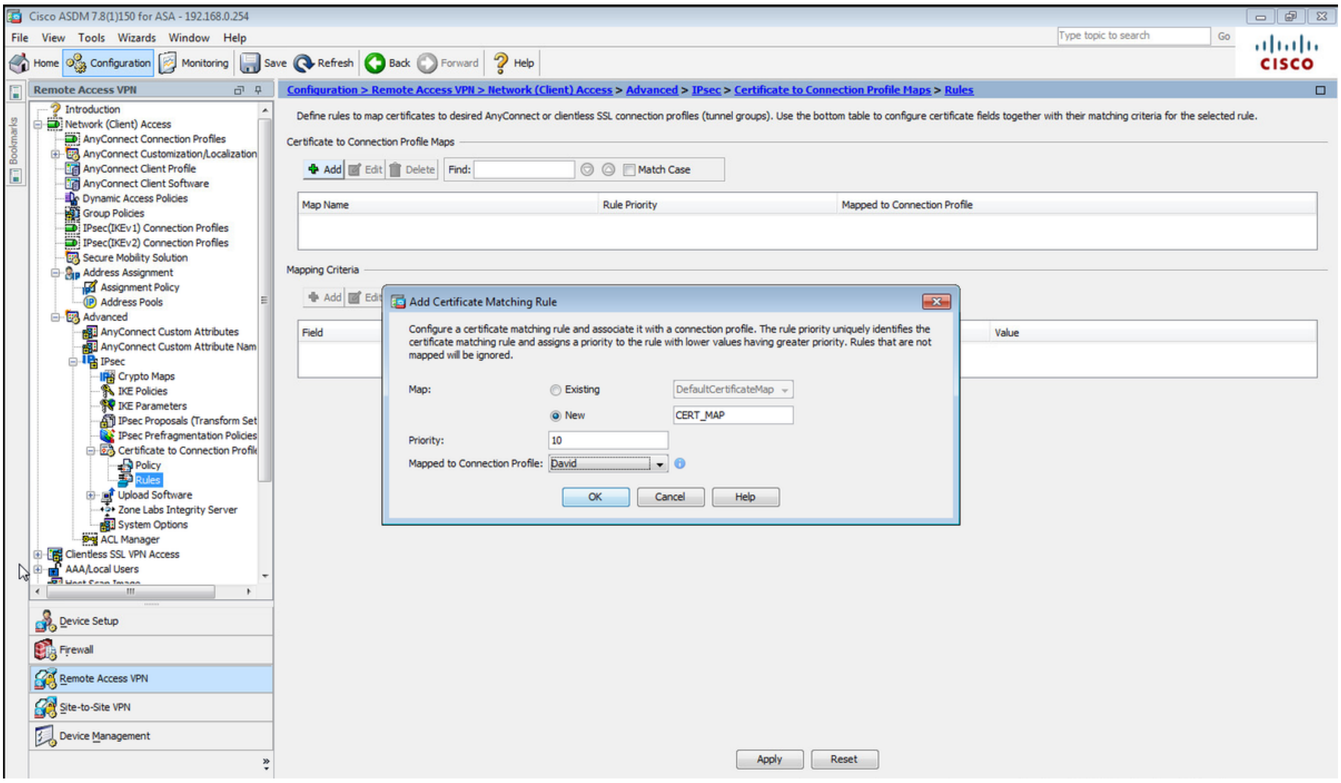
☑ Use the peer IP address to determine the Connection Profile

☑ Default to Connection Profile: DefaultRAGroup

在CLI上。

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

步骤8.导航至**Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules**并创建新的证书映射。选择**Add**并将其关联到隧道组。在本示例中，隧道组命名为**David**。



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

Mapping Criteria

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

在CLI上。

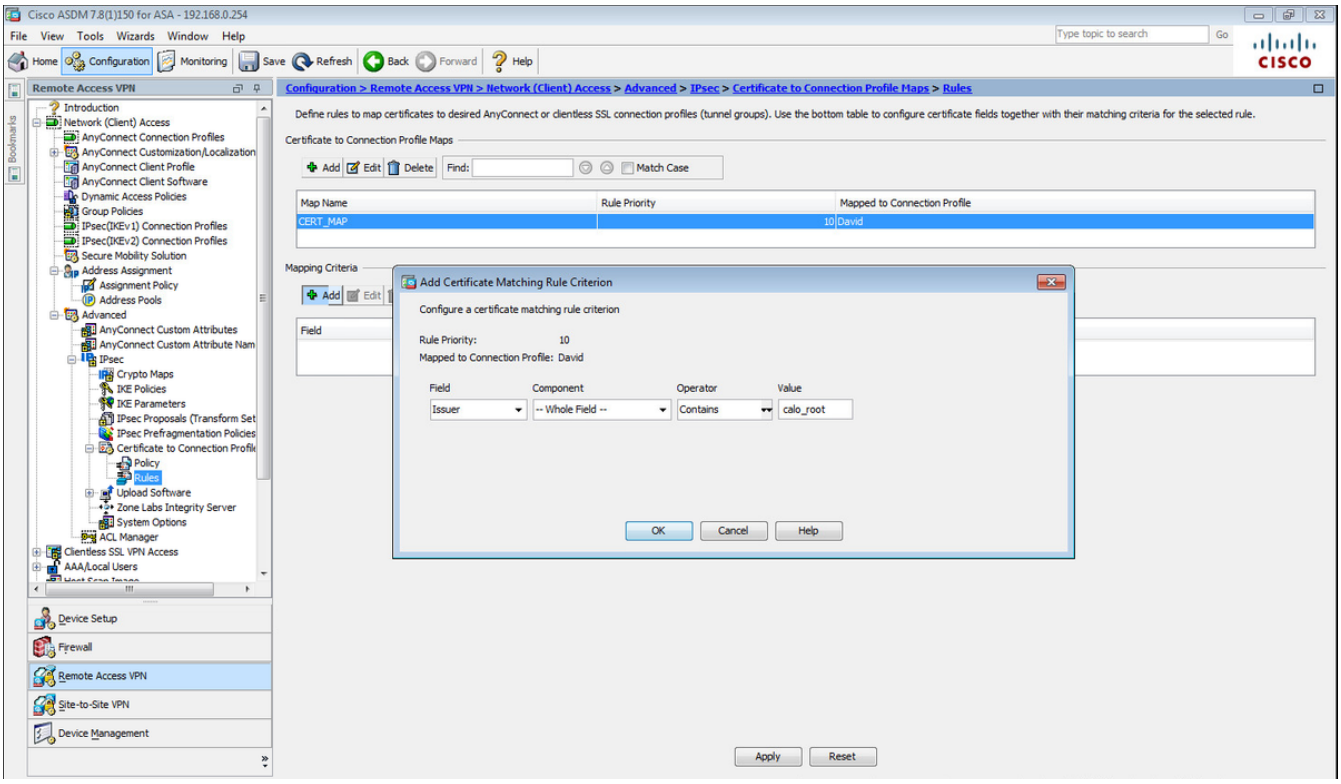
```
tunnel-group-map CERT_MAP 10 David
```

步骤9.在“映**射标**准”部**分选择**添加并输入这些值。

字段:颁发者

操作员：包含

值：calo_root



Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

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

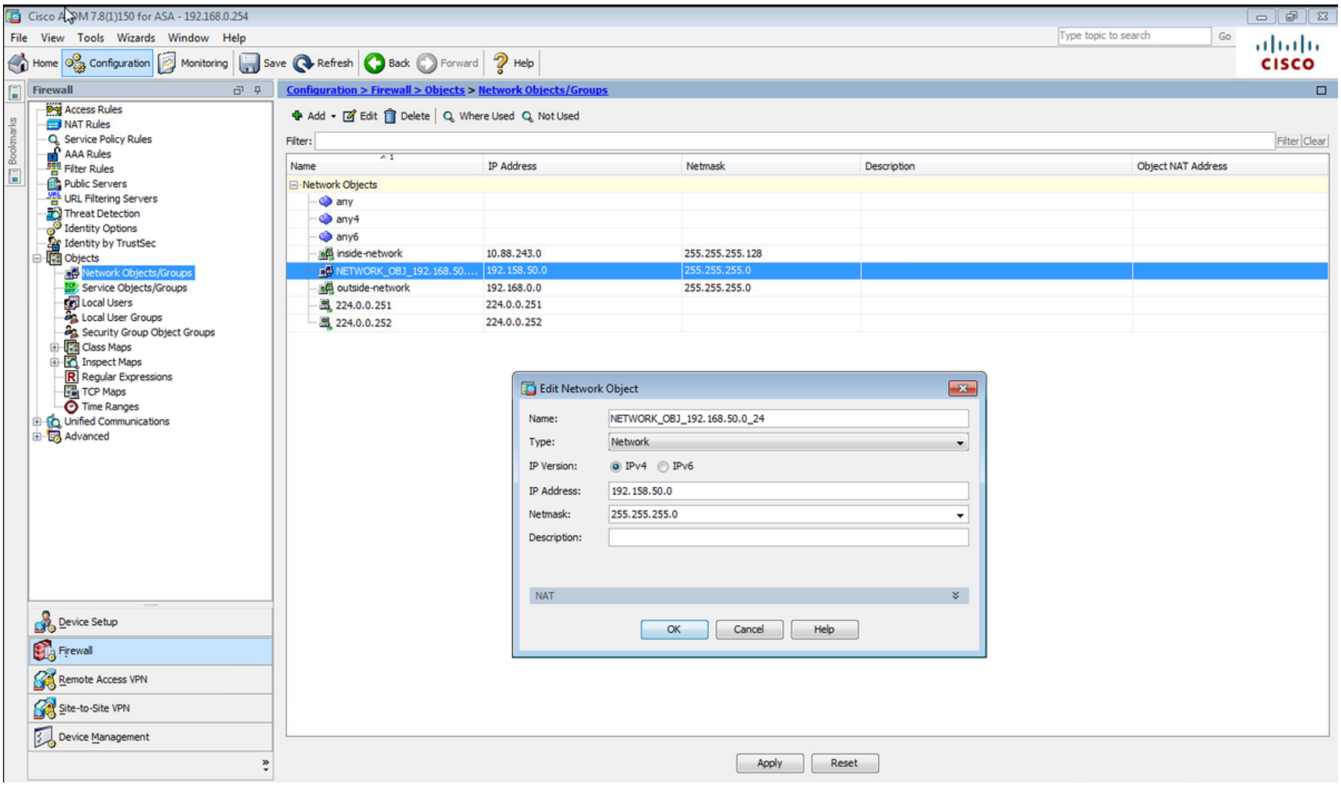
Mapped to Connection Profile: David

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

在CLI上。

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

步骤10.在**Configuration > Firewall > Objects > Network Objects/Groups> Add**下创建一个包含IP池网络的对象，以便添加（网络地址转换）NAT免除规则。



