ASA IKEv2 RA VPN mit Windows 7- oder Android-VPN-Clients und Konfiguration der Zertifikatauthentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Cisco Adaptive Security Appliance (ASA) Version 9.7.1 und höher konfiguriert wird, um es Windows 7- und Android-VPN-Clients (Virtual Private Network) zu ermöglichen, eine (Remote Access) RA VPN-Verbindung unter Verwendung von Internet Key Exchange Protocol (IKEv2) und Zertifikaten als Authentifizierungsmethode herzustellen.

Mitarbeiter: David Rivera und Cesar Lopez Zamarripa, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zertifizierungsstelle (Certificate Authority, CA)
- Public Key Infrastructure (PKI)
- RA VPN mit IKEv2 auf ASA
- Integrierter Windows 7-VPN-Client
- Android-nativer VPN-Client

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- CISCO1921/K9 - 15.5(3)M4a als IOS CA-Server
- ASA5506X - 9.7(1) als VPN-Headend
- Windows 7 als Client-Computer
- Galaxy J5 - Android 6.0.1 als mobiler Client

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Übersicht

Dies sind die Schritte zur Konfiguration der nativen VPN-Clients von Windows 7 und Android für die Verbindung mit einem ASA-Headend:

Zertifizierungsstelle konfigurieren

Die CA ermöglicht das Einbetten der erforderlichen Extended Key Usage (EKU) in das Zertifikat. Für das ASA-Headend ist das Zertifikat Server Auth EKU erforderlich, während das Client-Zertifikat Client Auth EKU erfordert.

Es können verschiedene CA-Server verwendet werden, z. B.:

- Cisco IOS CA-Server
- OpenSSL CA-Server
- Microsoft CA-Server
- $1^{Standard}$ Parteien-CAs

Für dieses Konfigurationsbeispiel wird der IOS CA Server verwendet.

In diesem Abschnitt wird die Basiskonfiguration beschrieben, mit der ein CISCO1921/K9 mit Version 15.5(3)M4a als CA-Server verwendet werden kann.

Schritt 1: Stellen Sie sicher, dass das Gerät und die Version den Befehl eku unterstützen.

```
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
```

Schritt 2: Aktivieren Sie den HTTP-Server auf dem Router.

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

Schritt 3: Generieren einer exportfähigen RSA-Tastatur

```
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)
```

Schritt 4: Konfigurieren eines Vertrauenspunkts

```
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>
```

> **Hinweis**: Die IP-Adresse für den Anmeldebefehl ist eine der vom Router konfigurierten IP-Adressen für eine erreichbare Schnittstelle.

Schritt 5: Authentifizieren Sie den Trustpoint (Zertifikat der Zertifizierungsstelle abrufen).

```
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.
```

Schritt 6: Registrieren Sie den Trustpoint (Identitätszertifikat abrufen).

```
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
```

Schritt 7: Überprüfen Sie die Zertifikate.

```
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
```

Schritt 8: Exportieren Sie den HeadEnd-Trustpoint in ein Terminal im PKCS12-Format, um das Identitätszertifikat abzurufen. Das CA-Zertifikat und der private Schlüssel werden in einer Datei hinzugefügt.

```
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.
```

Schritt 9: Erstellen Sie einen leeren Trustpoint auf der ASA.

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

Schritt 10: Importieren Sie die PKCS12-Datei.

```
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
```

Schritt 11: Überprüfen der Zertifikatsinformationen

```
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
```

Erstellen eines Clientzertifikats

Schritt 1: Generieren einer exportfähigen RSA-Tastatur

```
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
```

Schritt 2: Konfigurieren eines Vertrauenspunkts

```
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>
```

Schritt 3: Authentifizieren Sie den konfigurierten Trustpoint (Zertifikat der Zertifizierungsstelle abrufen).

```
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.
```

Schritt 4: Registrieren Sie den authentifizierten Trustpoint (Identitätszertifikat abrufen).

```
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
```

Schritt 5: Überprüfen Sie die Zertifikatsinformationen.

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

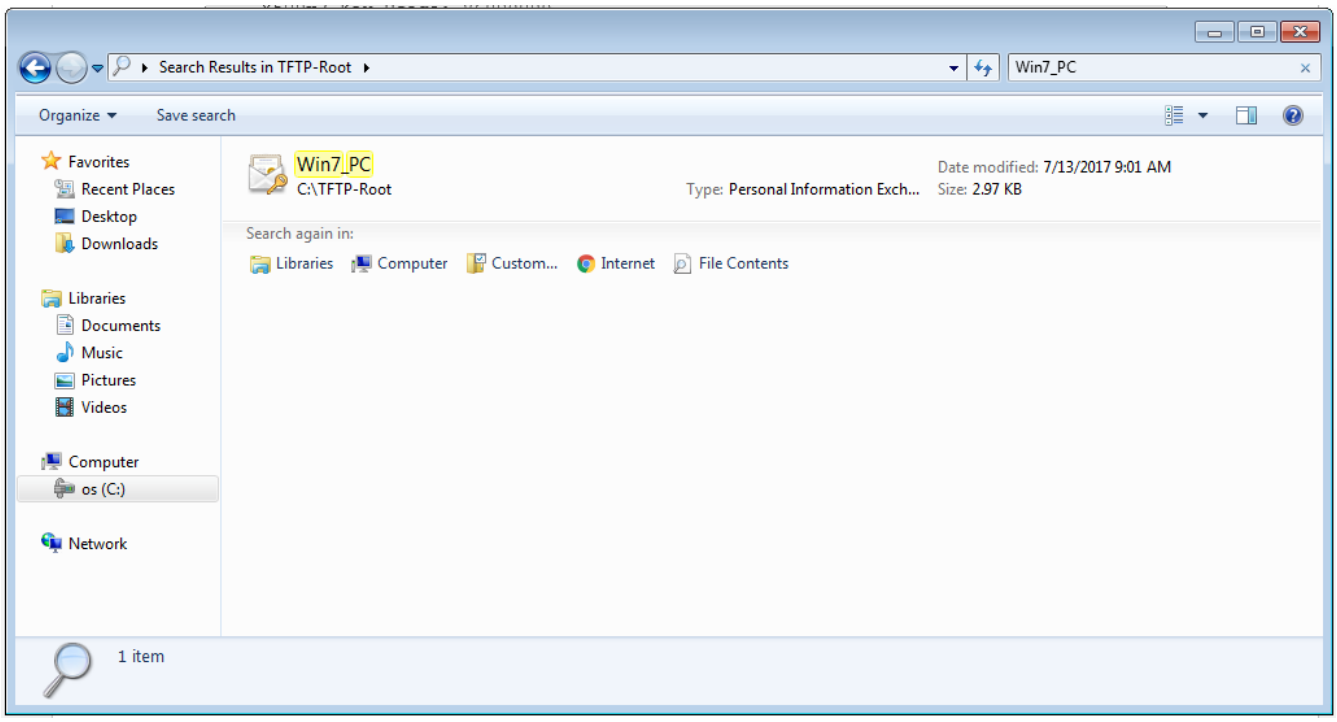
```
    cn=calo_root
  Subject:
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
    cn=Win7_PC.david.com
  Validity Date:
    start date: 13:29:51 UTC Jul 13 2017
    end   date: 13:29:51 UTC Jul 13 2018
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048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

Installieren des Identitätszertifikats auf dem Windows 7-Client-Computer

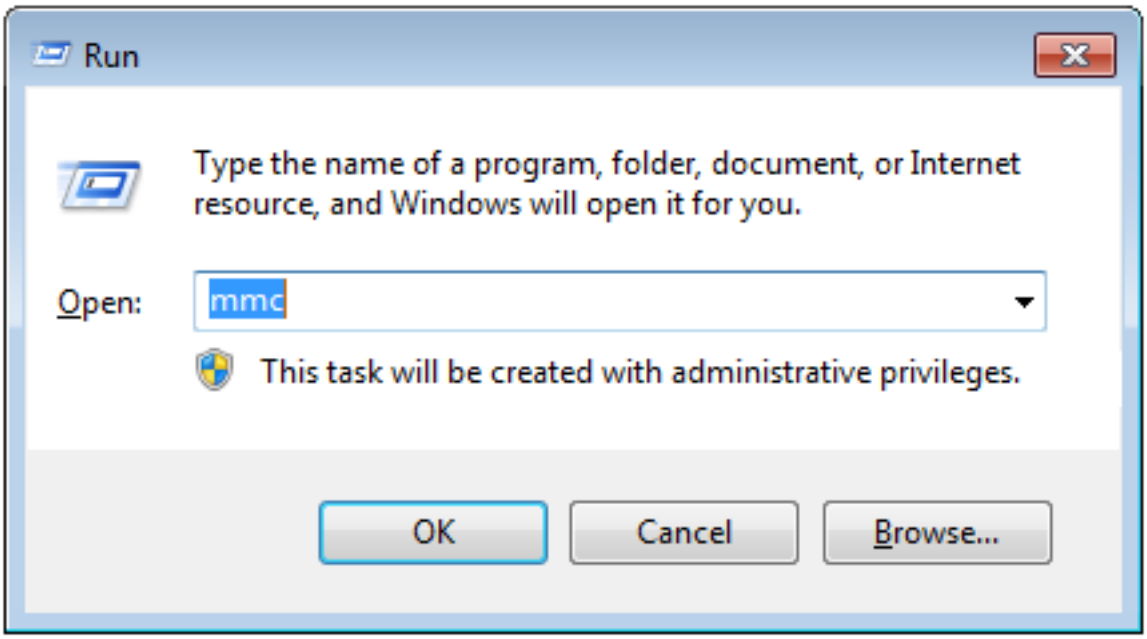
Schritt 1: Exportieren Sie den benannten Win7_PC-Trustpoint in einen FTP/TFTP-Server (installiert auf Ihrem Windows 7-Computer) im PKCS12-Format (.p12), um das Identitätszertifikat, das CA-Zertifikat und den privaten Schlüssel in einer einzigen Datei abzurufen.

```
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.
```

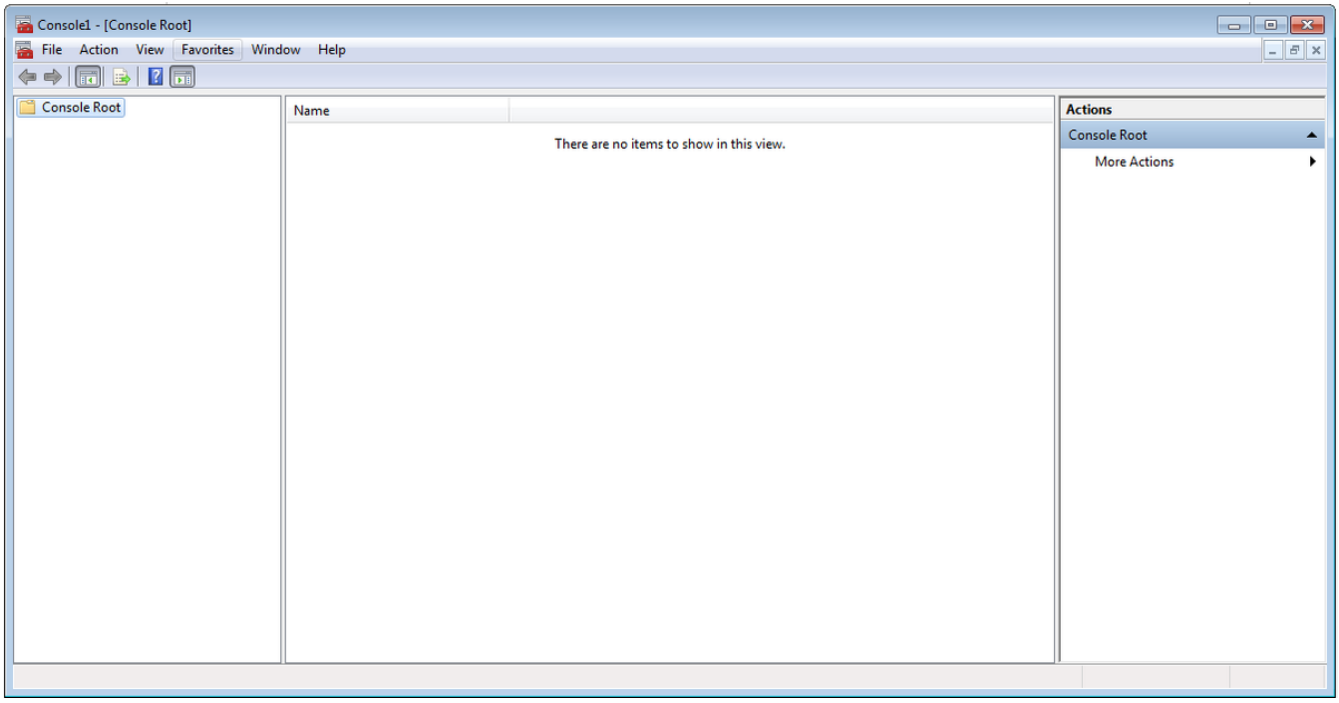
So sucht die exportierte Datei auf einem Clientcomputer.



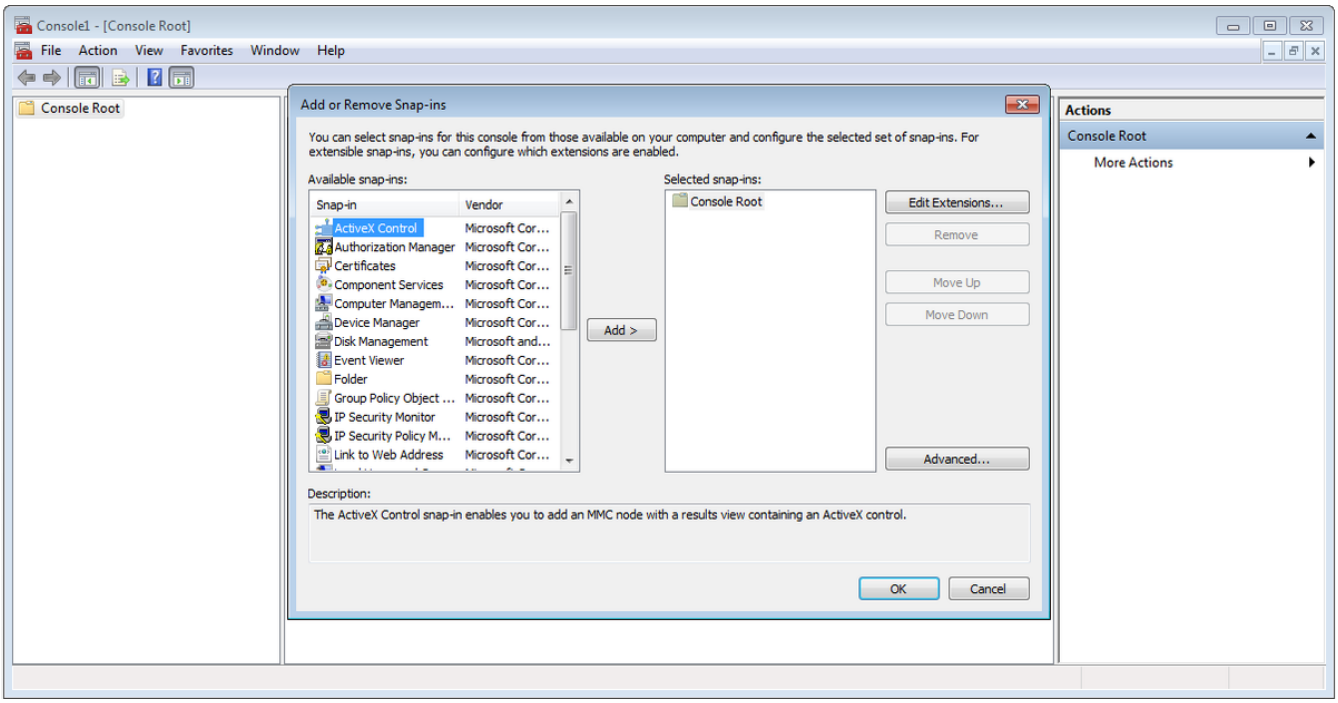
Schritt 2: Drücken Sie **Strg + R**, und geben Sie **mmc** ein, um die Microsoft Management Console (MMC) zu öffnen.



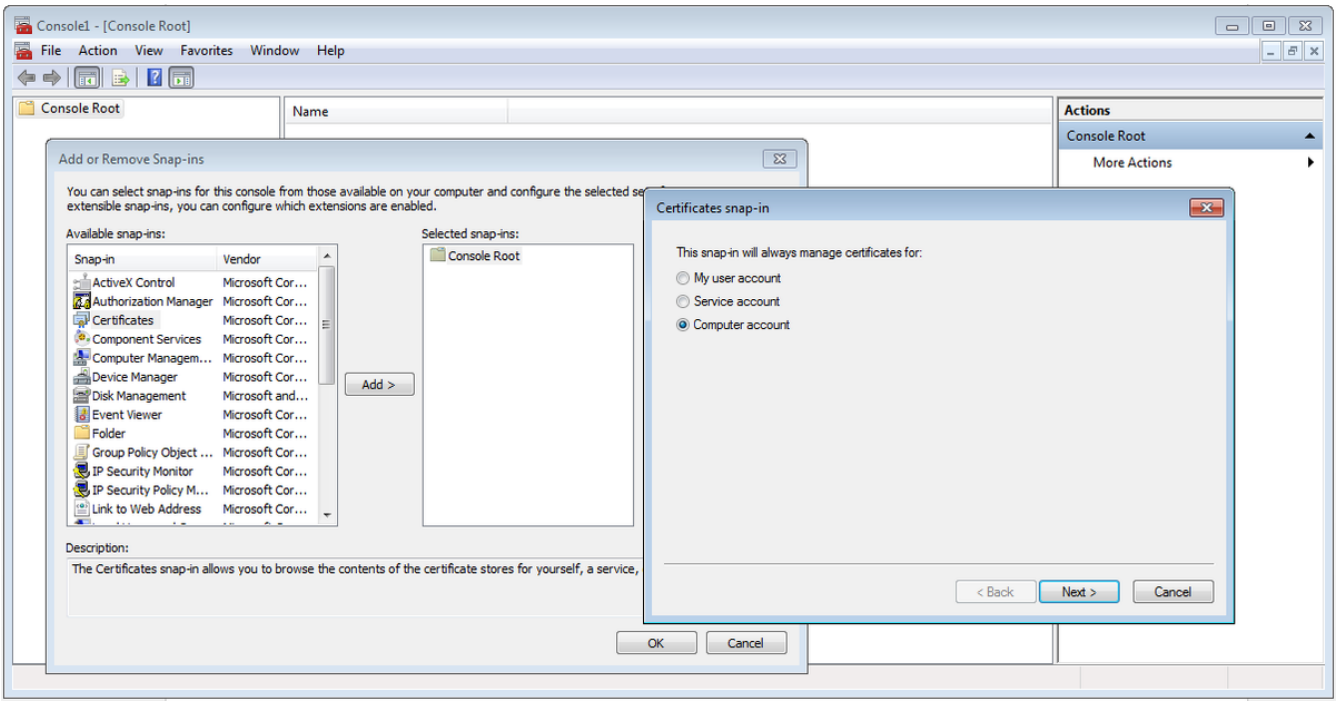
Schritt 3: Wählen Sie **OK aus**.



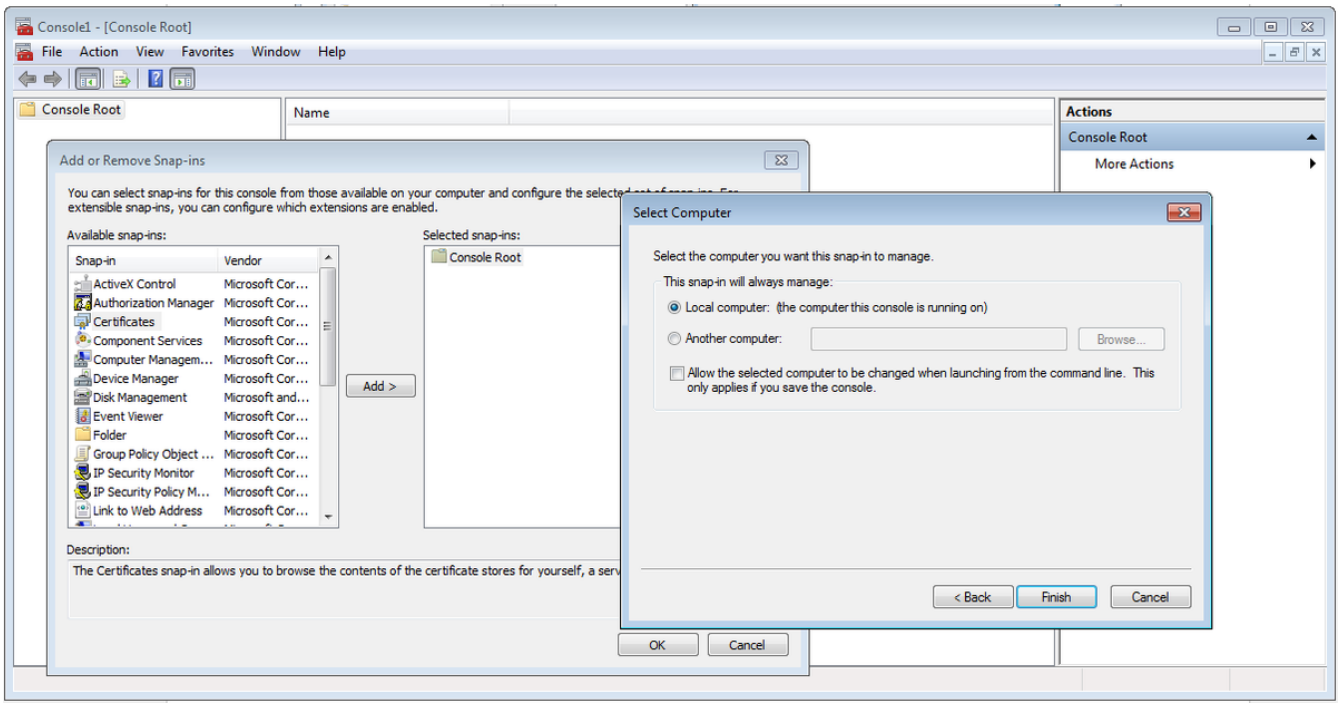
Schritt 4: Navigieren Sie zu **Datei > Snap-In hinzufügen/entfernen**.



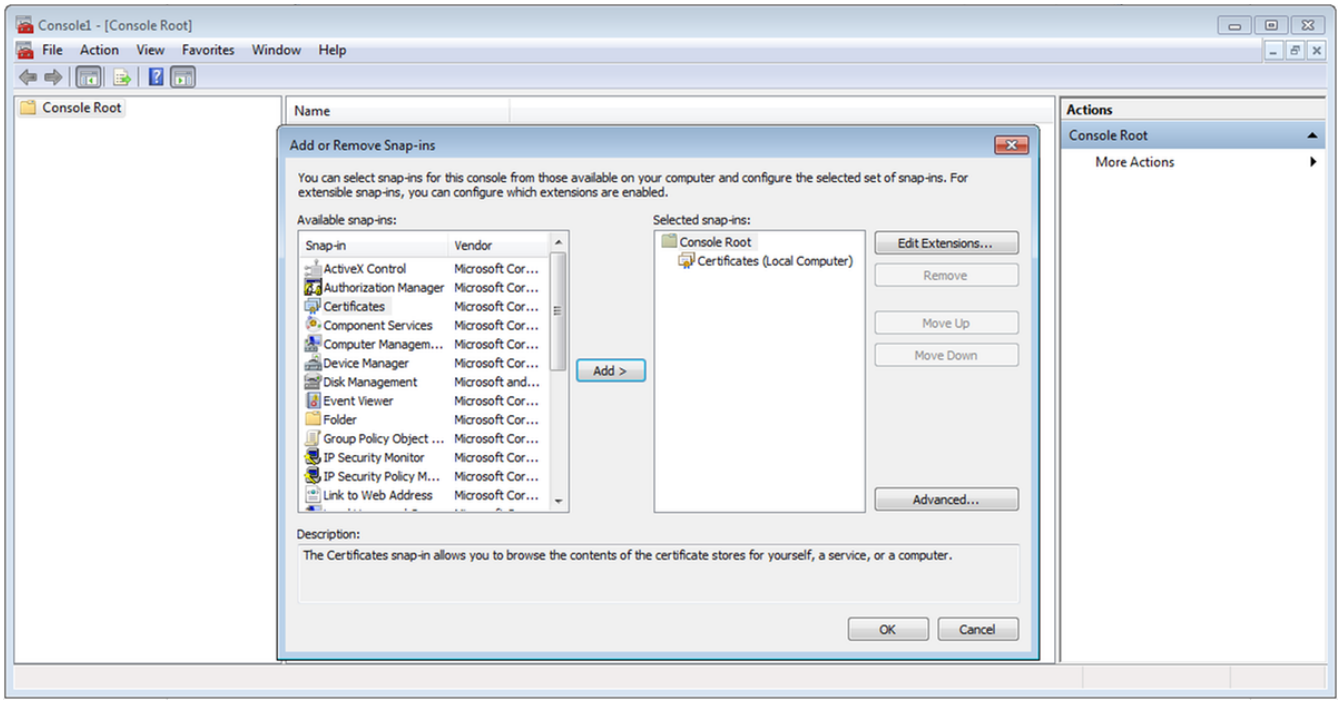
Schritt 5: Wählen Sie **Zertifikate > Hinzufügen > Computerkonto aus**.



Schritt 6: Wählen Sie **Weiter**,

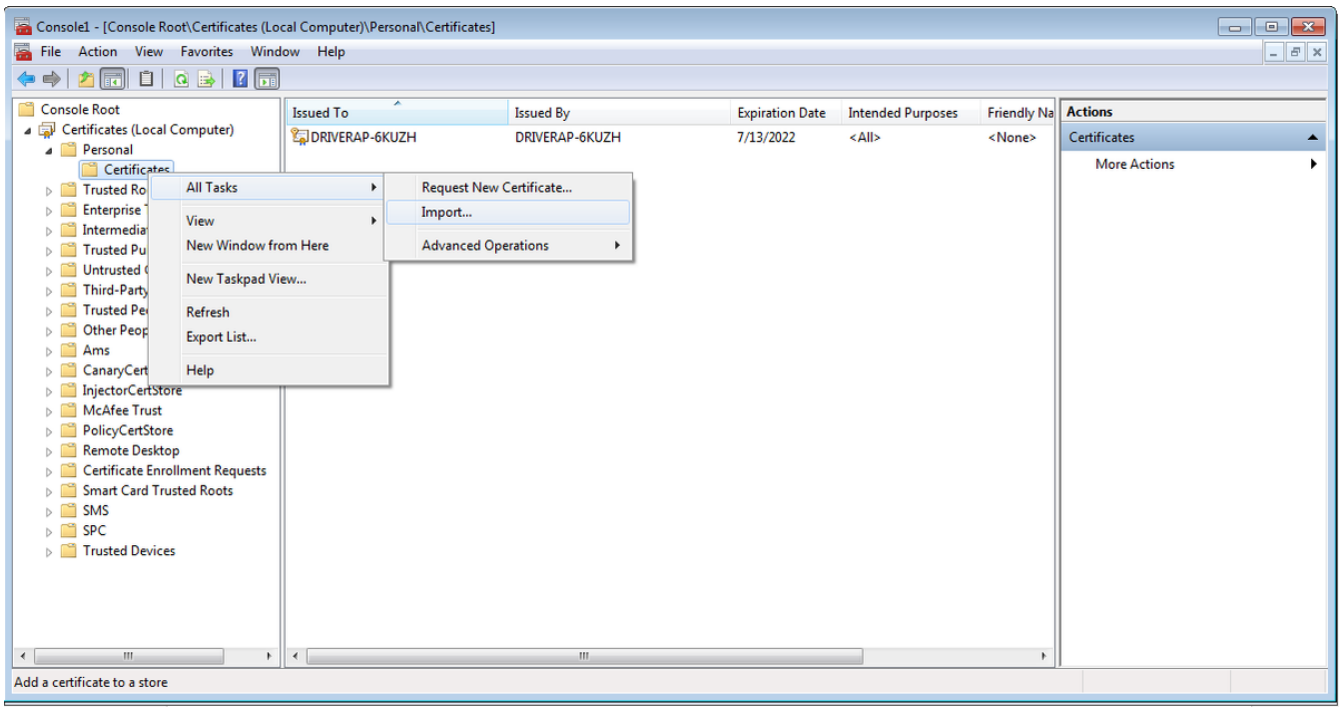


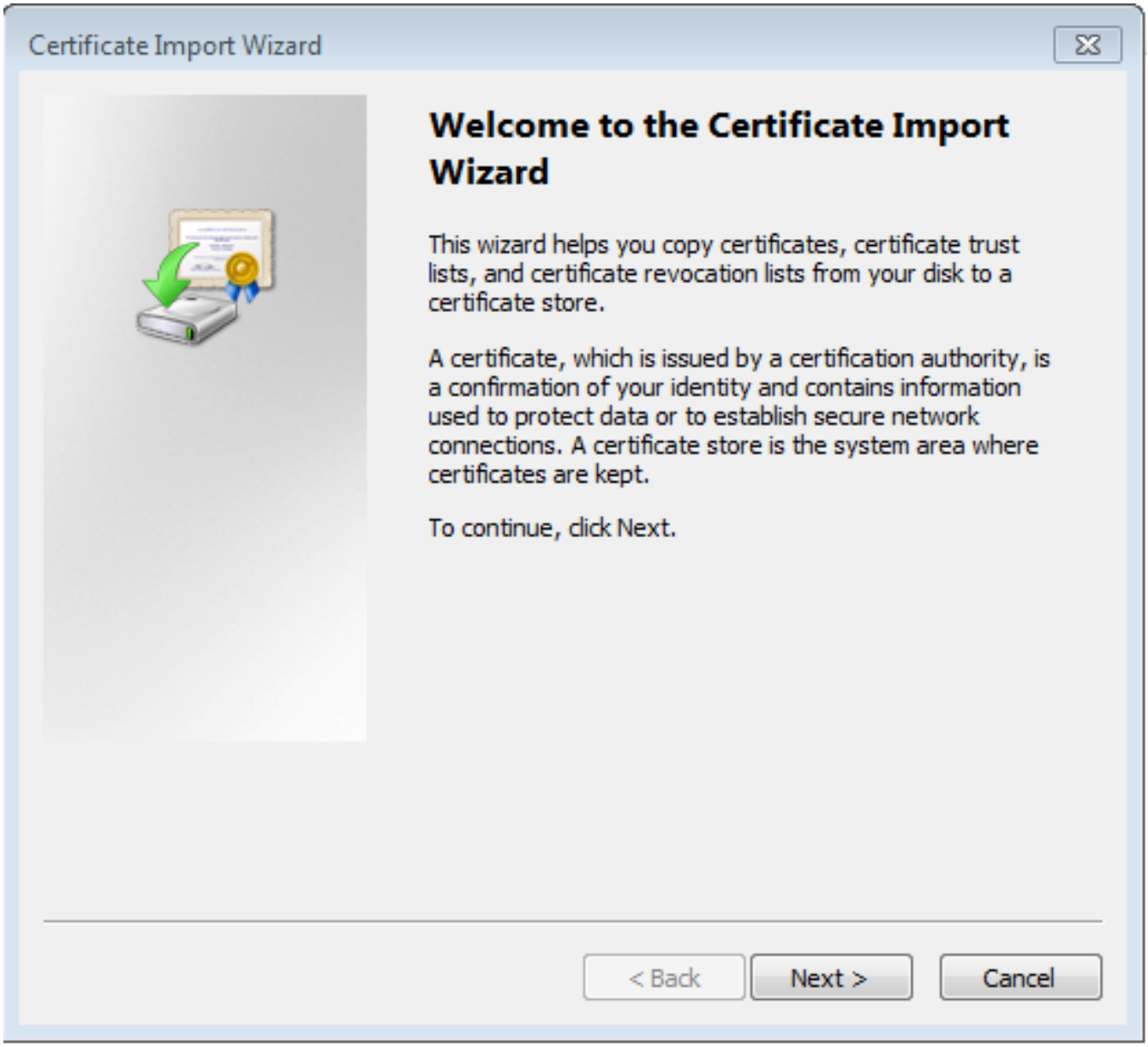
Schritt 7: **Beenden Sie**.



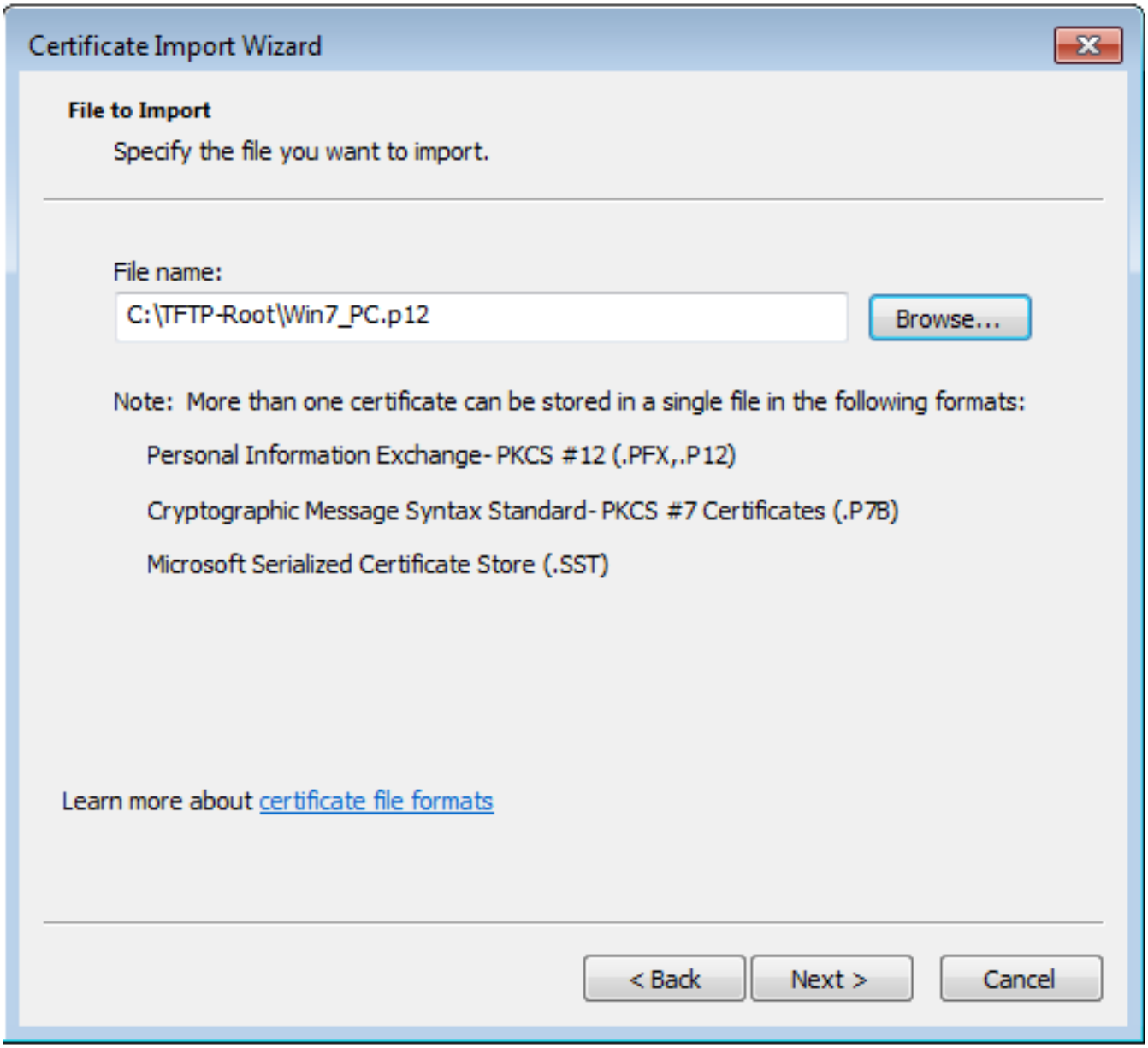
Schritt 8: Wählen Sie **OK aus**.

Schritt 9: Gehen Sie zu **Certificates (Local Computer)>Personal>Certificates**, klicken Sie mit der rechten Maustaste auf den Ordner, und navigieren Sie zu **All Tasks>Import**:

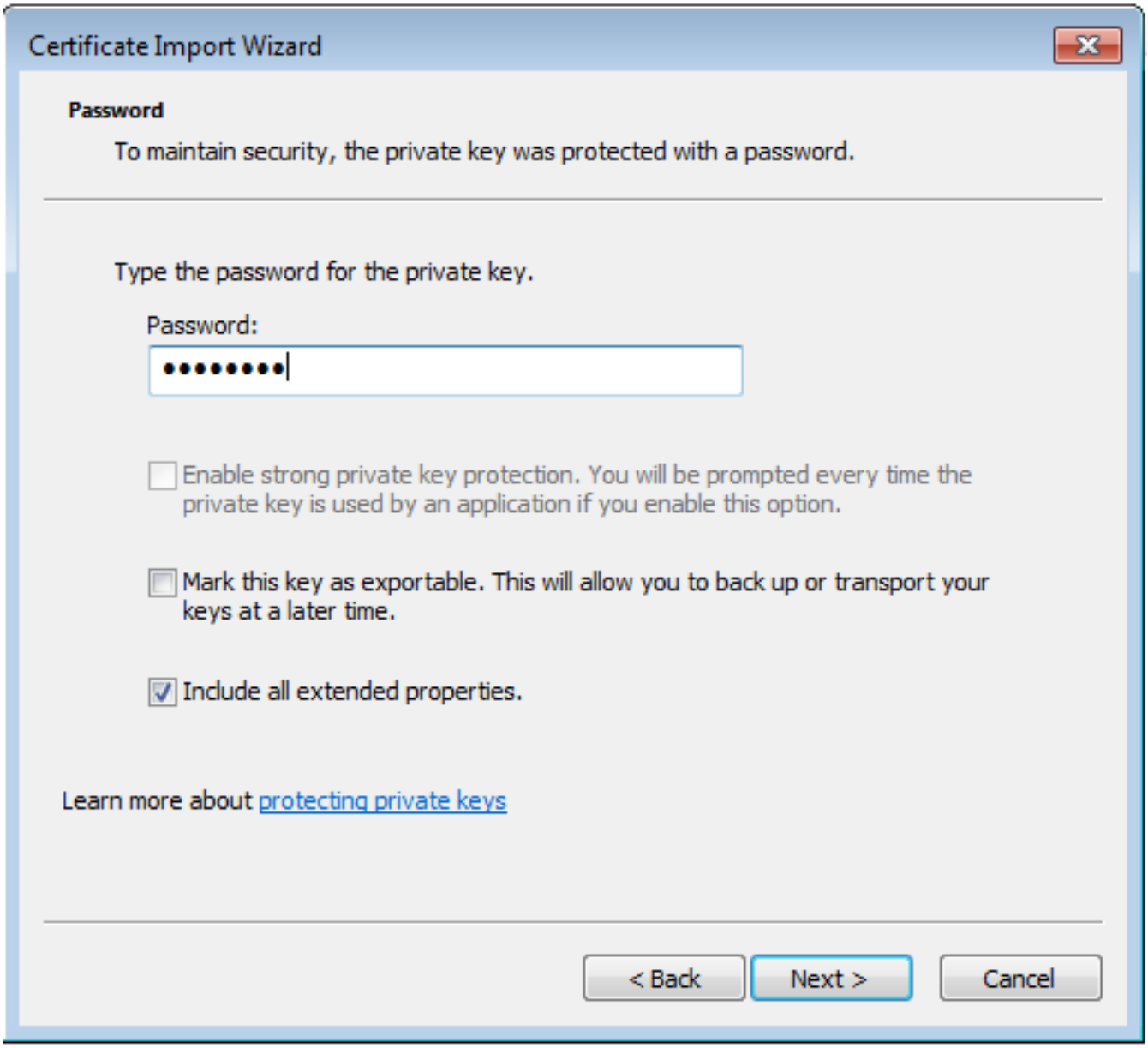




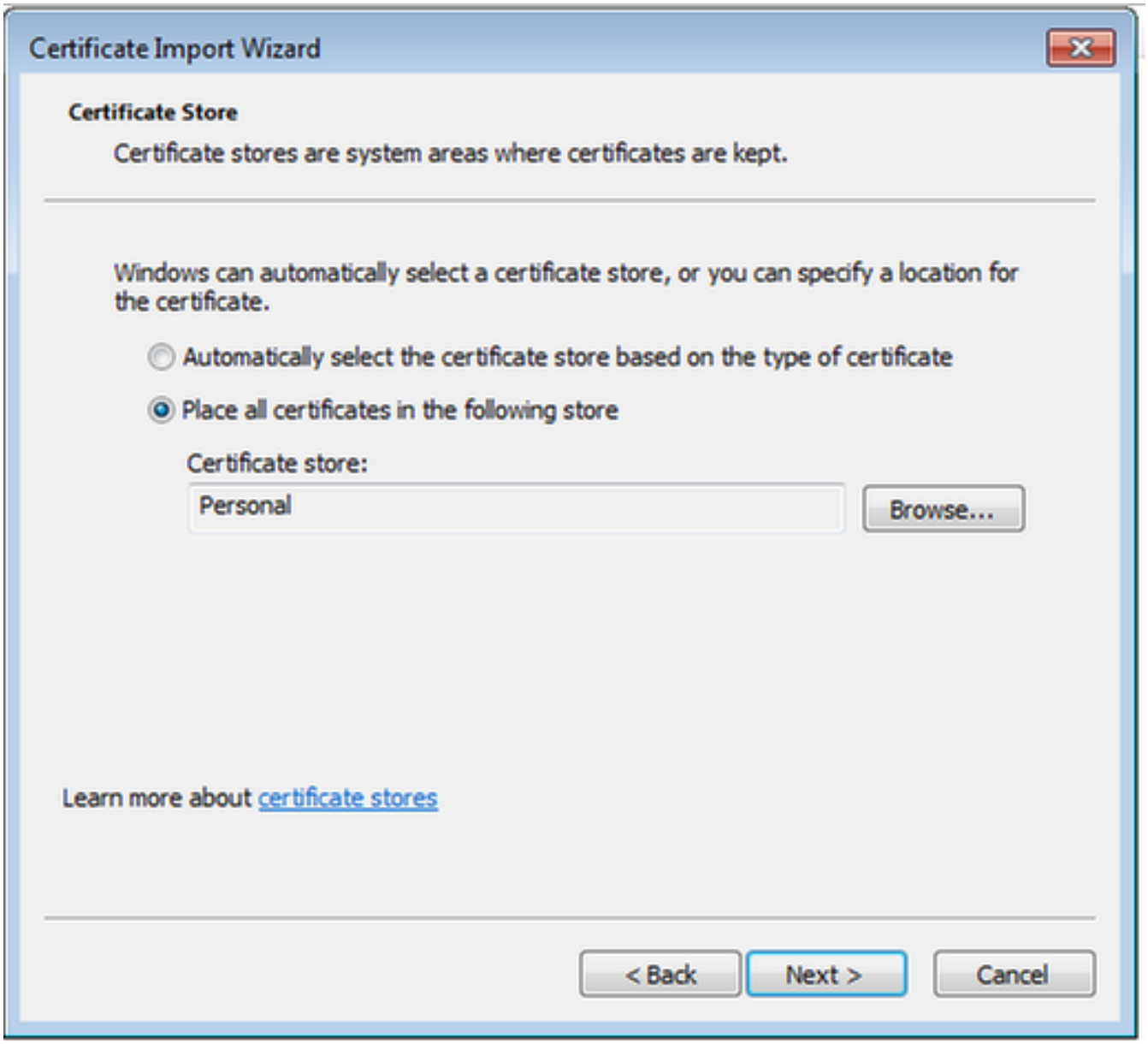
Schritt 10: Klicken Sie auf **Weiter**. Geben Sie den Pfad an, in dem die PKCS12-Datei gespeichert ist.



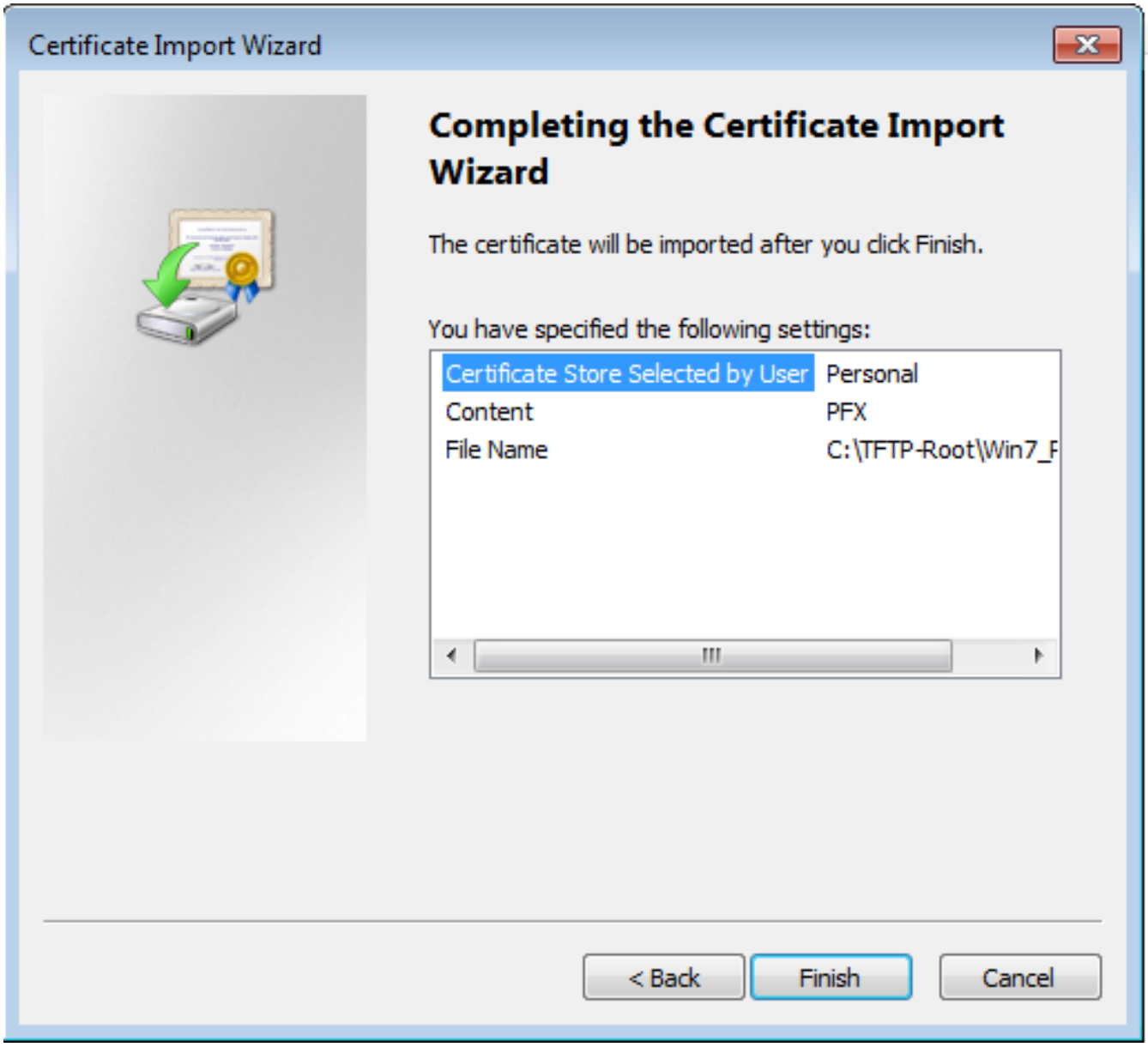
Schritt 11: Wählen Sie **Weiter** erneut aus, und geben Sie das Kennwort ein, das im *crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>* Befehl *eingegeben wurde*.



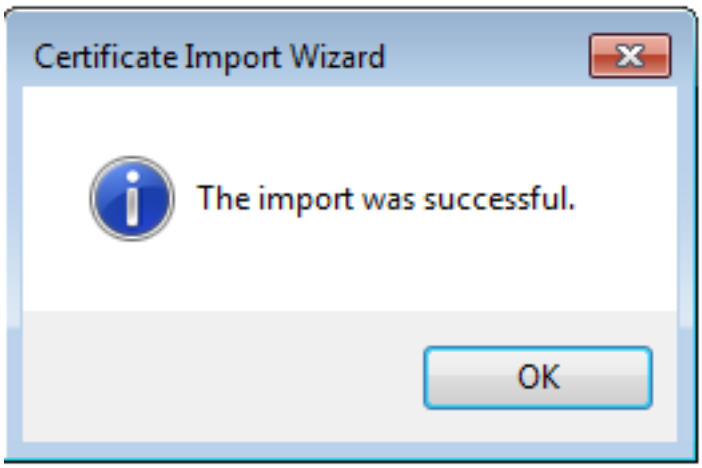
Schritt 12: Wählen Sie **Weiter aus**.



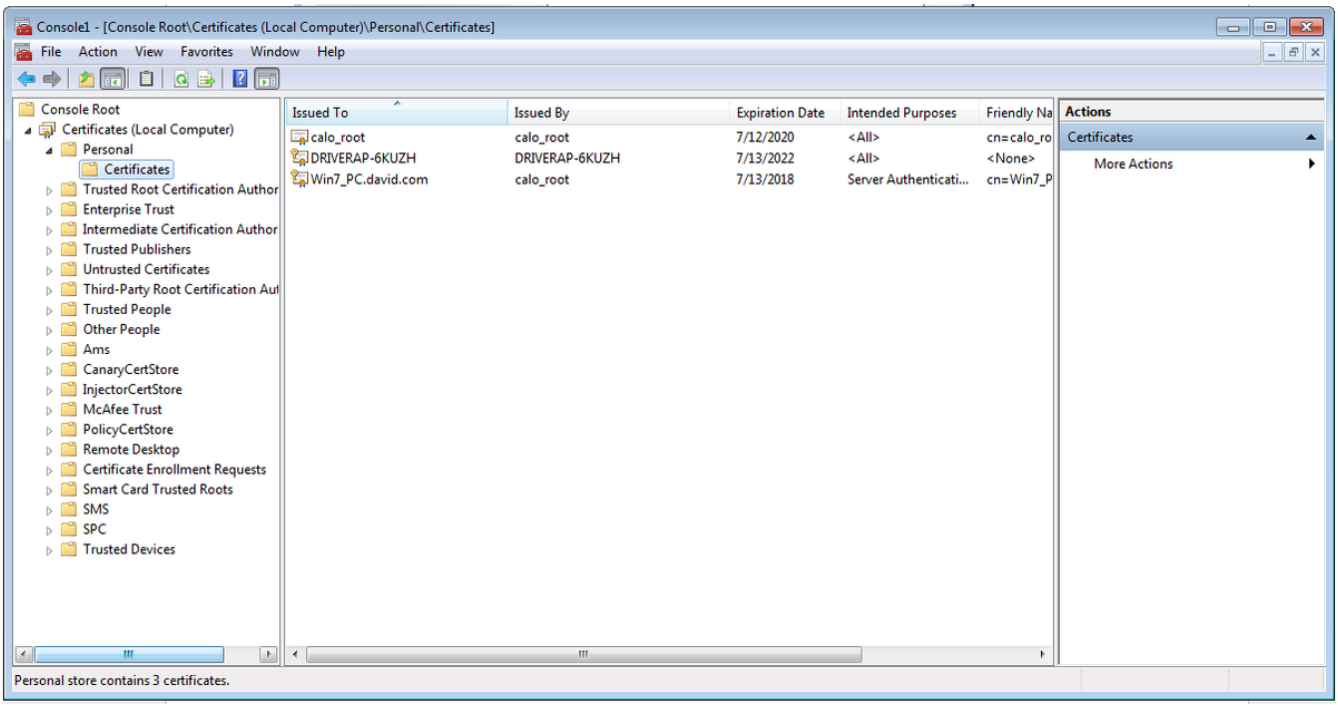
Schritt 13: Wählen Sie noch einmal **Weiter** aus.



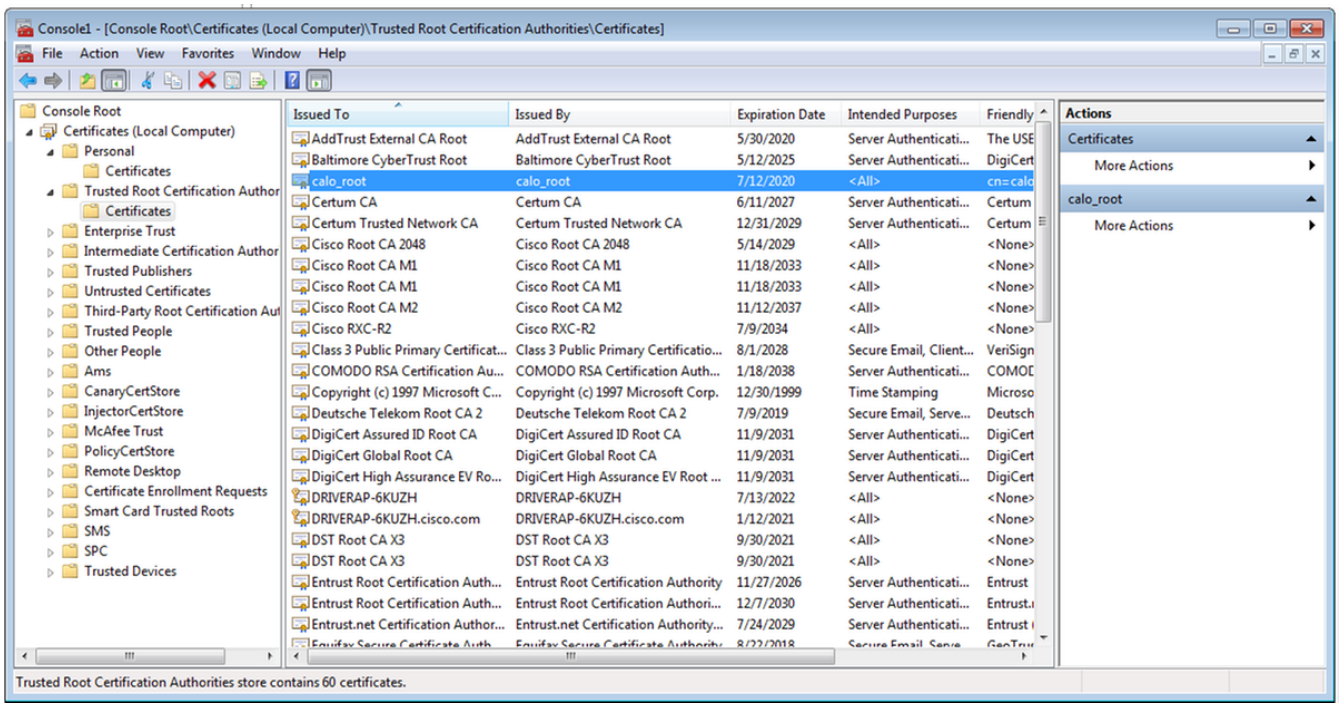
Schritt 14: Wählen Sie **Fertig stellen aus**.

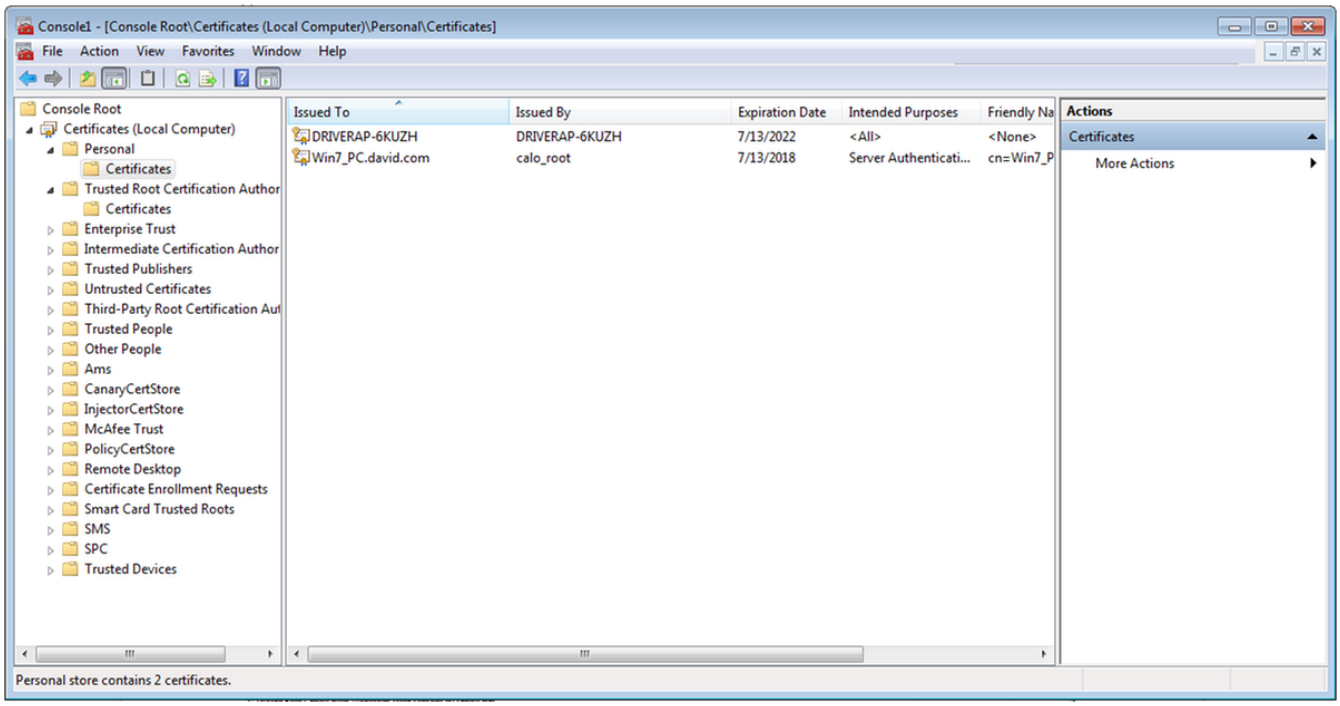


Schritt 15: Wählen Sie **OK aus**. Nun werden die installierten Zertifikate angezeigt (sowohl das Zertifizierungsstellenzertifikat als auch das Identitätszertifikat).



Schritt 16: Ziehen Sie das CA-Zertifikat aus **Zertifikaten (Lokaler Computer)>Personal>Zertifikate** auf **Zertifikate (Lokaler Computer)>Vertrauenswürdige Stammzertifizierungsstelle>Zertifikate.**



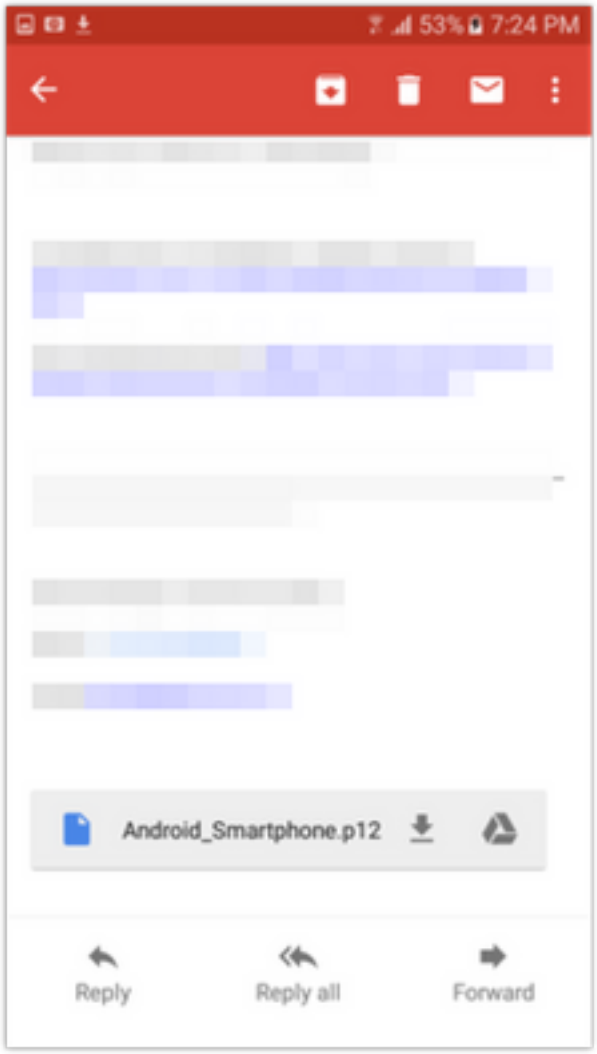


So installieren Sie das Identitätszertifikat auf Ihrem Android-Mobilgerät

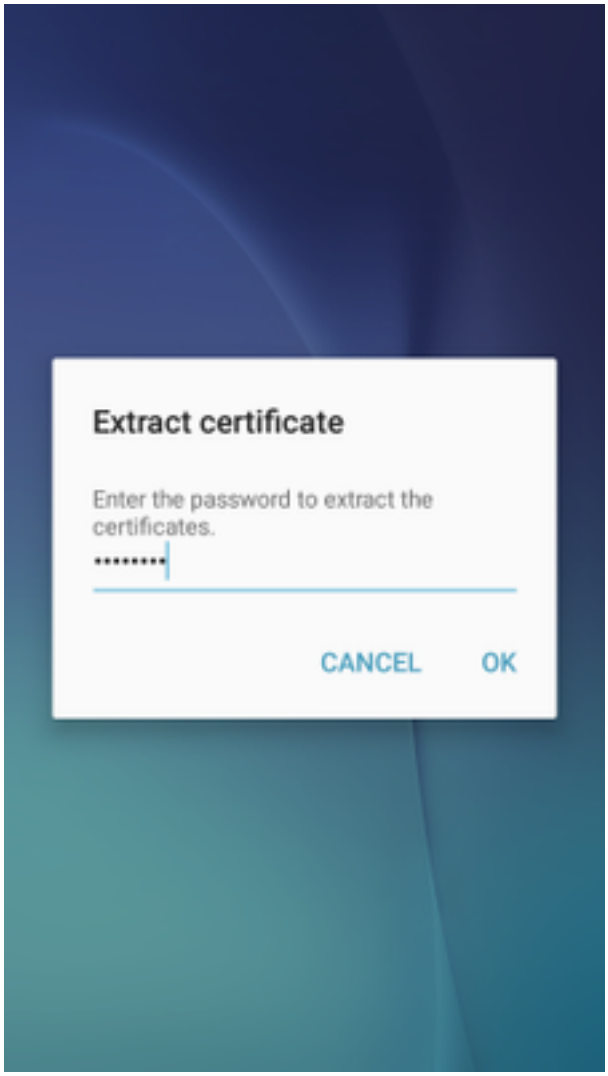
Hinweis: Android unterstützt PKCS#12-Schlüsselspeicherdateien mit der Erweiterung .pfx oder .p12.

Hinweis: Android unterstützt nur DER-codierte X.509 SSL-Zertifikate.

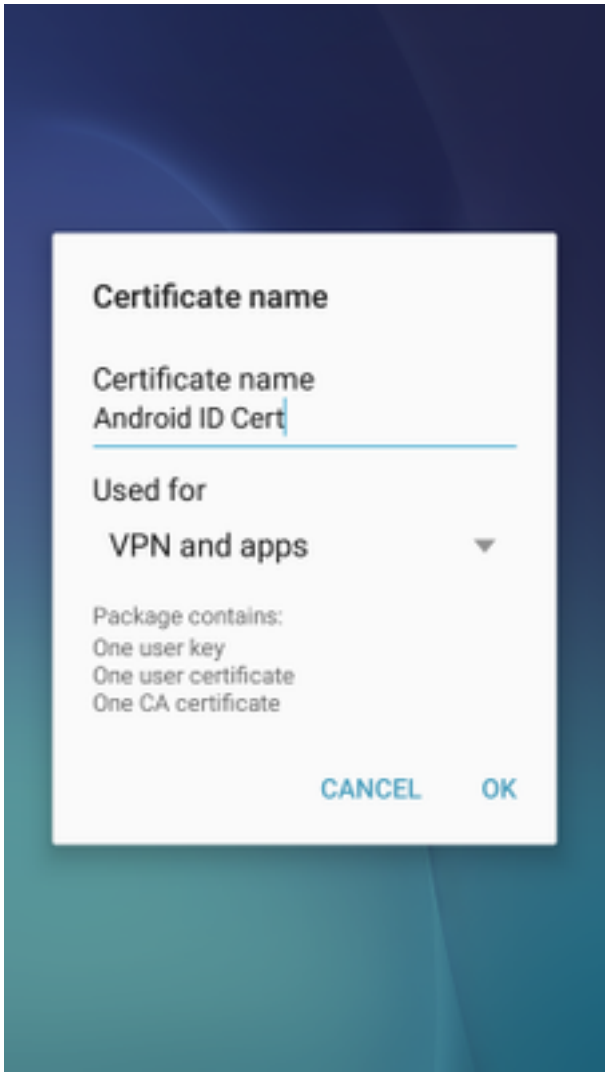
Schritt 1: Senden Sie die Datei nach dem Export des Client-Zertifikats vom IOS CA-Server im PKCS12-Format (p12) per E-Mail an das Android-Gerät. Wenn Sie die Datei dort haben, tippen Sie auf den Namen der Datei, um die automatische Installation zu starten. (**Laden Sie die Datei nicht herunter**)



Schritt 2: Geben Sie das Kennwort ein, das für den Export des Zertifikats verwendet wird. In diesem Beispiel lautet das Kennwort **cisco123**.

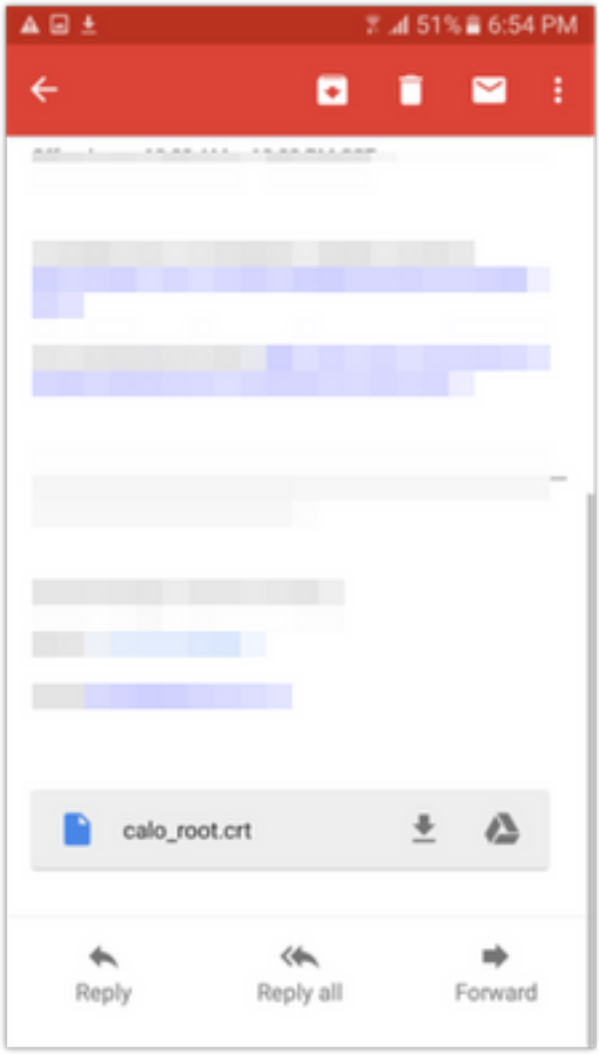