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

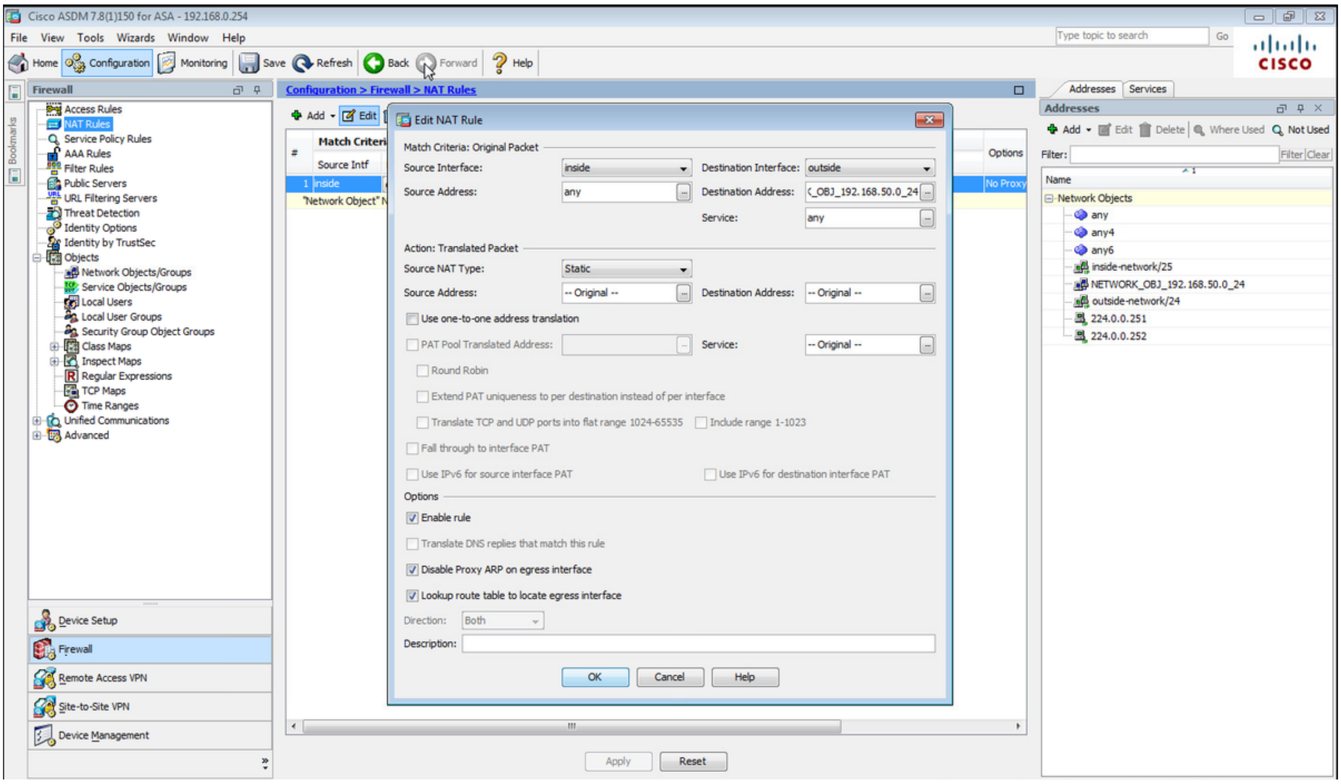
Netmask: 255.255.255.0

Description:

在CLI上。

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

步骤11.导航至**Configuration > Firewall > NAT Rules**，并选择**Add**为RA VPN流量创建NAT免除规则。



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:

在CLI上。

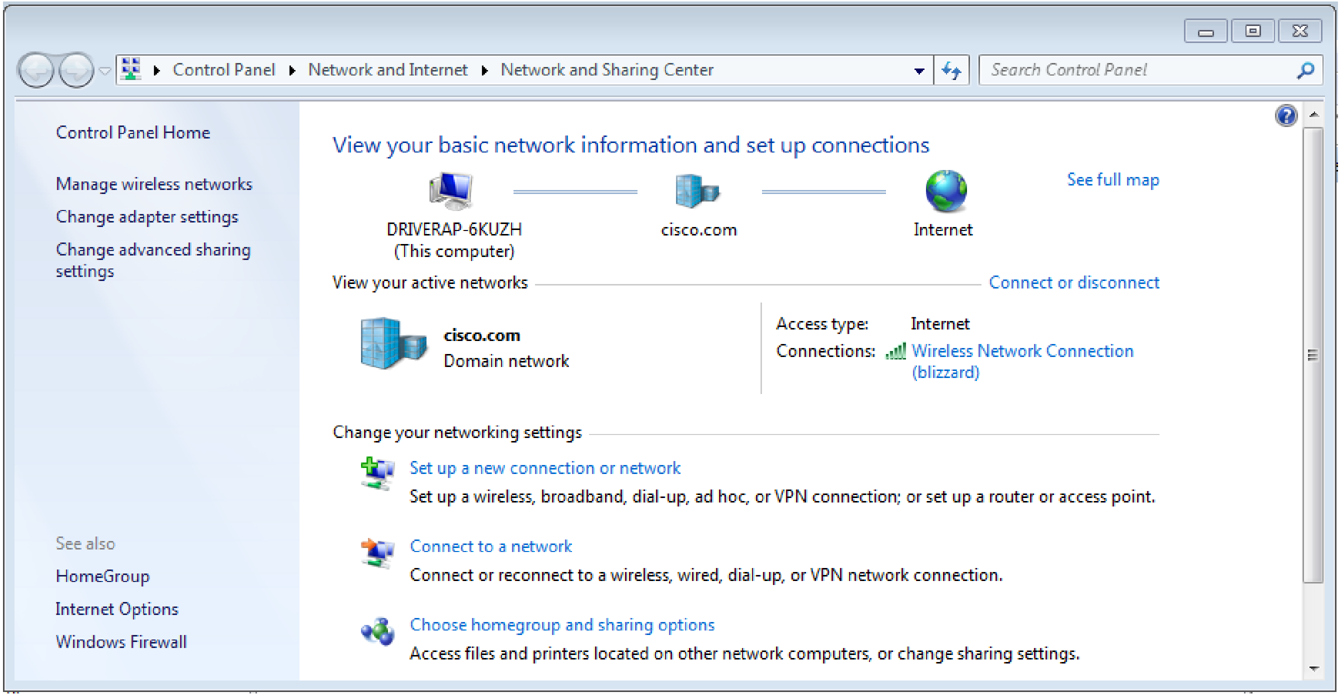
```
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup
```