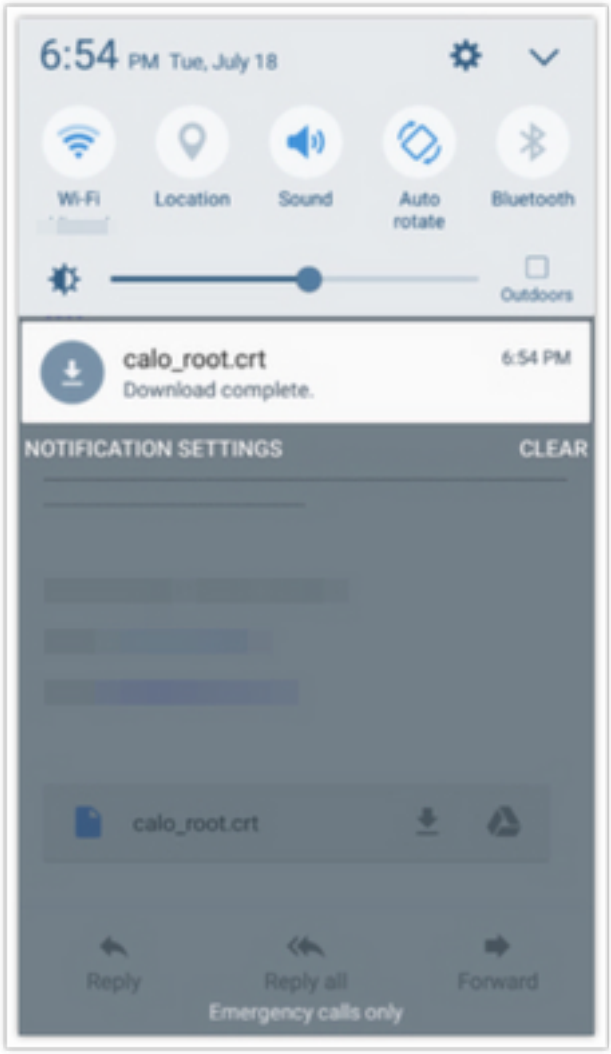
Schritt 3: Wählen Sie **OK** aus, und geben Sie einen **Zertifikatsnamen ein**. Es kann ein beliebiges Wort sein, in diesem Beispiel ist der Name **Android ID Cert** .



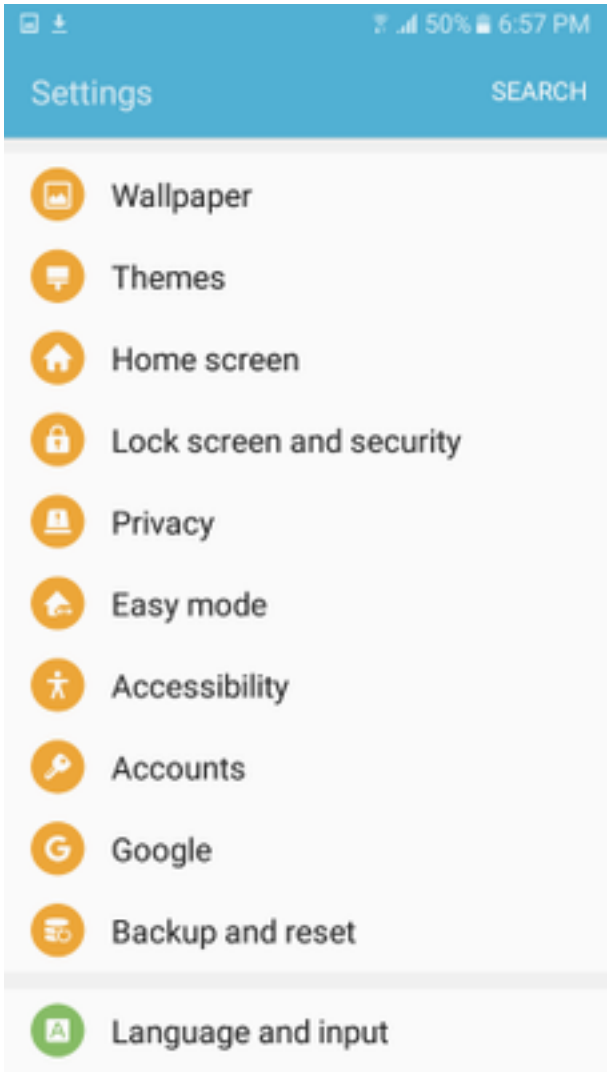
Schritt 4: Wählen Sie **OK**, und die Meldung "Android ID Cert installed" wird angezeigt.

Schritt 5: Um das Zertifizierungsstellenzertifikat zu installieren, extrahieren Sie es aus dem IOS CA-Server im Base64-Format und speichern es mit der Erweiterung .crt. Senden Sie die Datei per E-Mail an Ihr Android-Gerät. Dieses Mal müssen Sie die Datei herunterladen, indem Sie auf den Pfeil neben dem Namen der Datei.


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

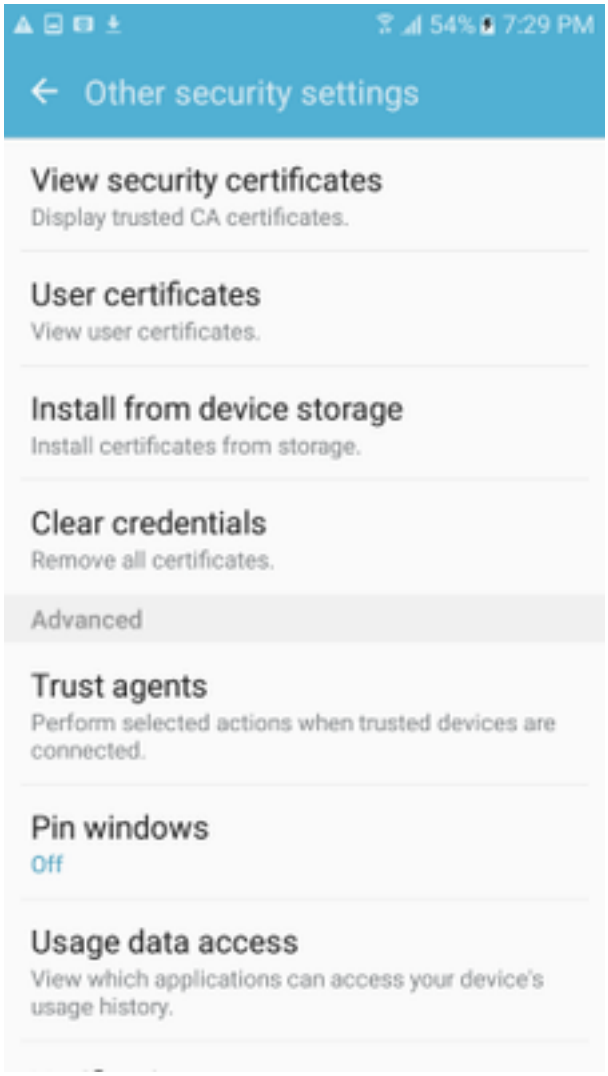


Schritt 6: Navigieren Sie zu **Einstellungen** und **Sperrbildschirm und Sicherheit.**

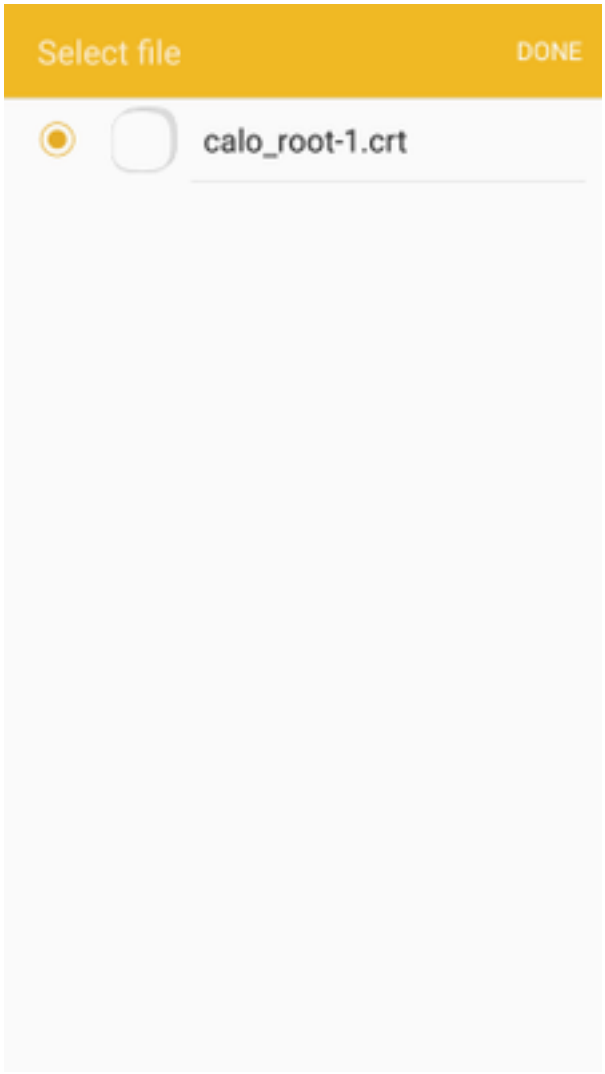


Schritt 7: Wählen Sie **Andere Sicherheitseinstellungen aus.**

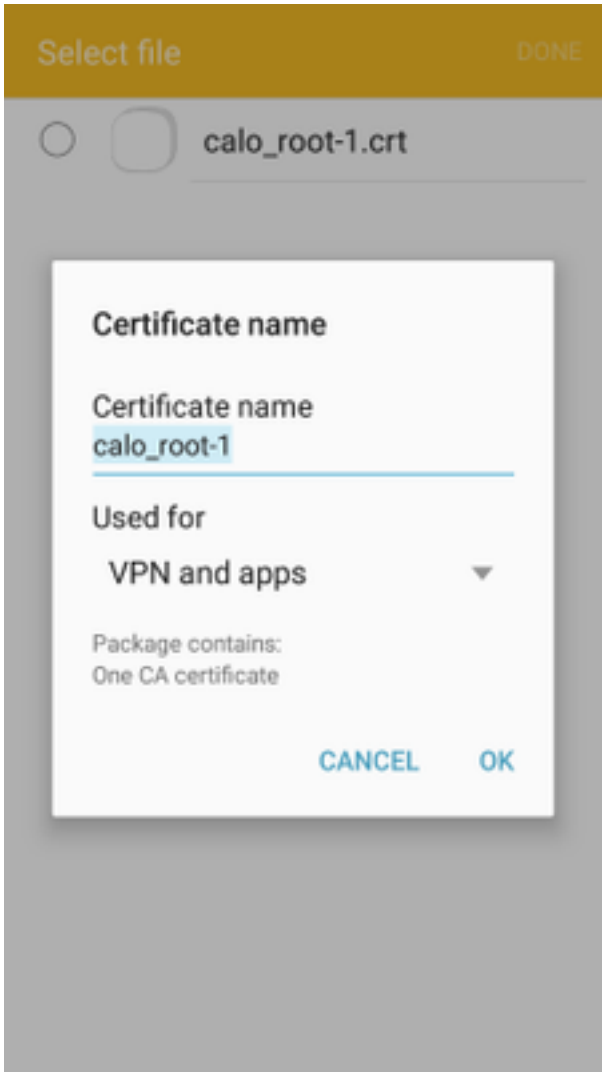
Schritt 8: Navigieren Sie zu **Installation vom Gerätespeicher.**



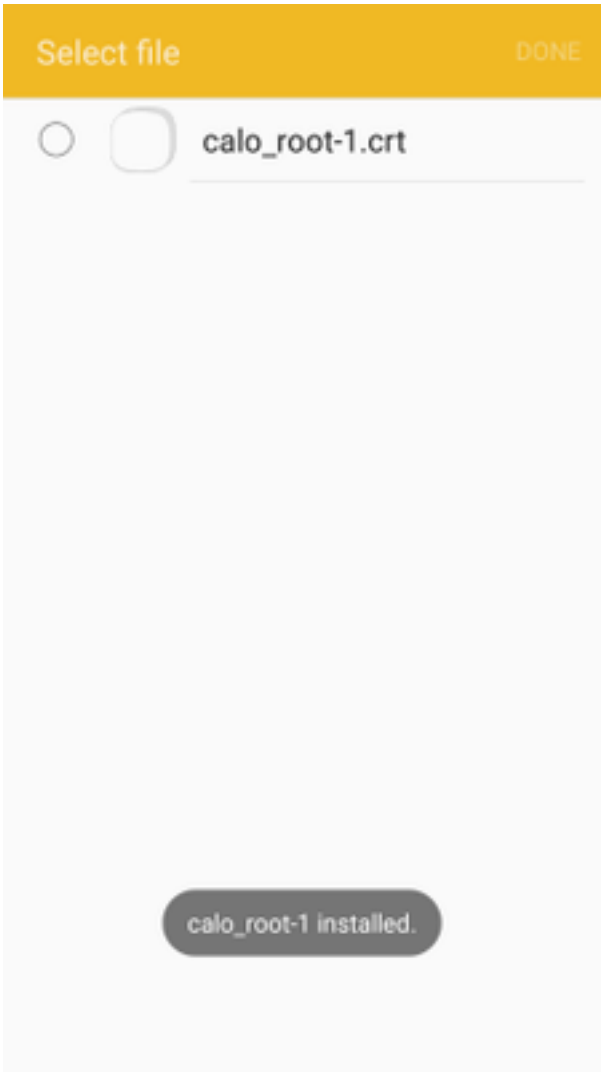
Schritt 9: Wählen Sie die Crt-Datei aus, und tippen Sie auf **Fertig.**



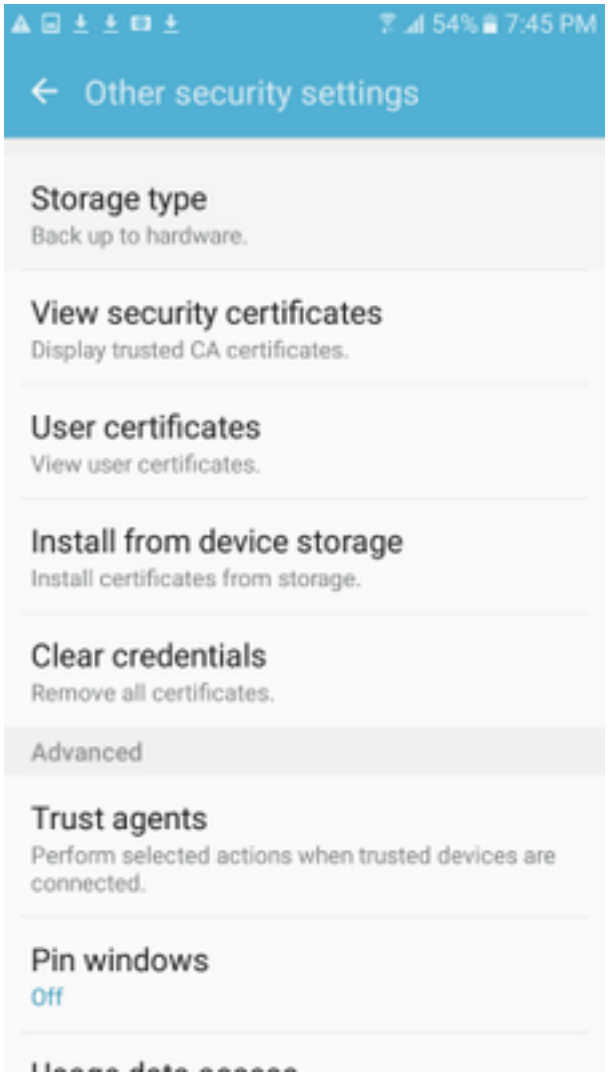
Schritt 10: Geben Sie einen **Zertifikatsnamen ein**. Es kann ein beliebiges Wort sein, in diesem Beispiel lautet der Name **calo_root-1**.



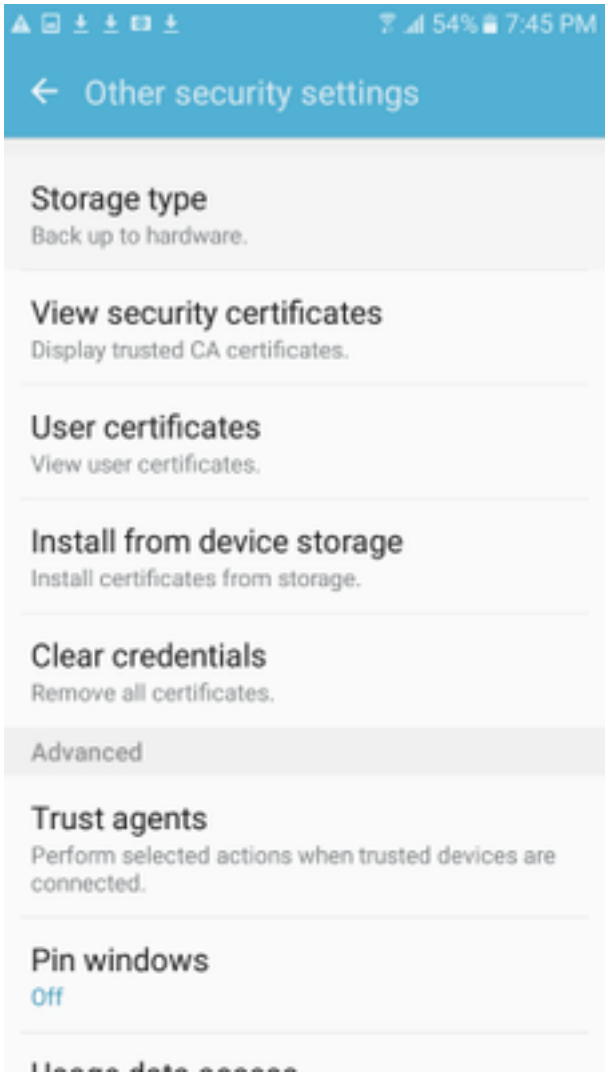
Schritt 10: Wählen Sie **OK**, und Sie sehen die Meldung "calo_root-1 installed".



Schritt 11: Um zu überprüfen, ob das Identitätszertifikat installiert ist, navigieren Sie zur **Registerkarte Einstellungen/Sperrbildschirm und Sicherheit/Andere > Sicherheitseinstellungen/Benutzerzertifikate/System.**


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

Schritt 12: Um zu überprüfen, ob das Zertifizierungsstellenzertifikat installiert ist, navigieren Sie zur **Registerkarte Einstellungen/Sperren und Sicherheit/Andere Sicherheitseinstellungen/Sicherheitszertifikate anzeigen/Benutzer.**


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

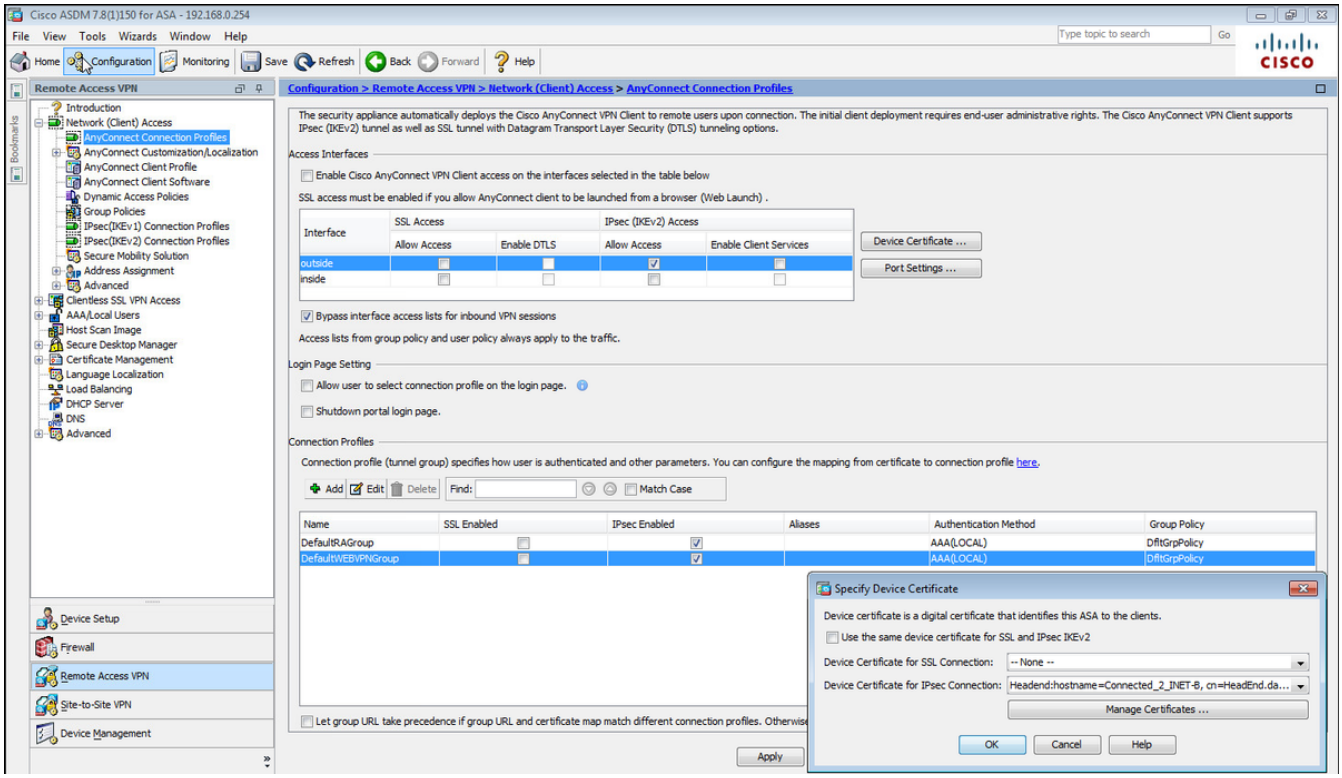
ASA-Headend für RA VPN mit IKEv2 konfigurieren

Schritt 1: Navigieren Sie im ASDM zu **Configuration > Remote Access VPN > Network (client) Access > AnyConnect Connection Profiles**. Aktivieren Sie das Kontrollkästchen **IPSec (IKEv2)-Zugriff zulassen** auf der Schnittstelle, die den VPN-Clients gegenübersteht (**Client-Services aktivieren** ist nicht erforderlich).

Schritt 2: Wählen Sie **Device Certificate aus**, und entfernen Sie das Häkchen aus **Verwenden Sie dasselbe Gerätezertifikat für SSL und IPSec IKEv2**.

Schritt 3: Wählen Sie das Headend-Zertifikat für die IPSec-Verbindung aus, und wählen Sie für die SSL-Verbindung "None" (Keine) aus.

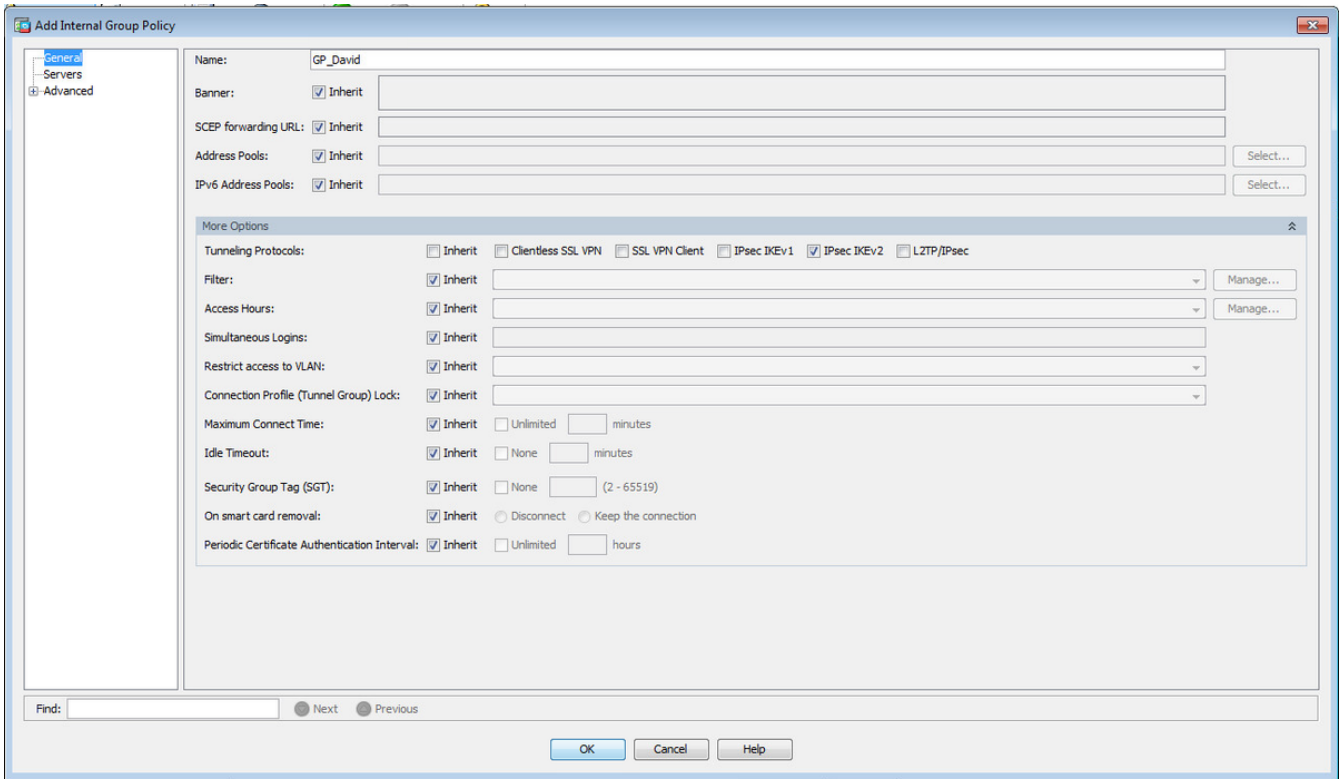
Mit dieser Option wird die Konfiguration crypto ikev2, crypto ipsec, crypto dynamic-map und crypto map implementiert.



Auf diese Weise wird die Konfiguration über die Befehlszeilenschnittstelle (CLI) angezeigt.