这是本示例使用的完整ASA配置。

```
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
```

配置Windows 7内置客户端

步骤1.导航至“控**制面板”>“网络和Internet”>“网络和共享中心”**。



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

View your active networks — Connect or disconnect

cisco.com
Domain network

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

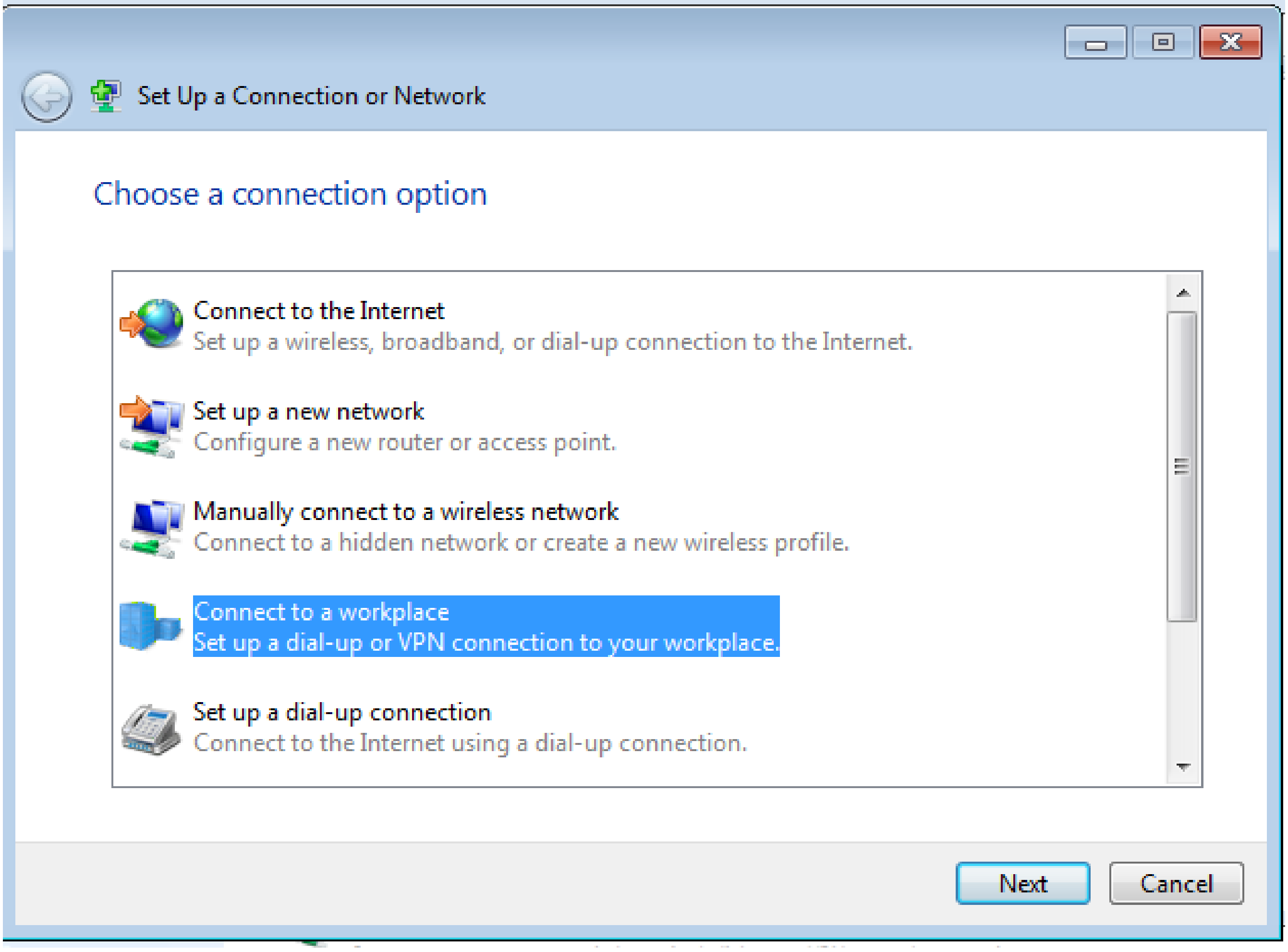
Change your networking settings

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.

步骤2.选择**Set up a new connection or network**。



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.

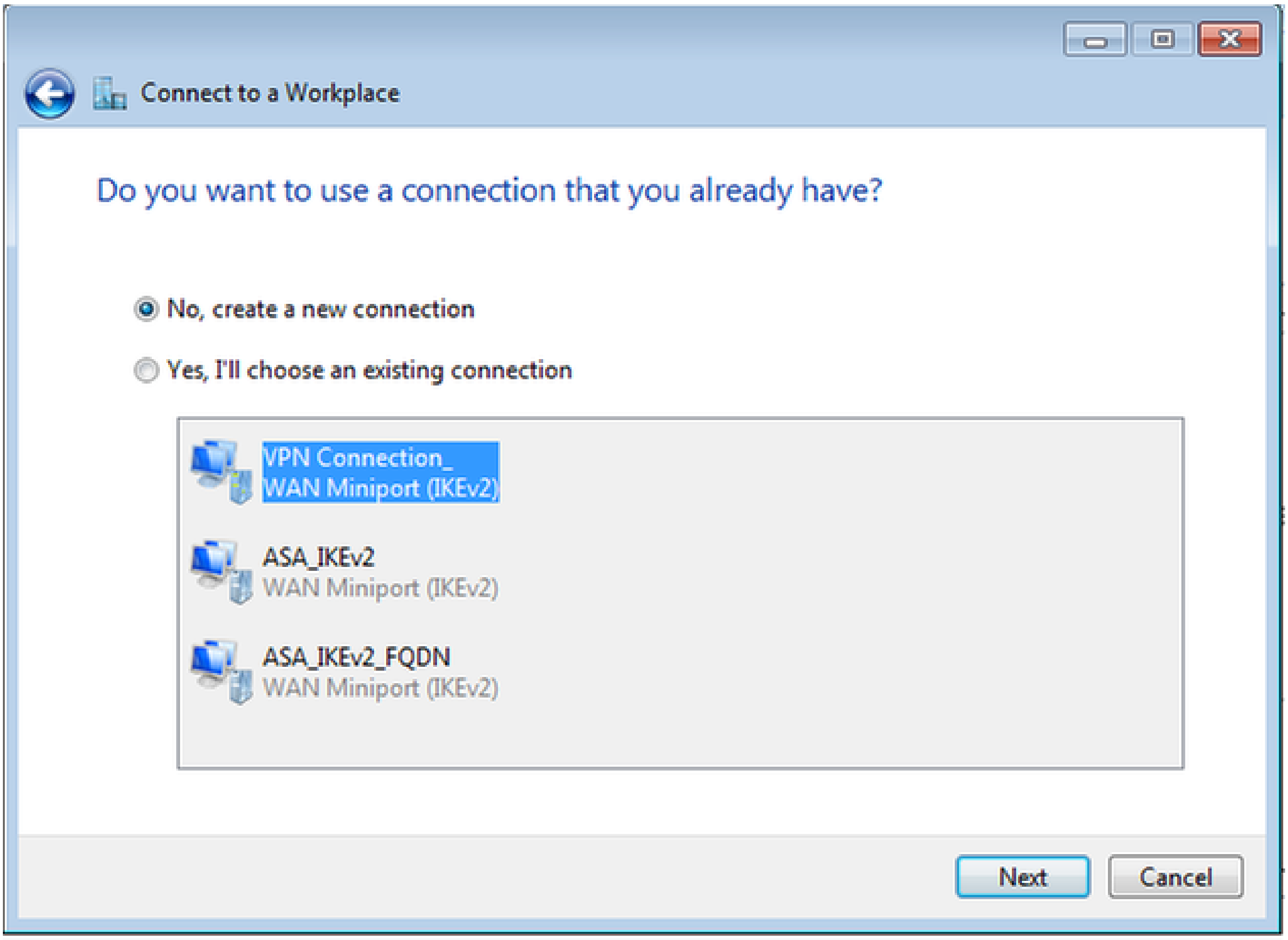
Set up a new network
Configure a new router or access point.

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.

步骤3.选择“连**接到工作区”**和“下**一步”**。



Connect to a Workplace

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

● No, create a new connection

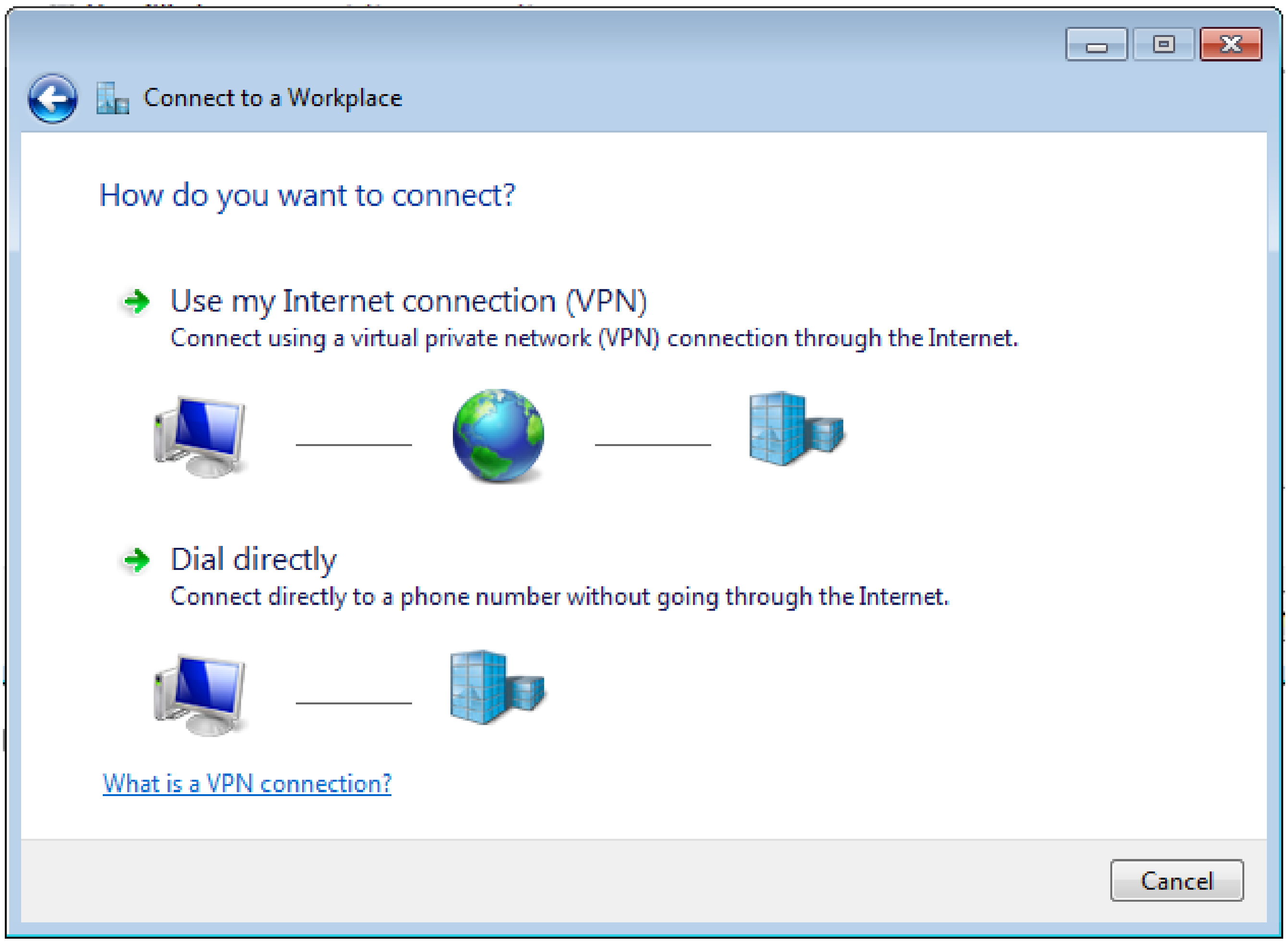
○ Yes, I'll choose an existing connection