```
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
```

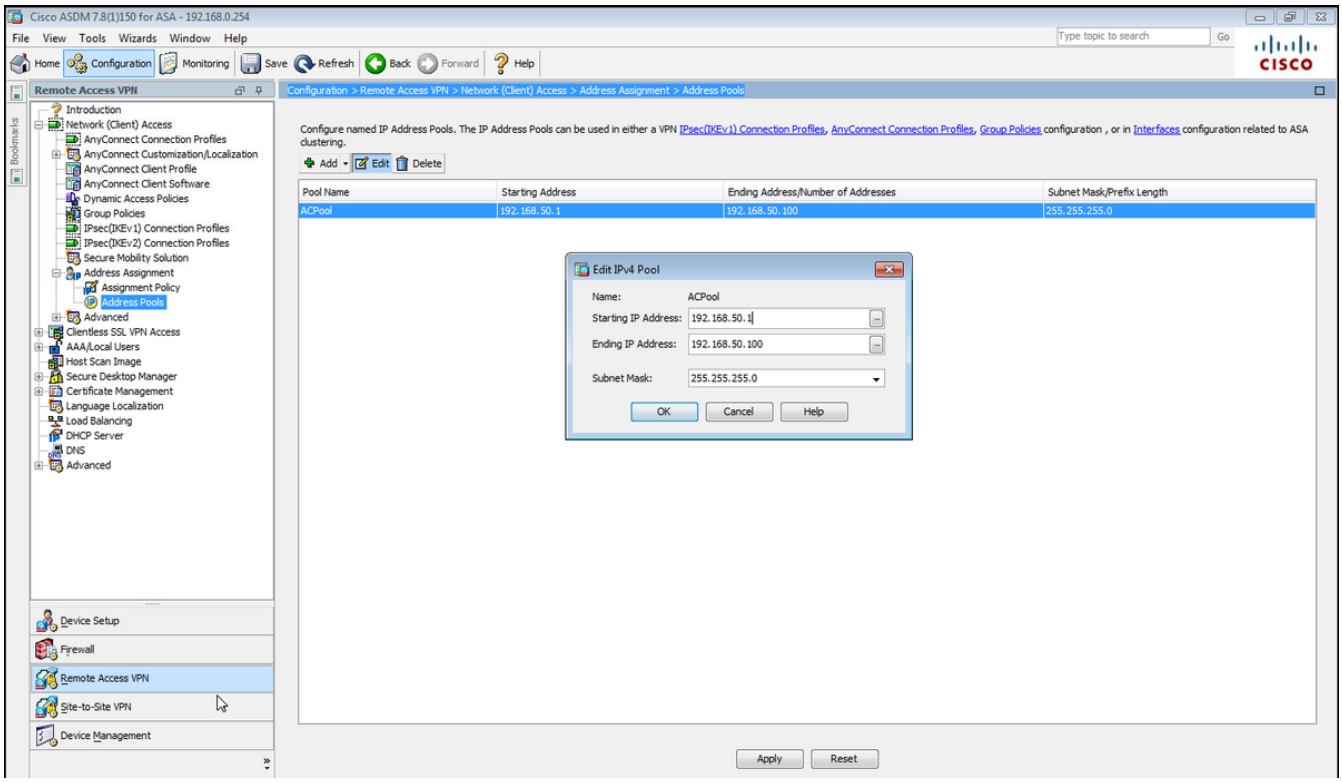
Schritt 4: Navigieren Sie zu **Konfiguration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Gruppenrichtlinien**, um eine Gruppenrichtlinie zu erstellen.



Auf CLI.

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

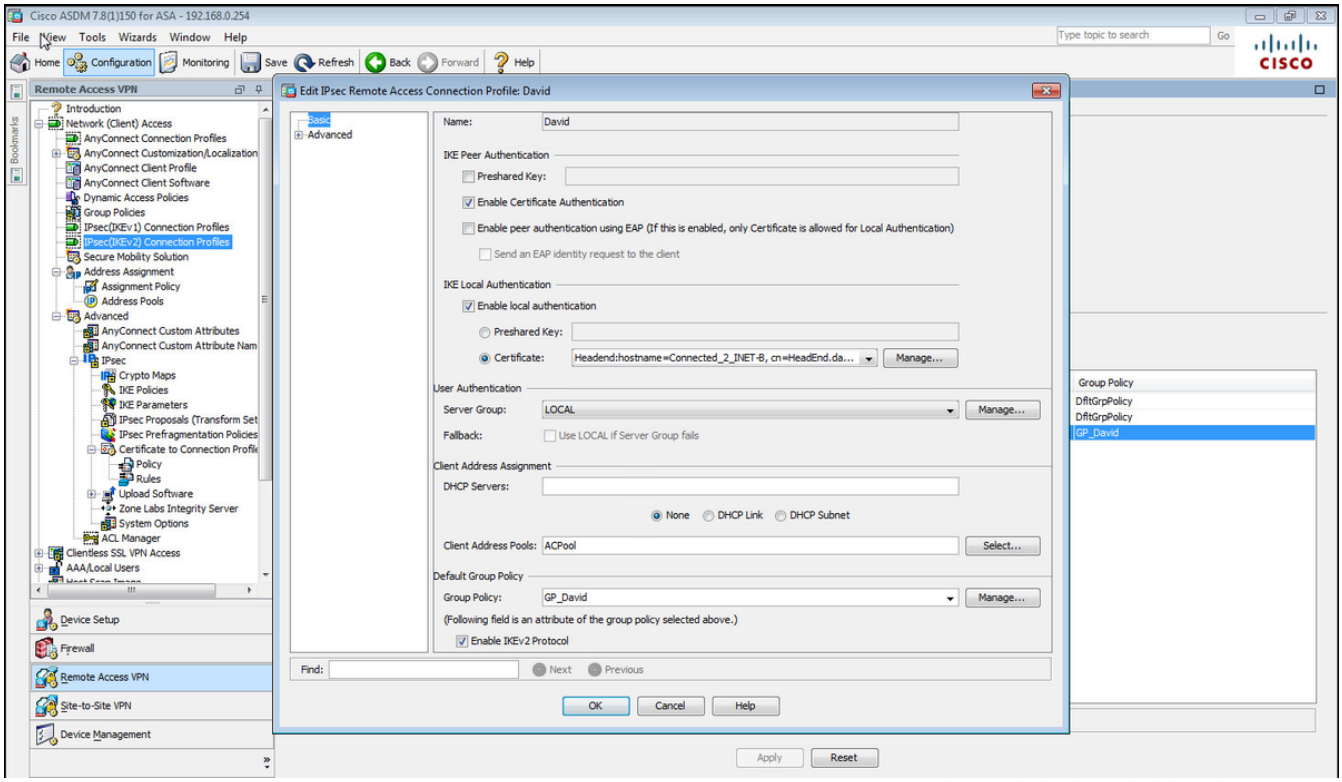
Schritt 5: Navigieren Sie zu **Konfiguration > Remote Access VPN > Network (Client) Access > Address Pools**, und wählen Sie **Add** aus, um einen IPv4-Pool zu erstellen.



Auf CLI.

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

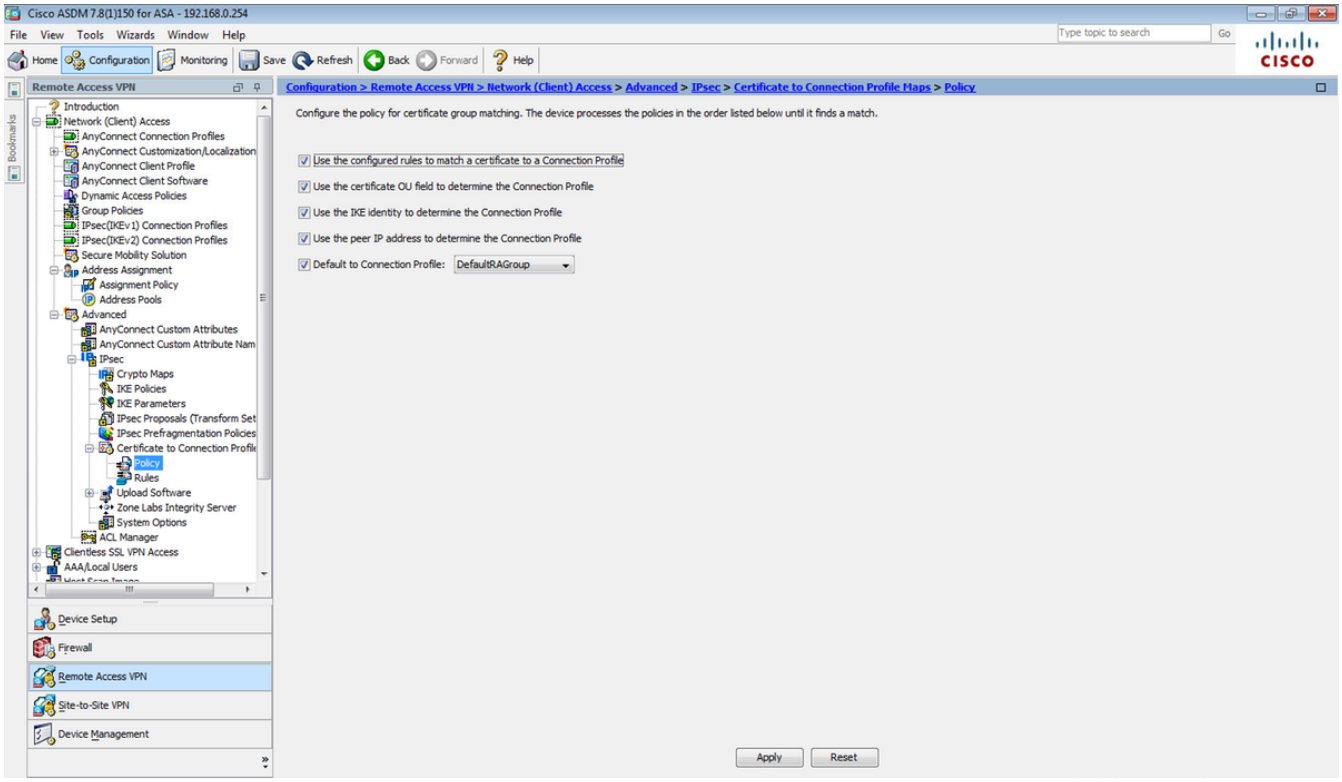
Schritt 6: Navigieren Sie zu **Konfiguration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles**, und wählen Sie **Add** aus, um eine neue Tunnelgruppe zu erstellen.



Auf 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
```

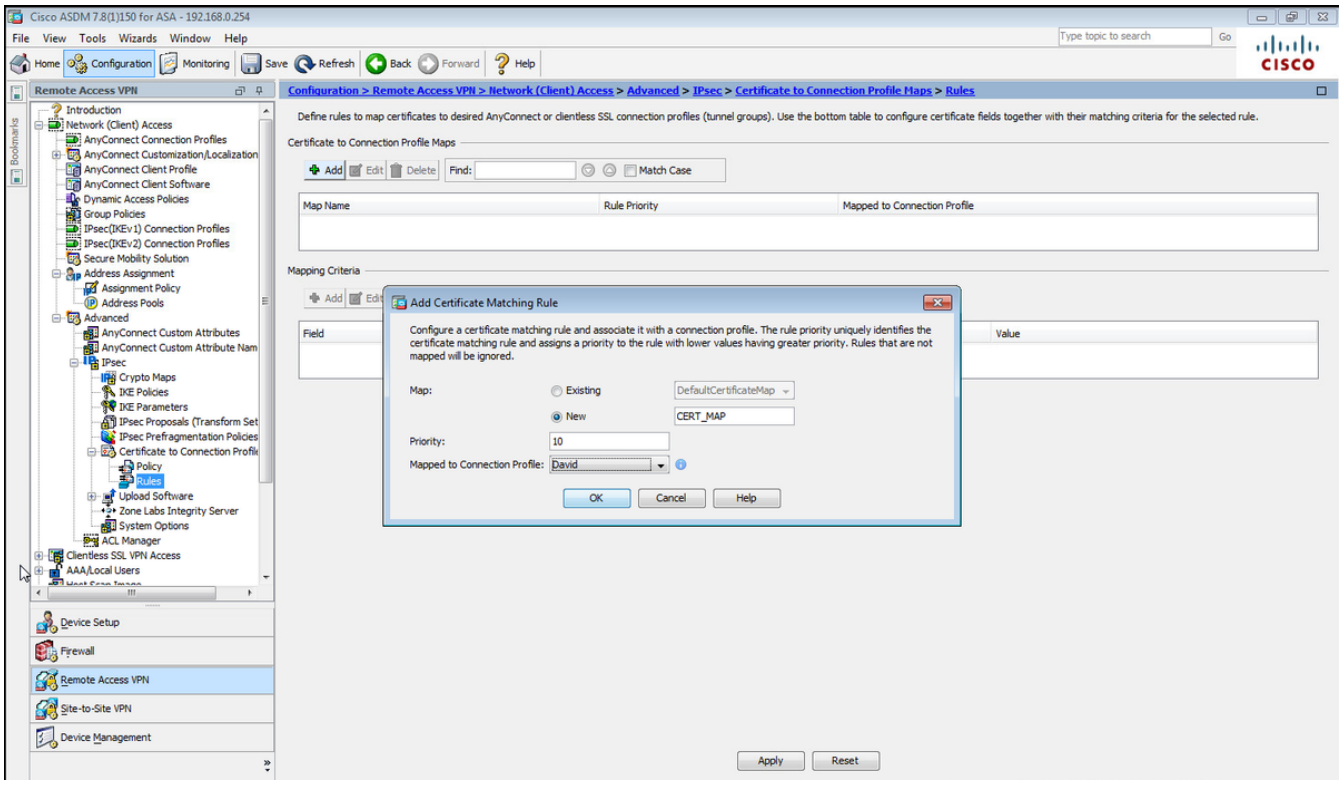
Schritt 7: Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy (Konfiguration > Remote Access VPN > Netzwerk (Client)-Zugriff > Advanced > IPsec > Certificate to Connection Profile maps (Zertifikat für Verbindungsprofil),** und aktivieren Sie das Kontrollkästchen **Used the** the **Used the Rules to Math a a Certificate to a Connection Profile**.