VPN Connection_
WAN Miniport (IKEv2)

ASA_IKEv2
WAN Miniport (IKEv2)

ASA_IKEv2_FQDN
WAN Miniport (IKEv2)

步骤4.选择“**否”，创建新连接**，然后**选择“下**一步”。



Connect to a Workplace

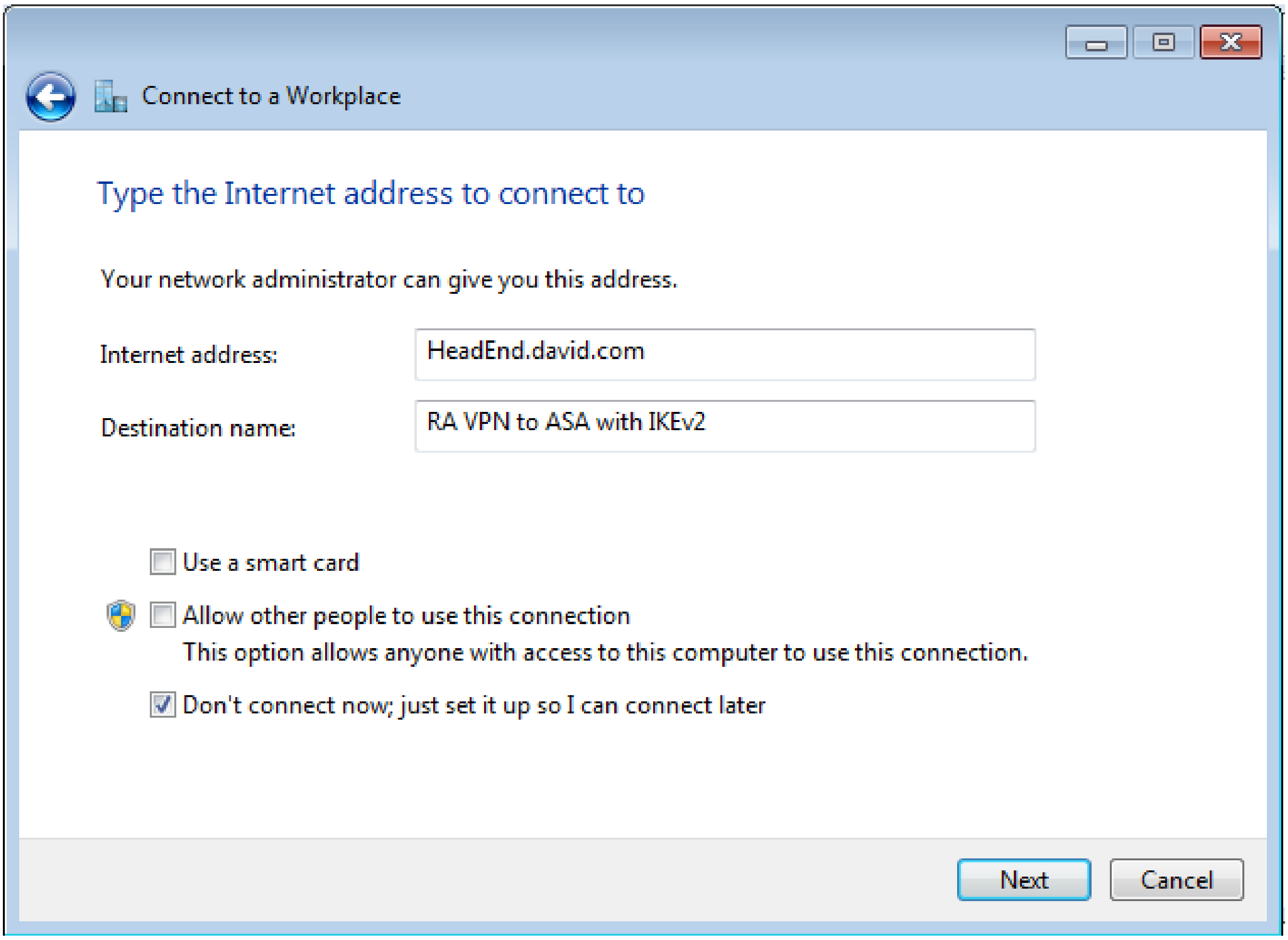
How do you want to connect?

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?

步骤5.选择**使用我的Internet连接(VPN)**，并在Internet地址字段中添加HeadEnd证书公用名**(CN)字**符串。在“目**标名称**”字段中，键入连接的名称。它可以是任何字符串。请确保选中“**立即不连接；只需设置它，以便我稍后连**接。



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: HeadEnd.david.com

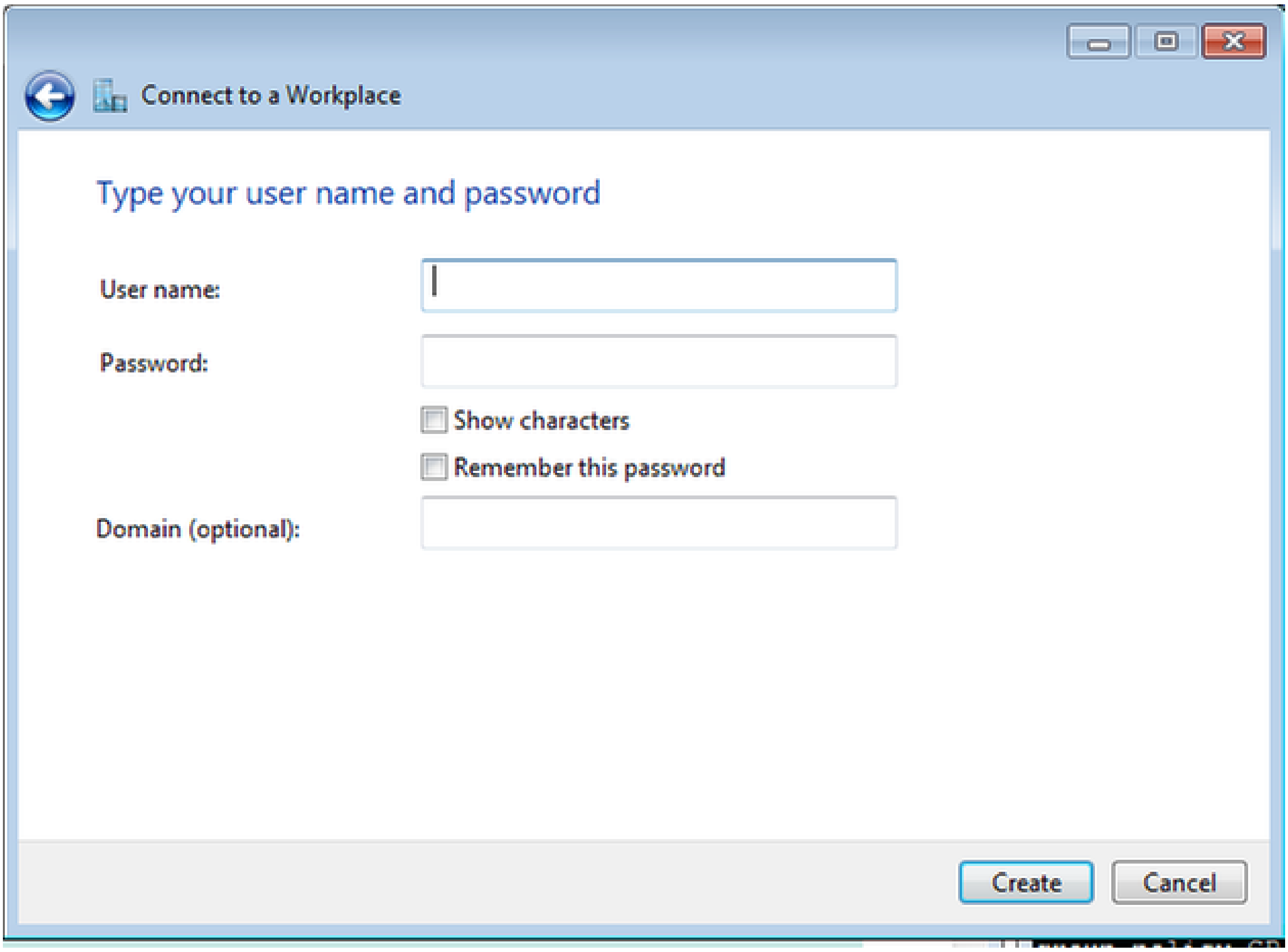
Destination name: RA VPN to ASA with IKEv2

□ 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

步骤6.选择“下**一步**”。



Connect to a Workplace

Type your user name and password

User name:

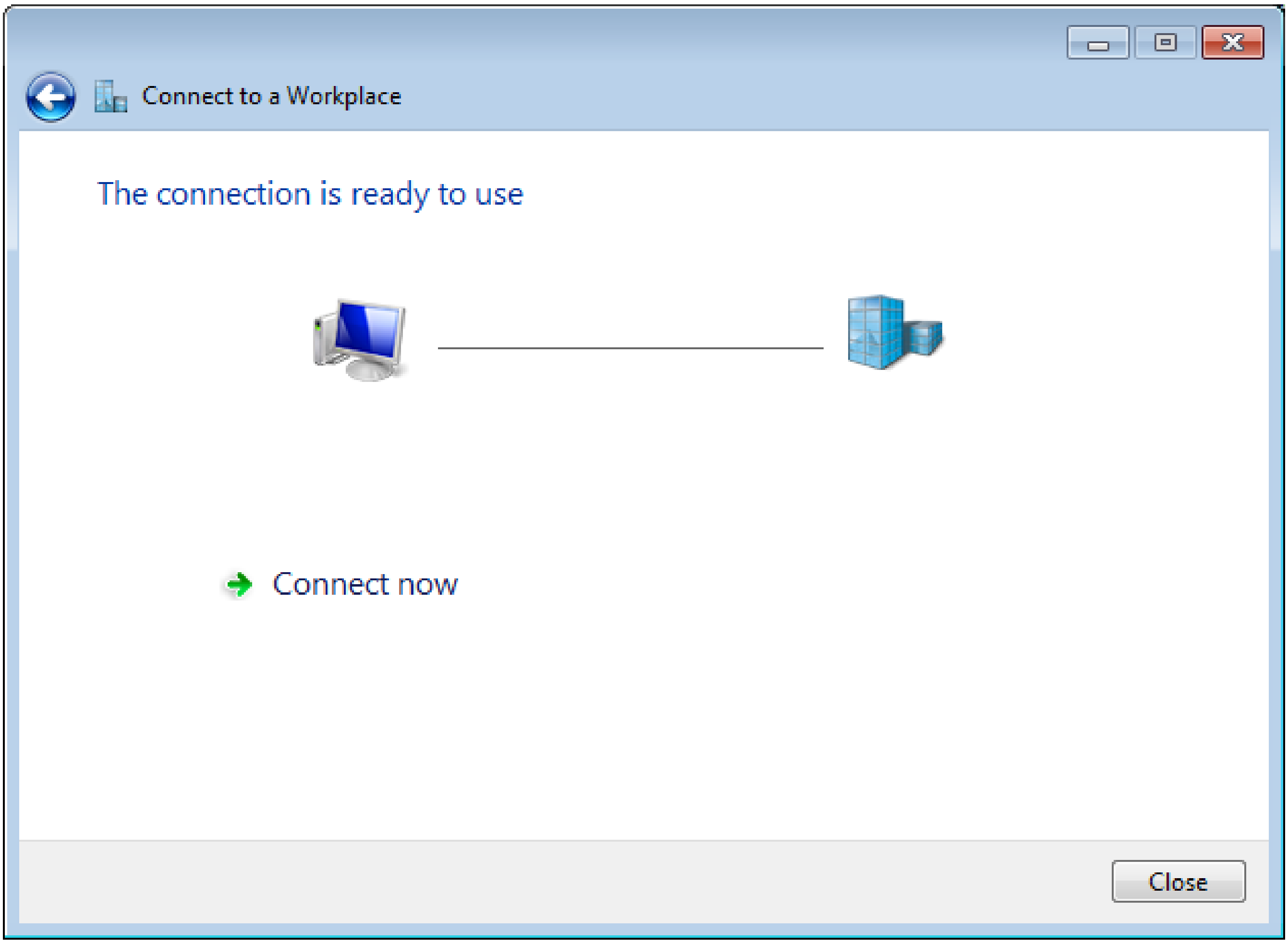
Password:

□ Show characters

□ Remember this password

Domain (optional):