Auf CLI.

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

Schritt 8: Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules**, und erstellen Sie eine neue Zertifikatszuordnung. Wählen Sie **Hinzufügen**, und ordnen Sie es der Tunnelgruppe zu. In diesem Beispiel heißt die Tunnelgruppe **David**.



Auf CLI.

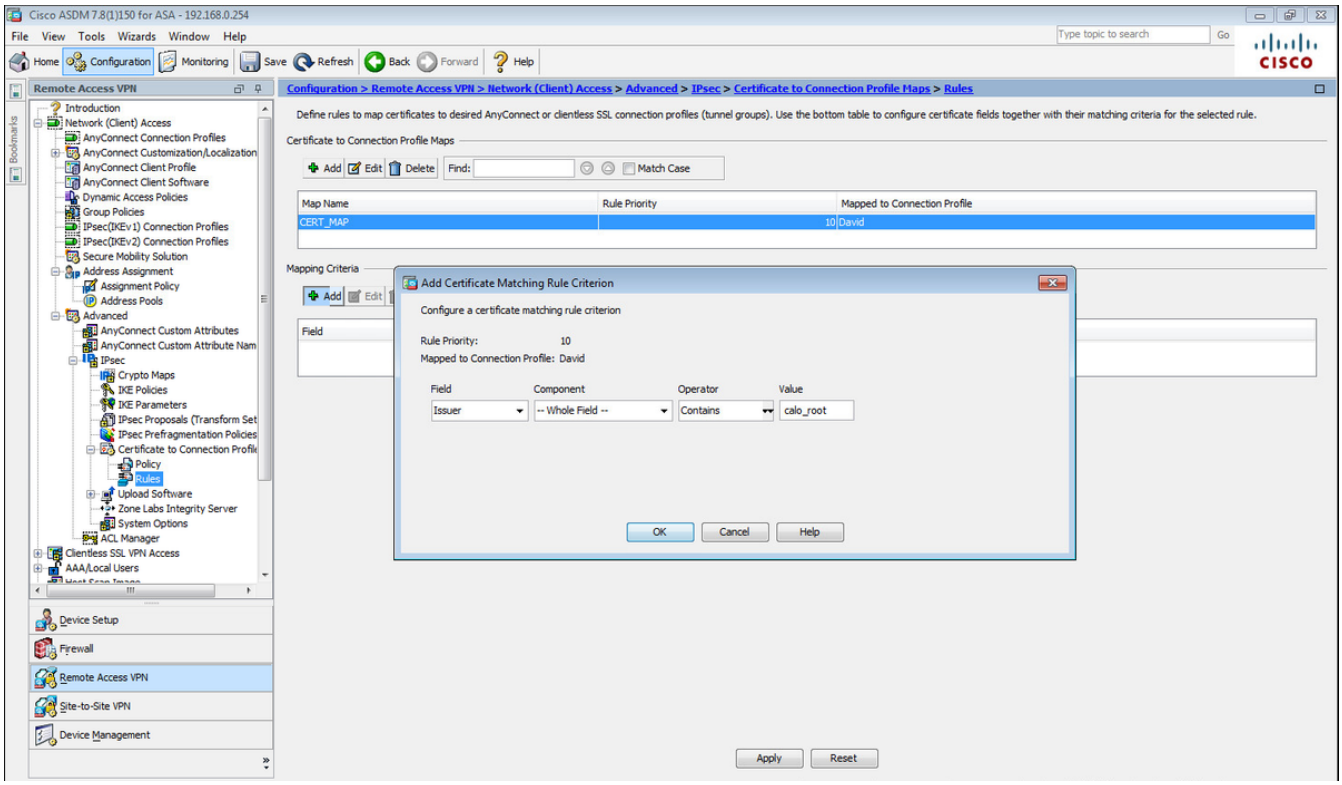
```
tunnel-group-map CERT_MAP 10 David
```

Schritt 9: Wählen Sie **Add** im Abschnitt **Zuordnungskriterien**, und geben Sie diese Werte ein.

Feld: Emittent

Betreiber: Enthält

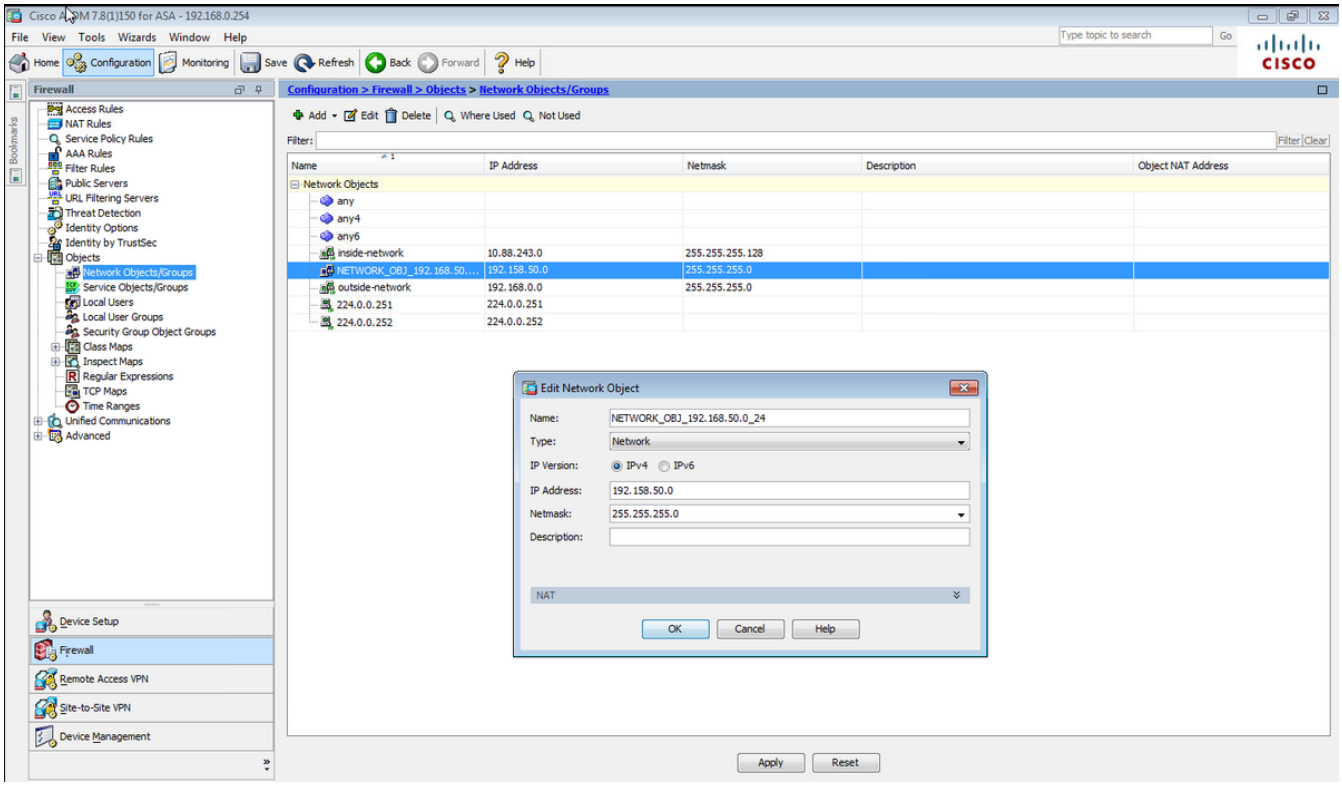
Wert: Calo-Root



Auf CLI.

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

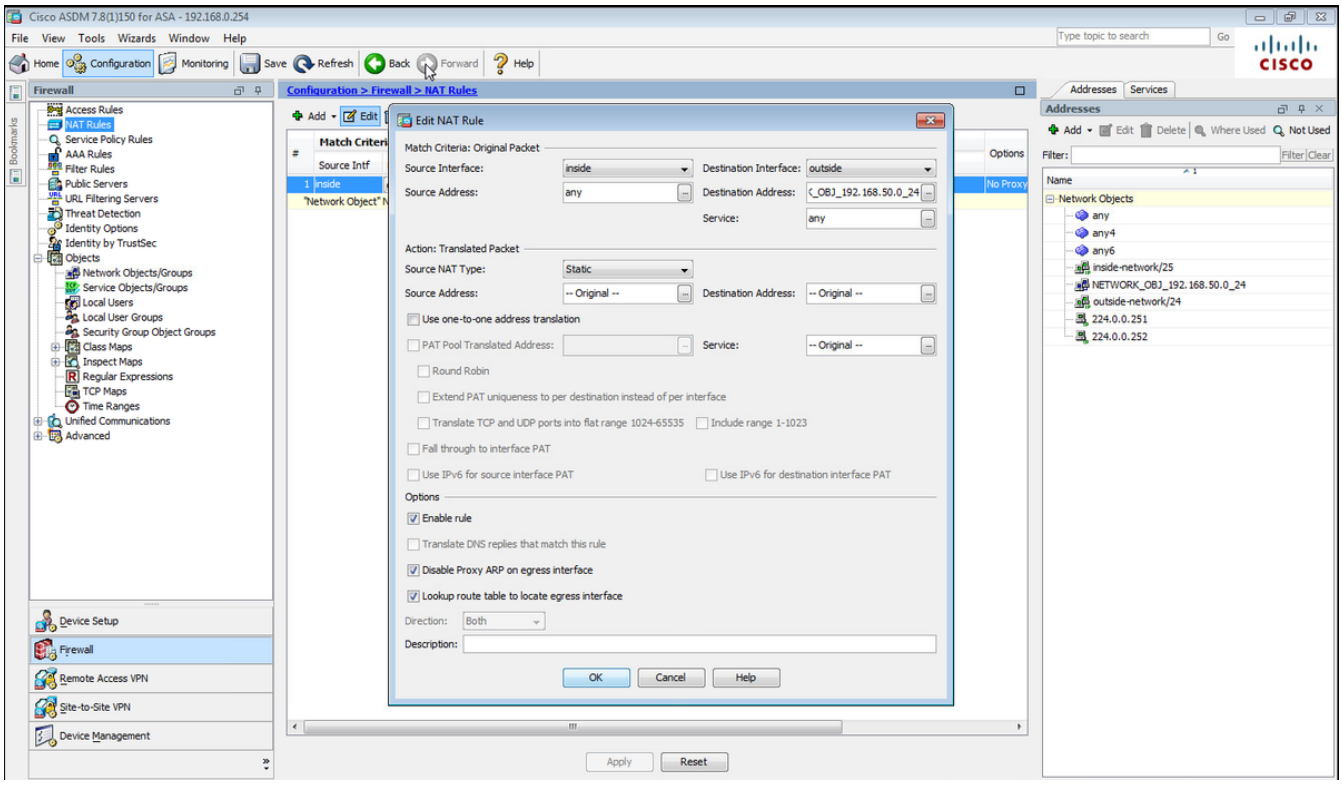
Schritt 10: Erstellen Sie ein Objekt mit dem IP-Pool-Netzwerk, das zum Hinzufügen einer (Network Address Translation) NAT-Ausnahmeregel unter **Konfiguration > Firewall > Objekte > Netzwerkobjekte/Gruppen> Hinzufügen** verwendet werden soll.



Auf CLI.

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

Schritt 11: Navigieren Sie zu **Konfiguration > Firewall > NAT Rules**, und wählen Sie **Add (Hinzufügen)** aus, um die NAT-Freistellungsregel für den RA VPN-Datenverkehr zu erstellen.



Auf CLI.

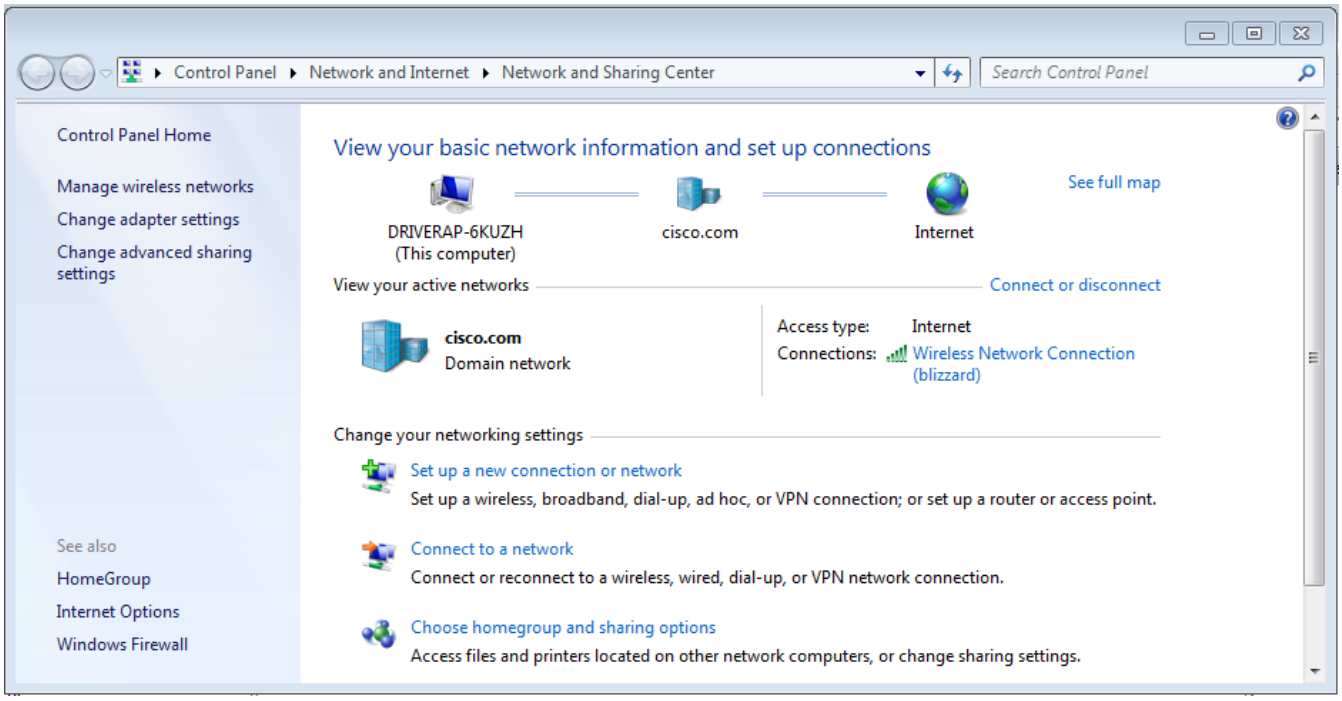
```
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup
```

Dies ist die vollständige ASA-Konfiguration für dieses Beispiel.