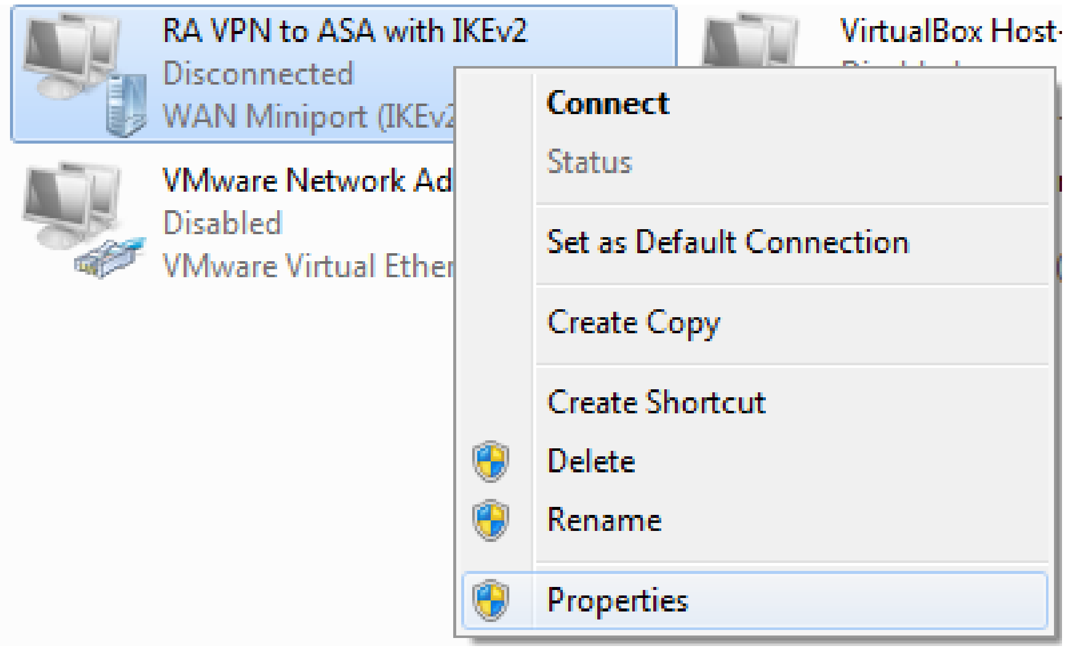
步骤7.选择“创**建”**。



Connect to a Workplace

The connection is ready to use

步骤8.选择“关**闭”**并导航**至“控制面板”>“网络和Internet”>“网络连接”**。选择创建的网络连接，然后右键点击它。选择属性。

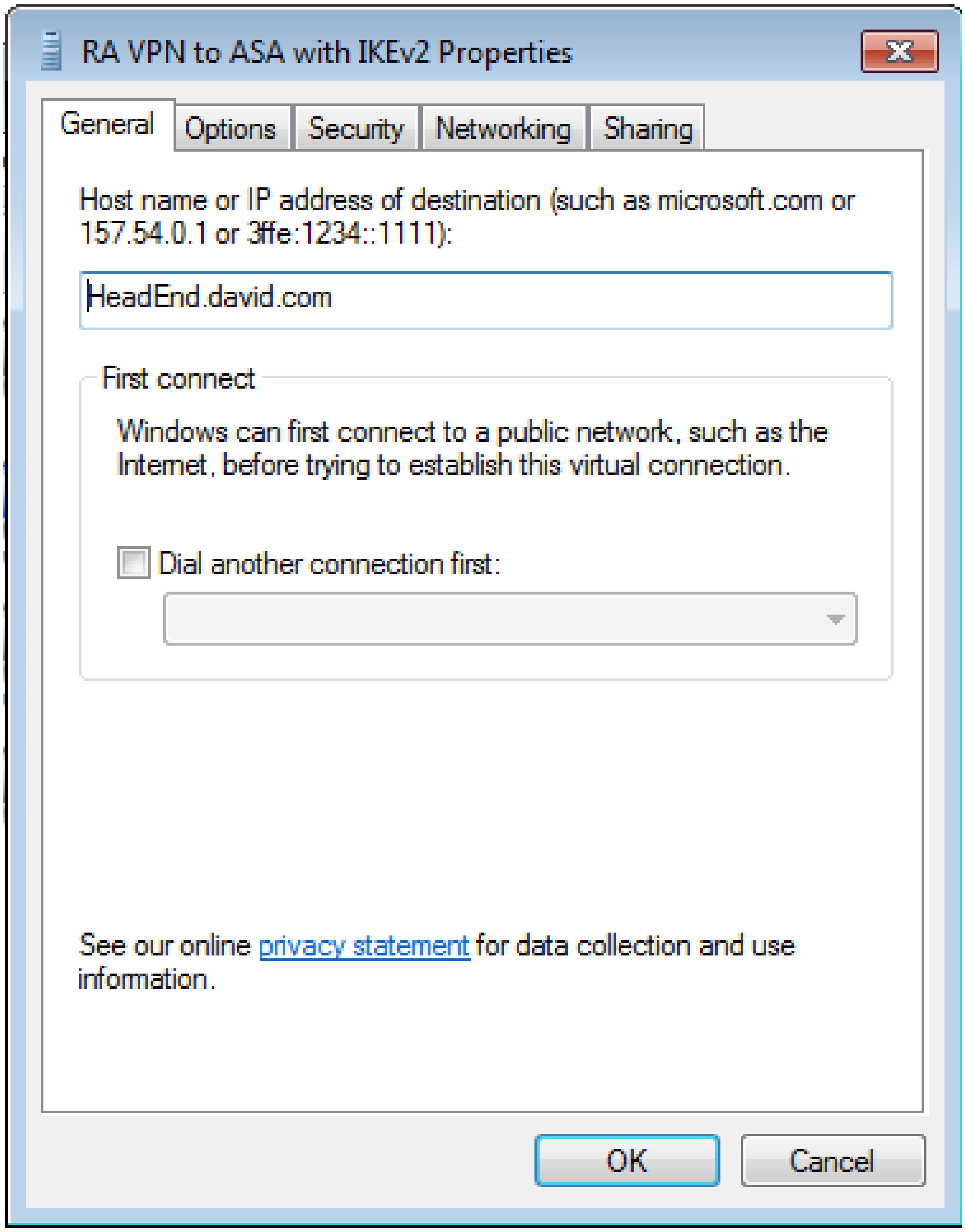


RA VPN to ASA with IKEv2
Disconnected
WAN Miniport (IKEv2

VMware Network Ad
Disabled
VMware Virtual Ether

VirtualBox Host-

步骤9.在“常**规”**选项卡中，您可以验证头端的适当主机名是否正确。您的计算机会将此名称解析为用于连接RA VPN用户的ASA IP地址。



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

HeadEnd.david.com

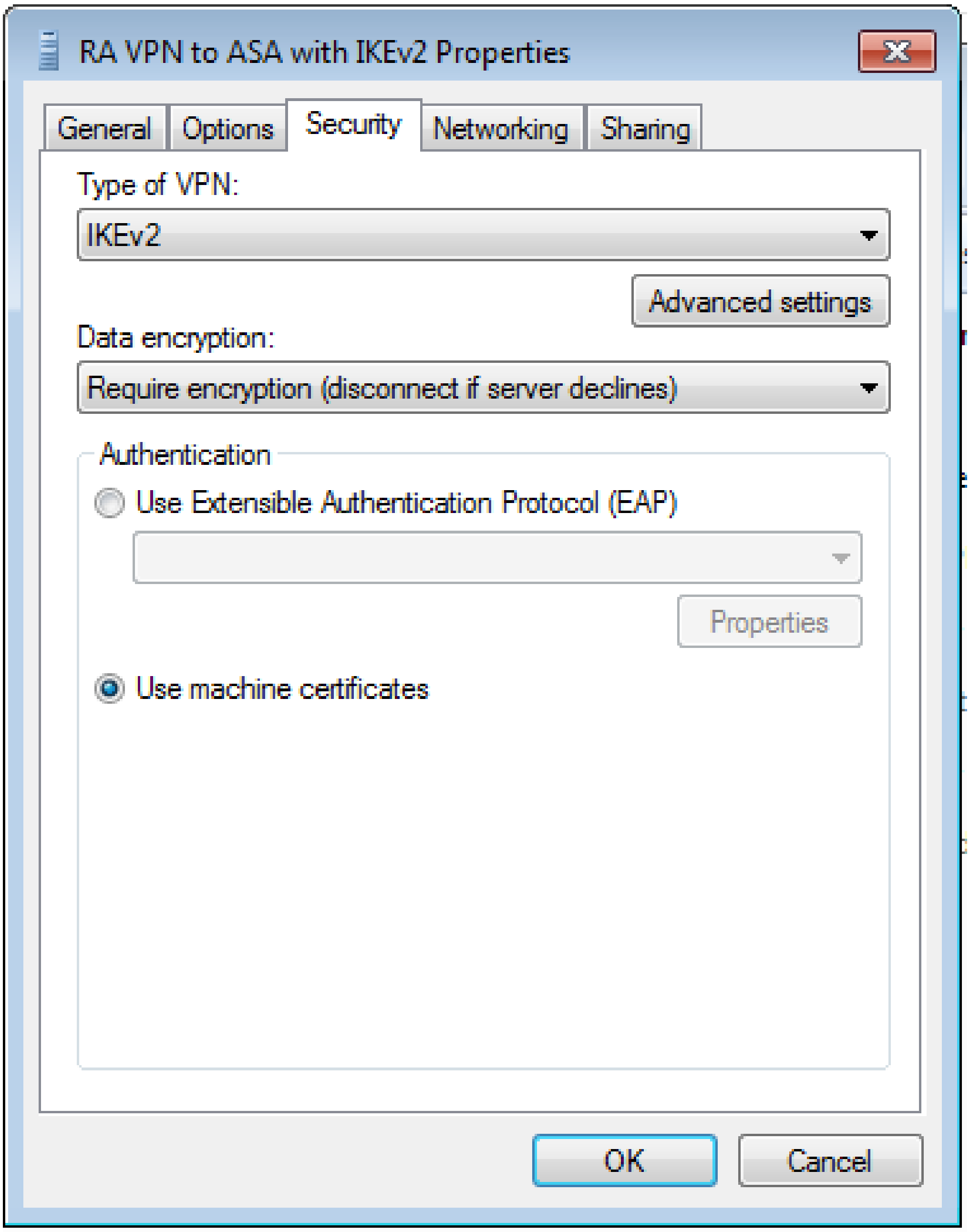
First connect

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.

步骤10.导航至“安**全”**选项卡，**并选择IKEv2**作为**VPN的类型**。在“身份验**证”部**分中，选**择“使用计算机证**书”。



RA VPN to ASA with IKEv2 Properties

Type of VPN: IKEv2

Data encryption: Require encryption (disconnect if server declines)

Authentication

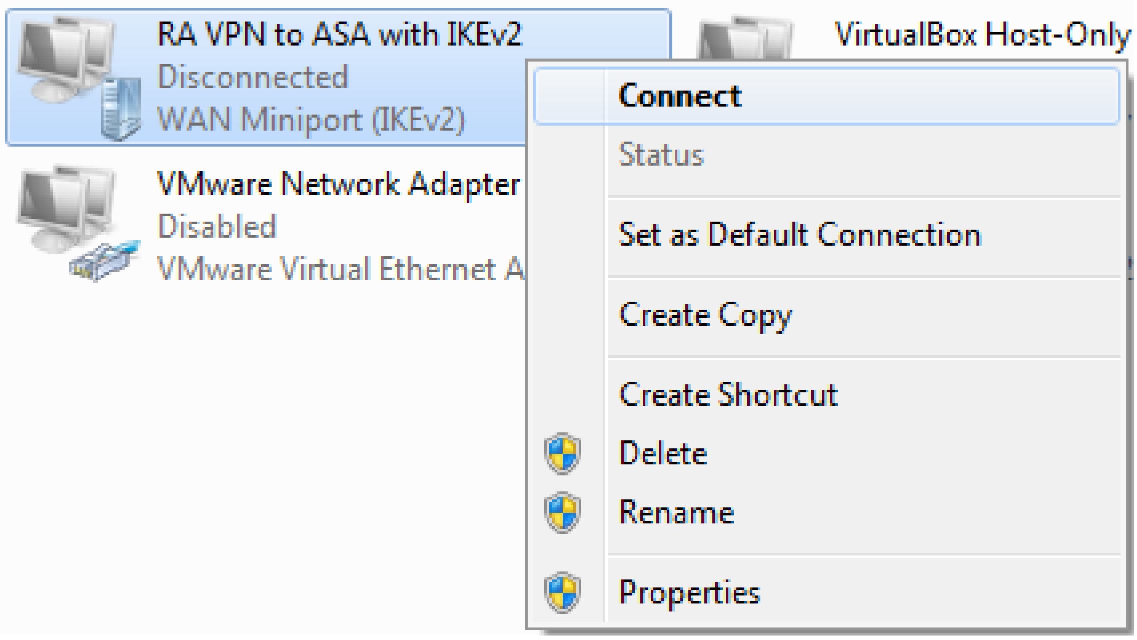
○ Use Extensible Authentication Protocol (EAP)

● Use machine certificates

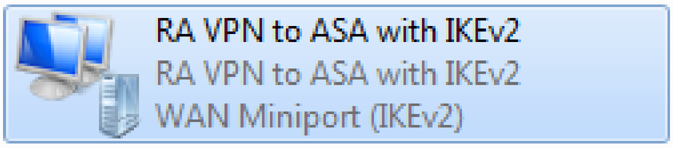
步骤11.选择OK并导航至C:\Windows\System32\drivers\etc。使用文本编辑器打开hosts文件。配置条目，将网络连接中配置的（完全限定域名）FQDN解析为ASA头端的IP地址（在本例中为外部接口）。

```
# 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
```

步骤12.返回“控制面板”>“网络和Internet”>“网络连接”。选择您创建的网络连接。右键单击它并选择“连接”。



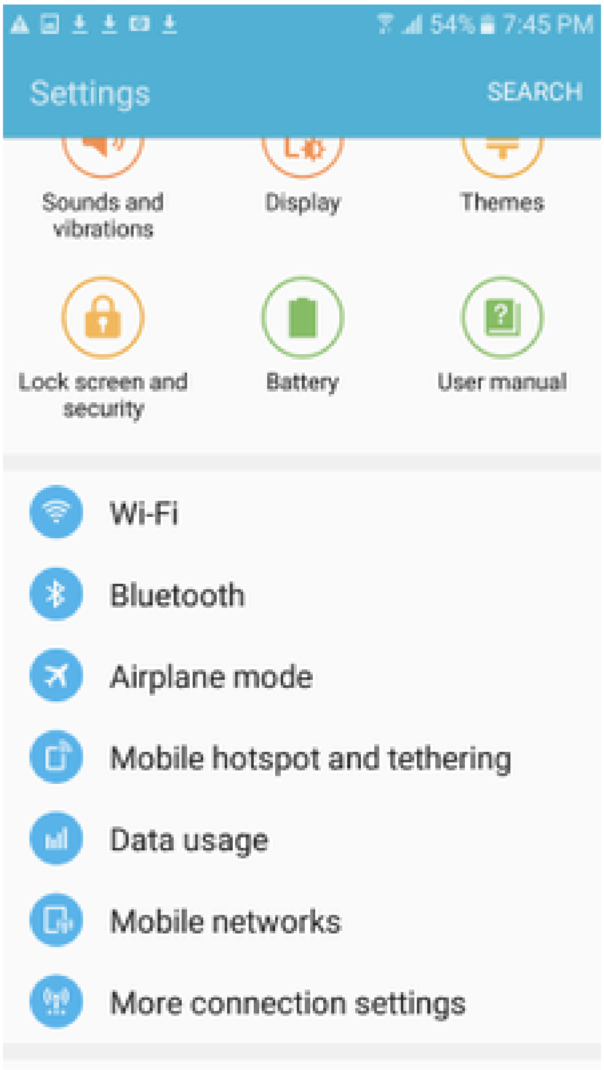
步骤13.网络连接状态从“已断开”(Disconnected)转变为“连接”(Connecting)，然后转变为“已连接”(Connected)。最后，显示您为网络连接指定的名称。



此时计算机已连接到VPN头端。

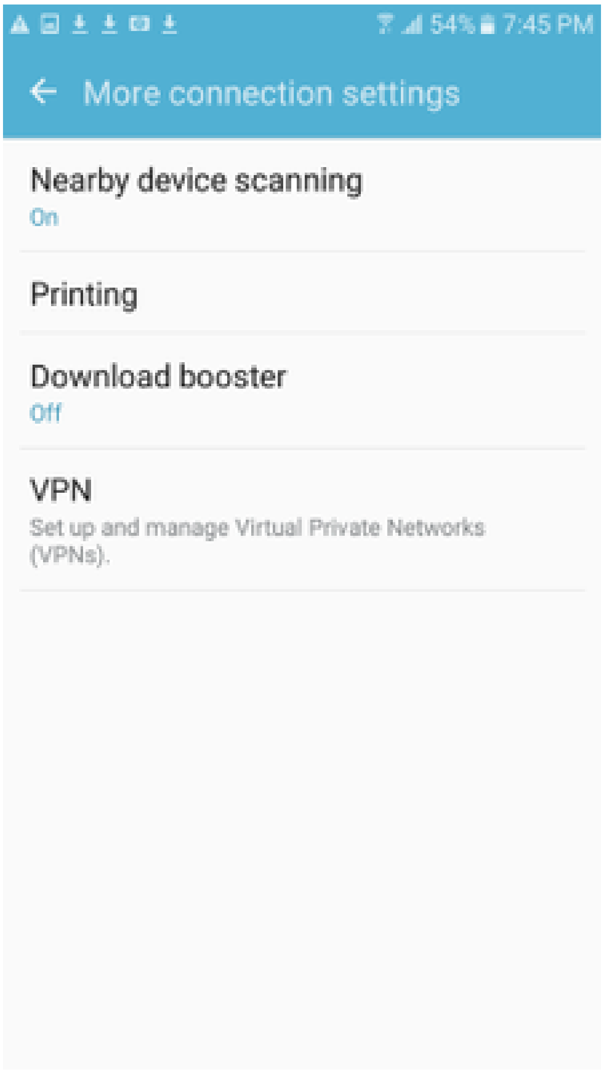
配置Android本地VPN客户端

步骤1.导航至“设**置”>“更多连接设置”**



54% 7:45 PM
Settings
SEARCH
Sounds and vibrations
Display
Themes
Lock screen and security
Battery
User manual
Wi-Fi
Bluetooth
Airplane mode
Mobile hotspot and tethering
Data usage
Mobile networks
More connection settings

步骤2.选择VPN



54% 7:45 PM

More connection settings

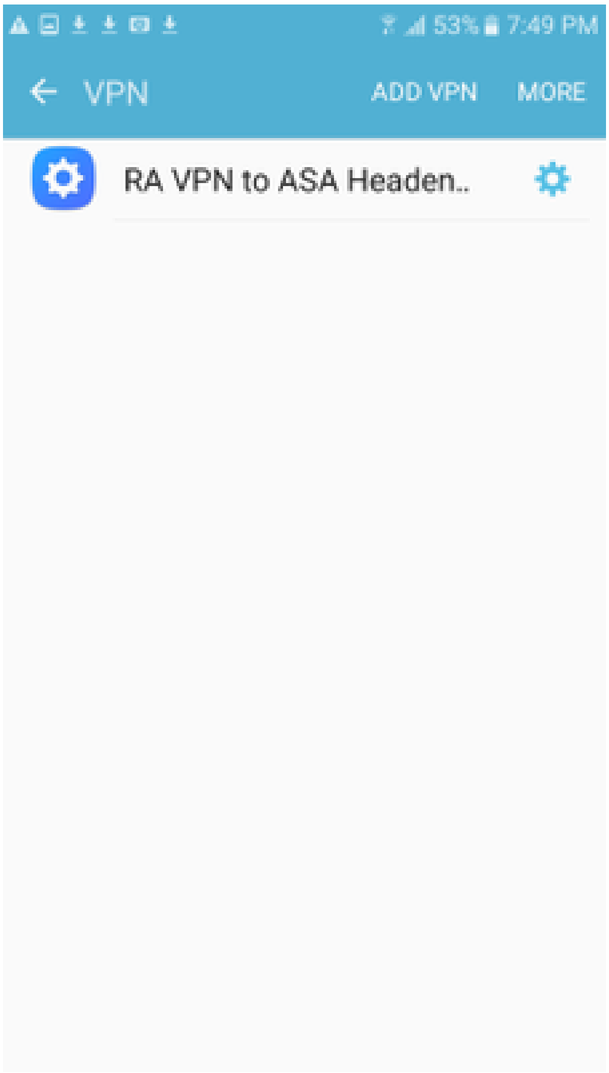
Nearby device scanning
On

Printing

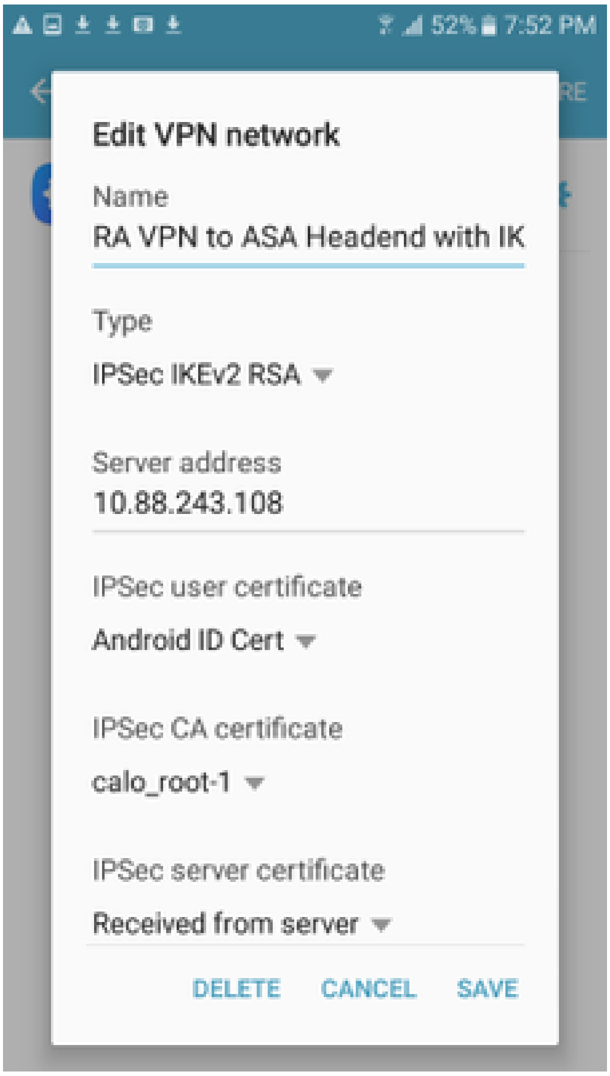
Download booster
Off

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

步骤3.选择**Add VPN**。如果连接已如本示例中所示创建，请轻触引擎图标进行编辑。在“类型”字段中指**定IPSec IKEv2** RSA。服**务器地址**是启用IKEv2的ASA接口IP地址。对于**IPSec用户证书**和**IPSec CA证书**，请通过轻触下拉菜单选择安装的证书。将**IPSec服务器证书**保留为默认选项“从服务器接收”。



RA VPN to ASA Headen..