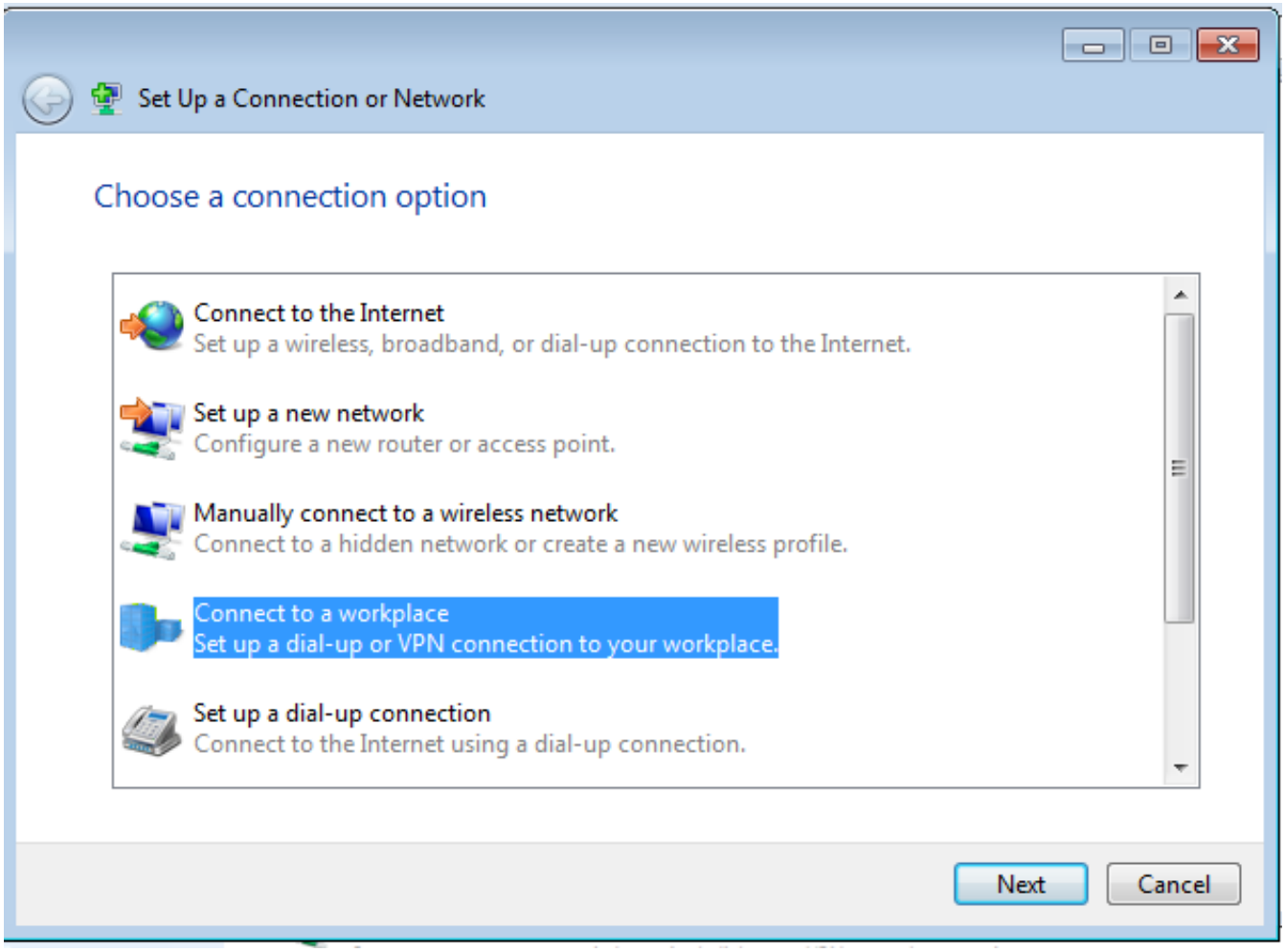
```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.88.243.108 255.255.255.128

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
```

Integrierten Windows 7-Client konfigurieren

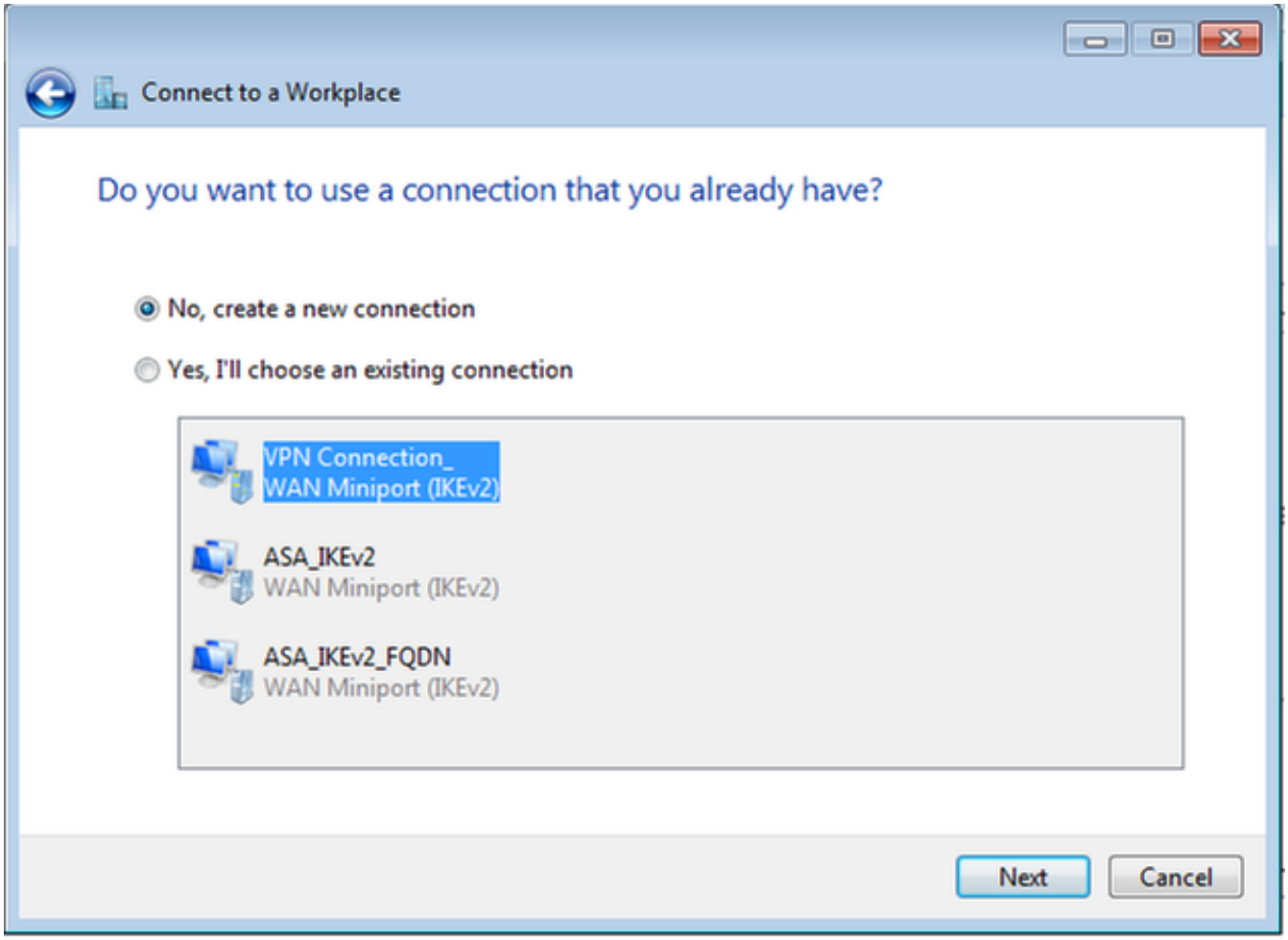
Schritt 1: Navigieren Sie zu **Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter**.



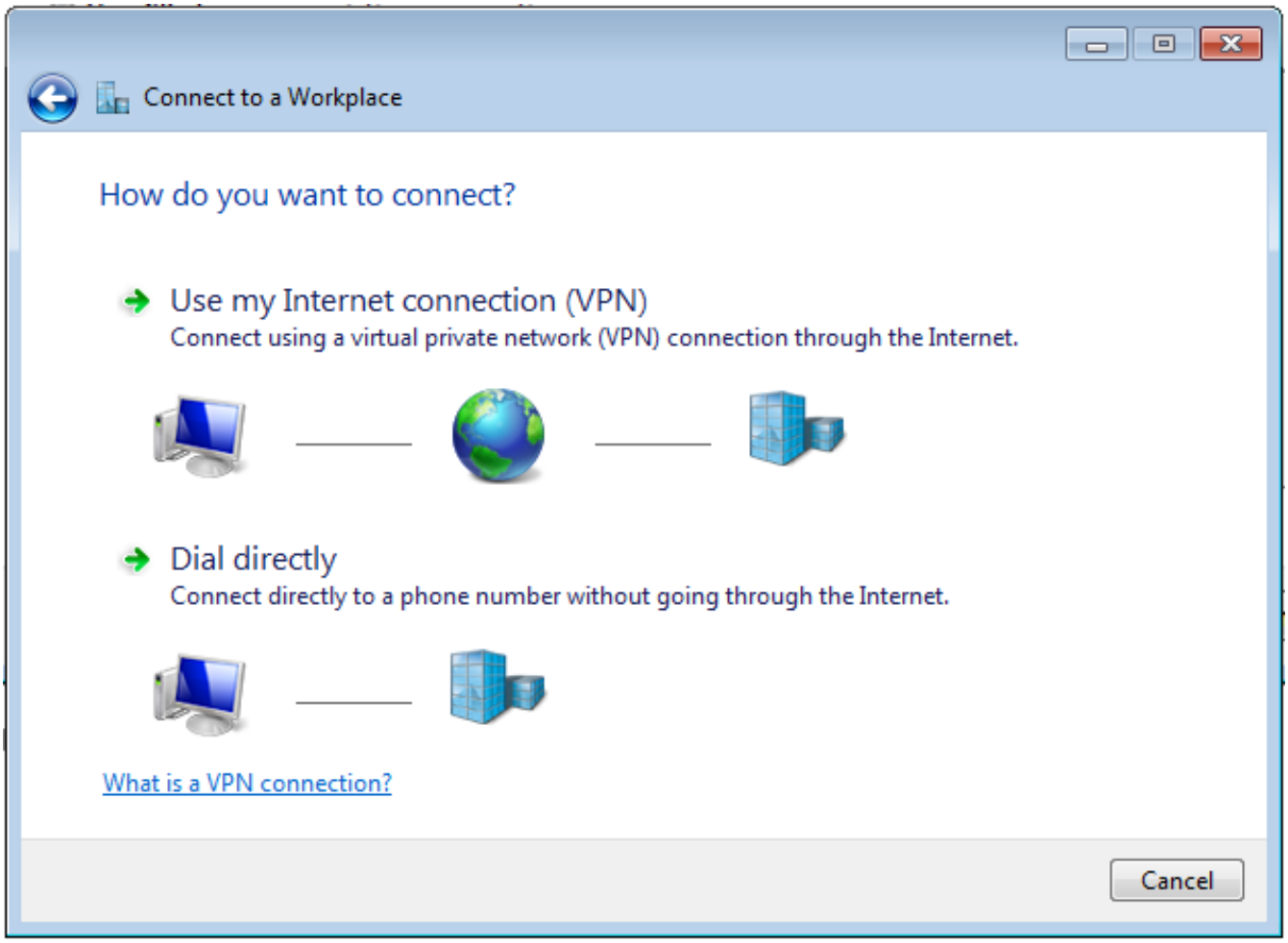
Schritt 2: Wählen Sie **Neue Verbindung oder neues Netzwerk einrichten aus**.



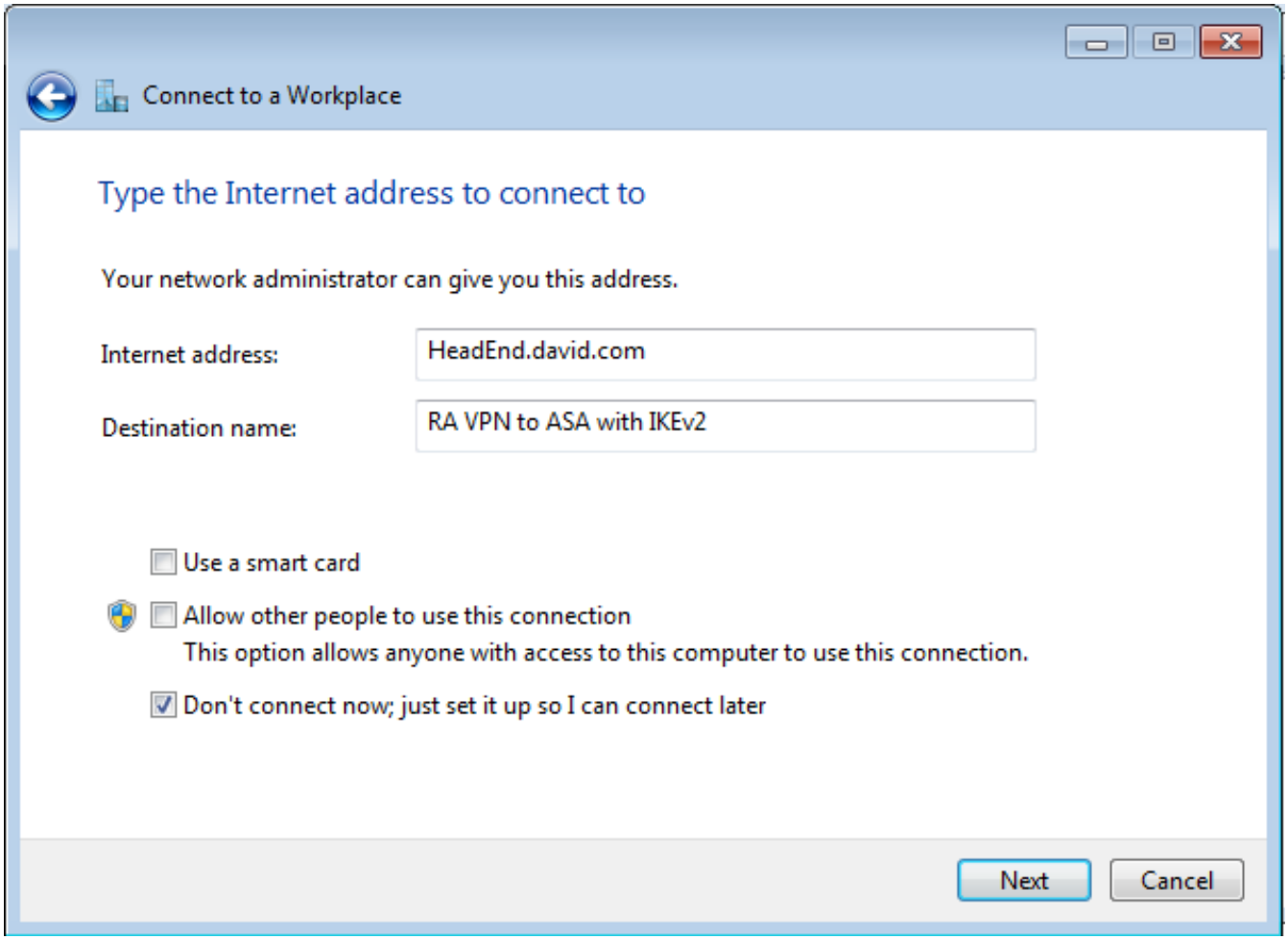
Schritt 3: Wählen Sie **Verbinden mit Arbeitsplatz** und **Weiter aus**.



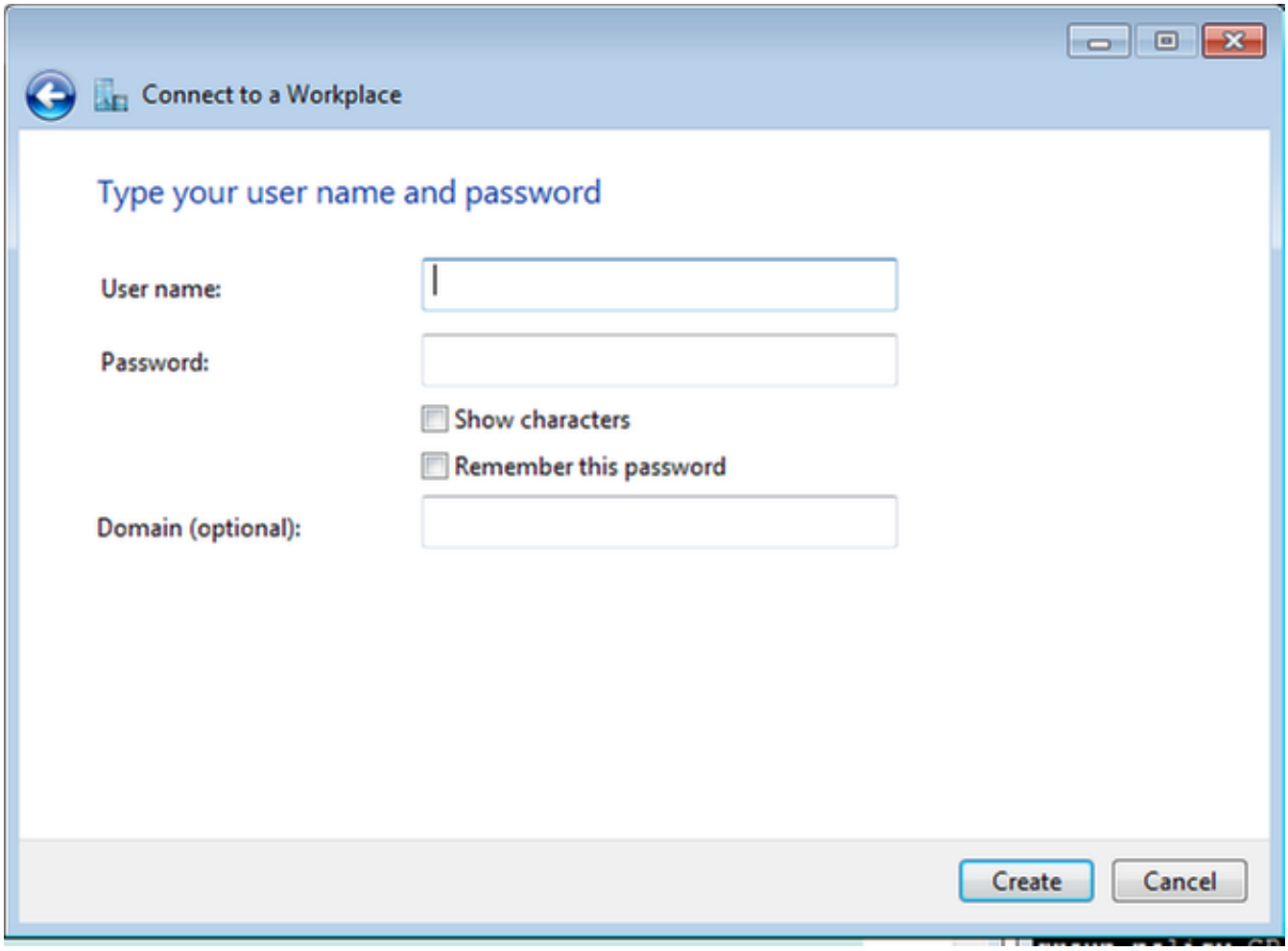
Schritt 4: Wählen Sie **Nein, neue Verbindung erstellen** und **Weiter aus**.