Edit VPN network

Name
RA VPN to ASA Headend with IK

Type
IPSec IKEv2 RSA

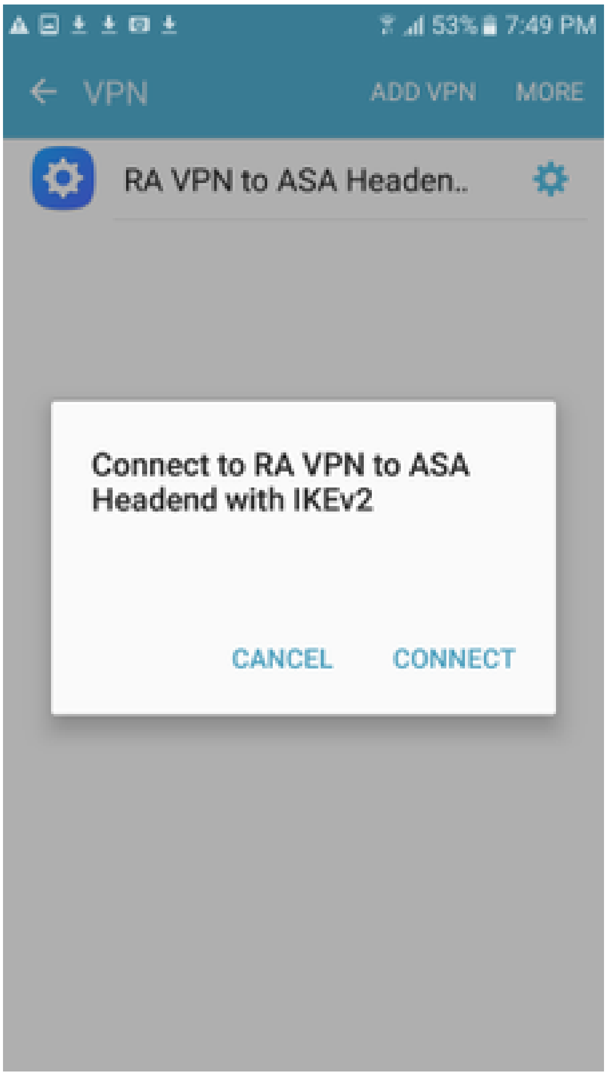
Server address
10.88.243.108

IPSec user certificate
Android ID Cert

IPSec CA certificate
calo_root-1

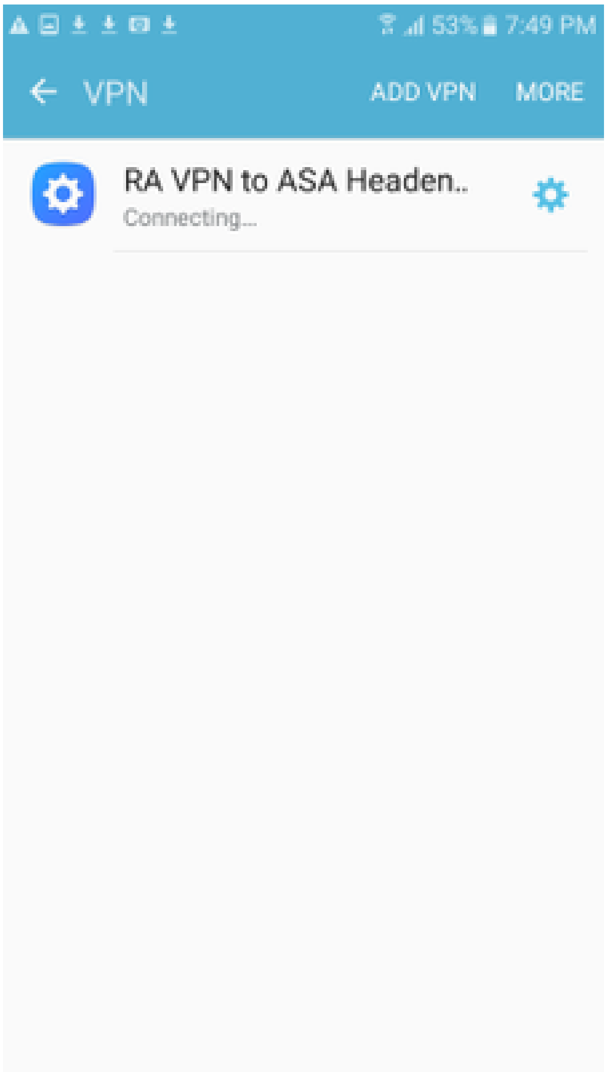
IPSec server certificate
Received from server

步骤4.选择**Save**，然后轻触新VPN连接的名称。

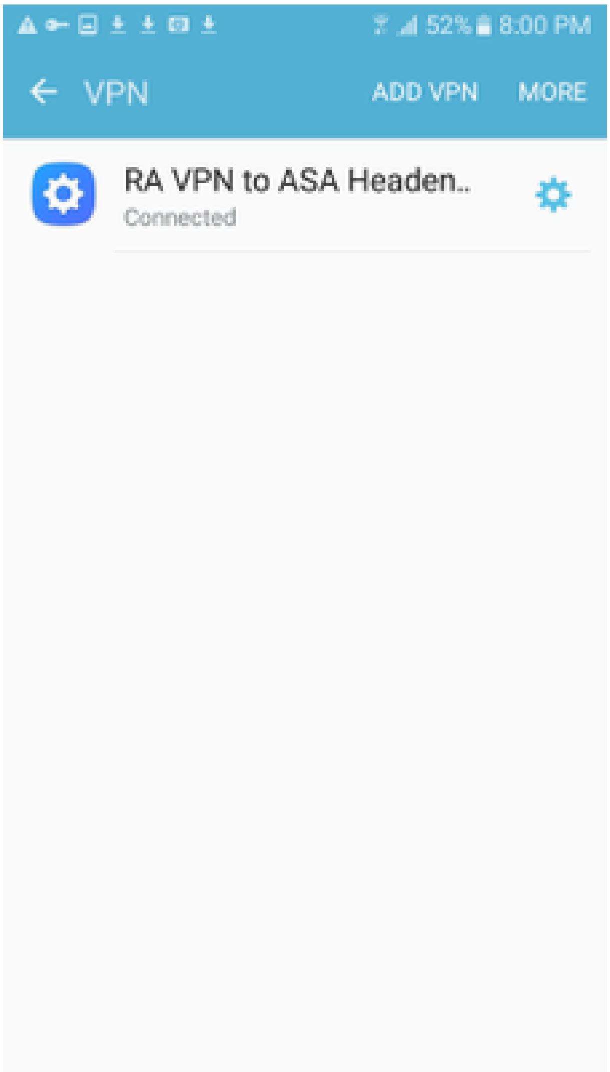


Connect to RA VPN to ASA Headend with IKEv2

步骤5.选择Connect。

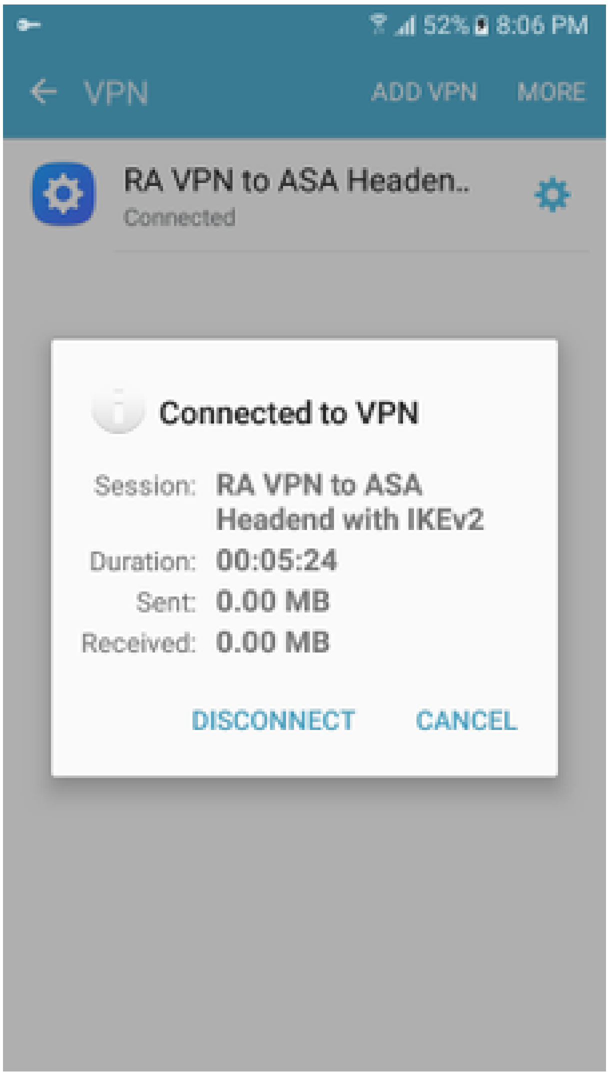


RA VPN to ASA Headen..
Connecting...



RA VPN to ASA Headen..
Connected

步骤6.再键入一次VPN连接以验证状态。它现在显示为“已**连接**”。



Connected to VPN

Session: RA VPN to ASA Headend with IKEv2

Duration: 00:05:24

Sent: 0.00 MB

Received: 0.00 MB

验证

ASA头端上的验证命令：

```
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
```

故障排除

本节提供可用于排除配置故障的信息。

> **注意**：在使用debug命令之前，请参阅有关Debug命令的重要信息。

> **注意**:在ASA上，可以设置各种调试级别；默认情况下，使用1级。如果更改调试级别，调试的详细程度会增加。请谨慎执行此操作，尤其是在生产环境中。

- **调试crypto ikev2协议15**
- **调试crypto ikev2平台15**
- **Debug crypto ca 255**