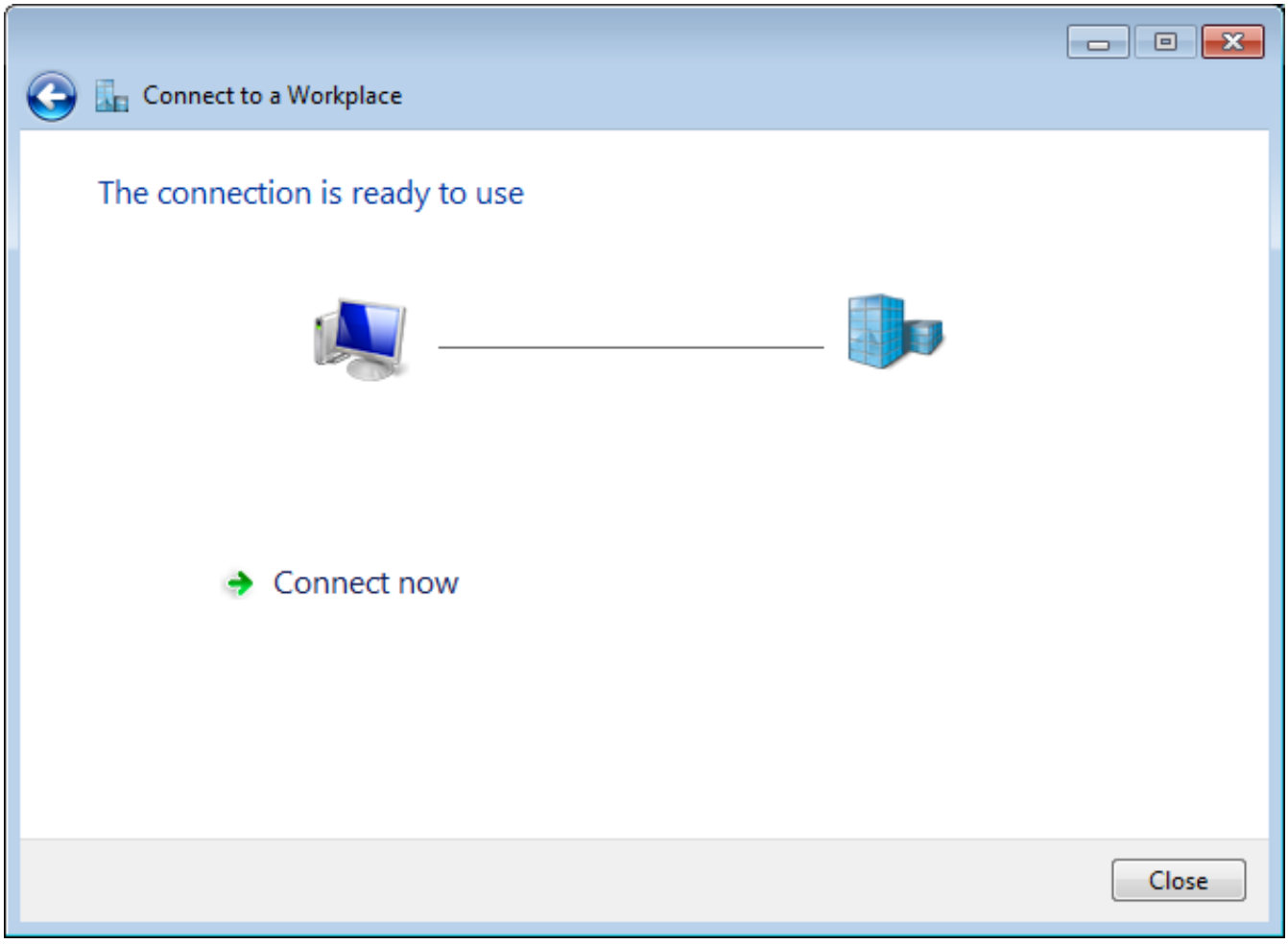
Schritt 5: Wählen Sie **Meine Internetverbindung verwenden (VPN)** aus, und fügen Sie die Zeichenfolge HeadEnd Certificate Common Name (CN) im Feld **Internetadresse** hinzu. Geben Sie im Feld **Zielname** den Namen der Verbindung ein. Dabei kann es sich um eine beliebige Zeichenfolge handeln. Stellen Sie sicher, dass Sie die Option **Keine Verbindung herstellen** aktivieren **aktivieren. einfach einrichten, damit ich später eine Verbindung herstellen kann**.



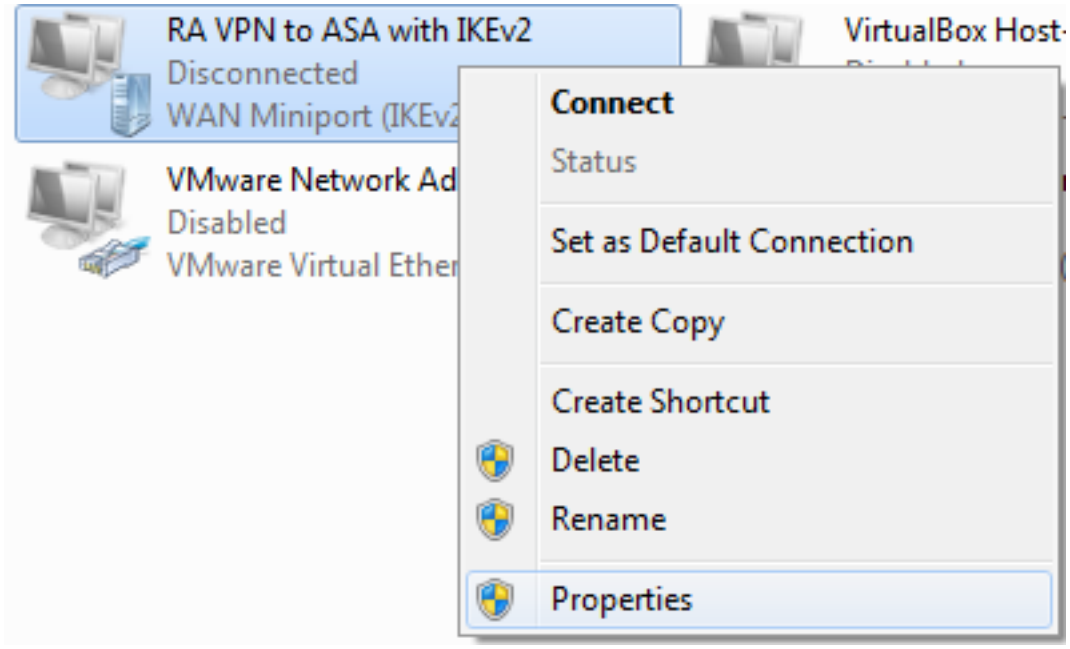
Schritt 6: Wählen Sie **Weiter aus**.



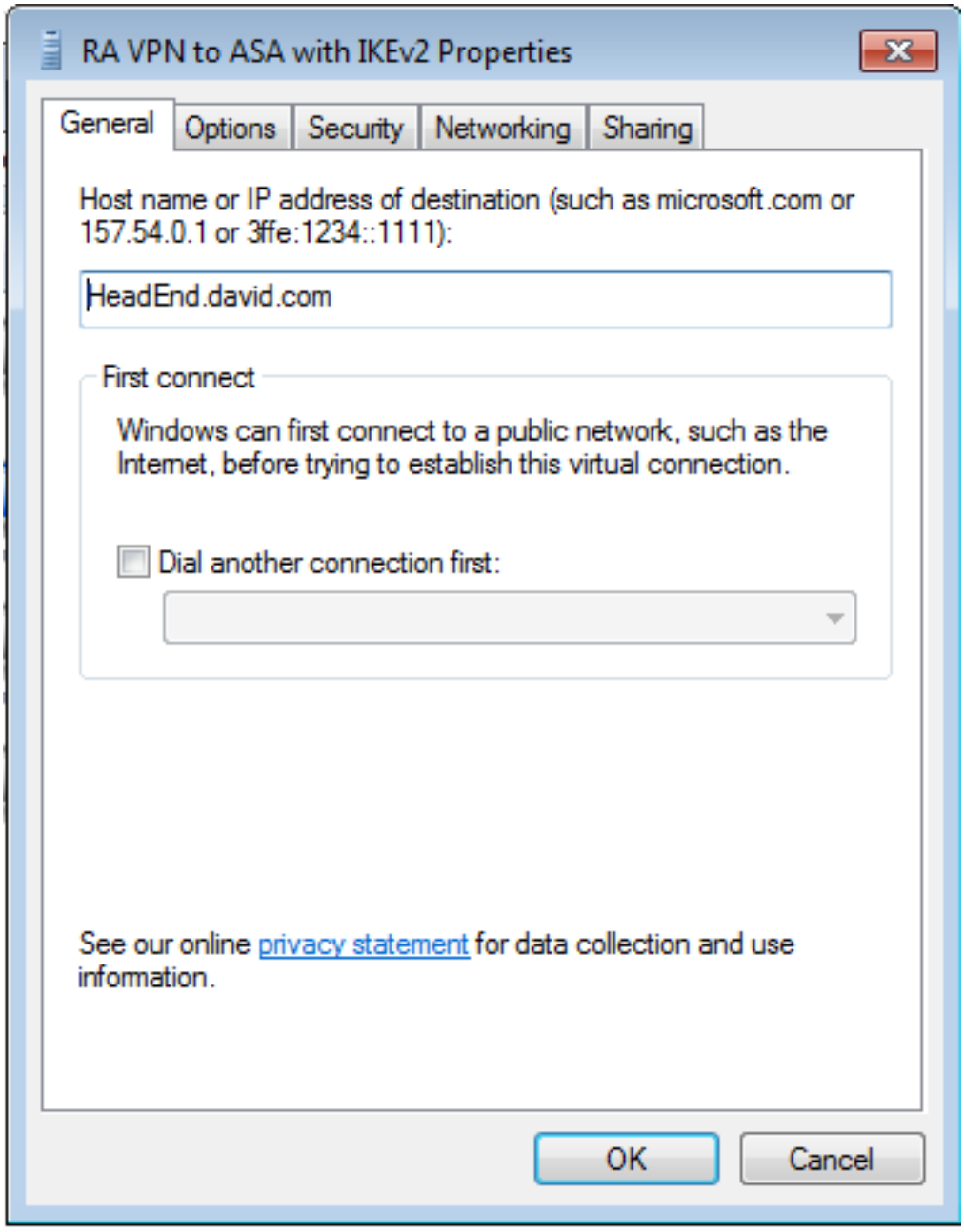
Schritt 7: Wählen Sie **Erstellen aus**.



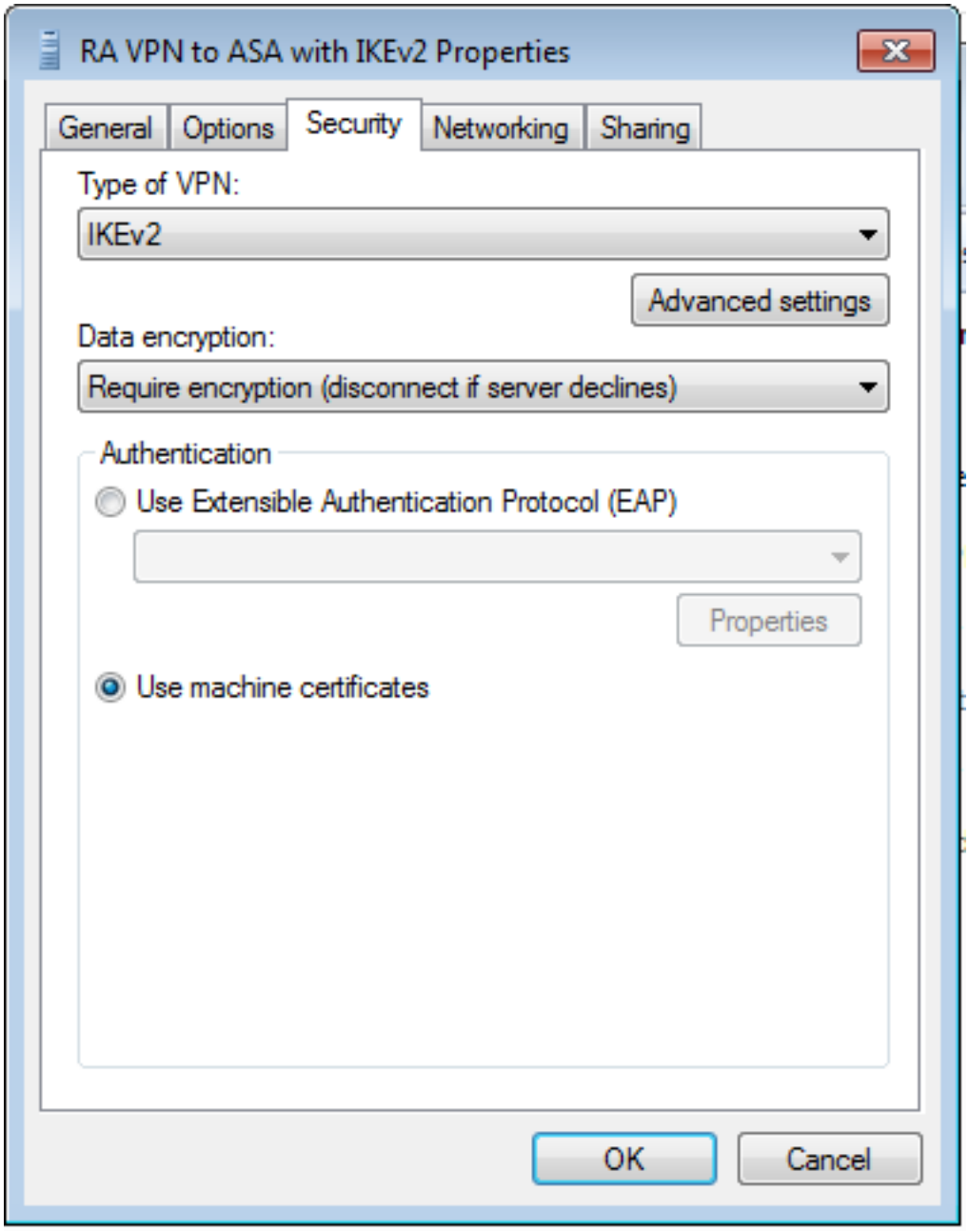
Schritt 8: Wählen Sie **Schließen** aus, und navigieren Sie zu **Systemsteuerung > Netzwerk und Internet > Netzwerkverbindungen**. Wählen Sie die erstellte Netzwerkverbindung aus, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie **Eigenschaften aus**.



Schritt 9: Auf der Registerkarte **Allgemein** können Sie überprüfen, ob der entsprechende Hostname für das Headend korrekt ist. Ihr Computer löst diesen Namen auf die ASA-IP-Adresse auf, die für die Verbindung von RA VPN-Benutzern verwendet wird.



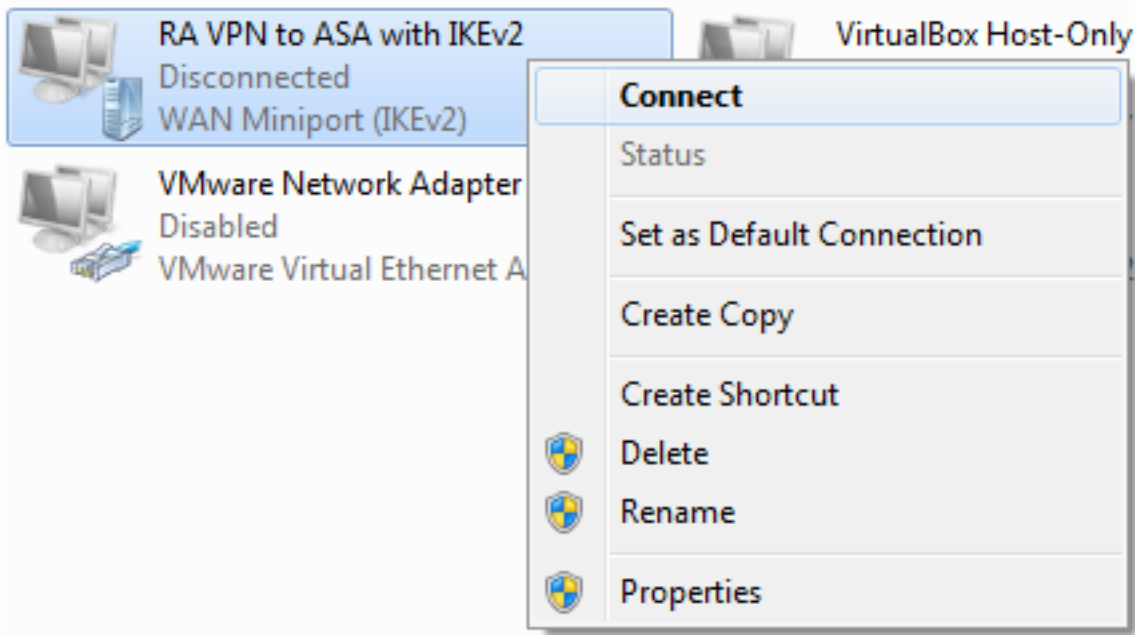
Schritt 10: Navigieren Sie zur Registerkarte **Sicherheit**, und wählen Sie **IKEv2** als **VPN-Typ aus**. Wählen Sie im Abschnitt **Authentifizierung** die Option **Computerzertifikate verwenden aus**.



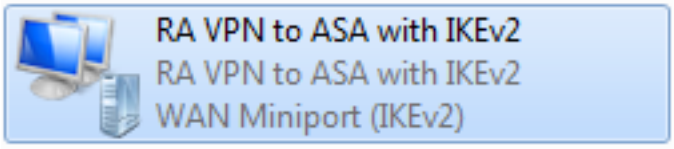
Schritt 11: Wählen Sie **OK** aus, und navigieren Sie zu **C:\Windows\System32\drivers\etc**. Öffnen Sie die **Hosts**-Datei mit einem Text-Editor. Konfigurieren Sie einen Eintrag, um den (vollqualifizierten Domänennamen) FQDN aufzulösen, der in der Netzwerkverbindung mit der IP-Adresse des ASA-Headends konfiguriert wurde (in diesem Beispiel die externe Schnittstelle).

```
# 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
```

Schritt 12: Gehen Sie zurück zu **Systemsteuerung > Netzwerk und Internet > Netzwerkverbindungen**. Wählen Sie die von Ihnen erstellte Netzwerkverbindung aus. Klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Verbinden aus.**



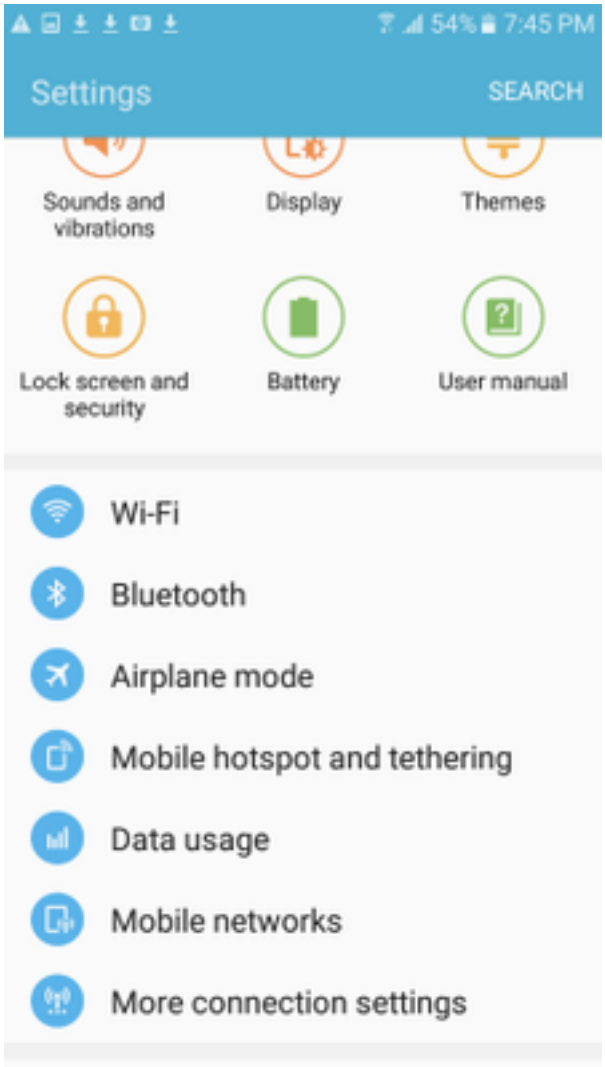
Schritt 13: Der Status der Netzwerkverbindung wechselt von "getrennt" zu "Verbindung" und dann zu "Verbunden". Schließlich wird der Name angezeigt, den Sie für die Netzwerkverbindung angegeben haben.



Der Computer ist an diesem Punkt mit dem VPN-Headend verbunden.

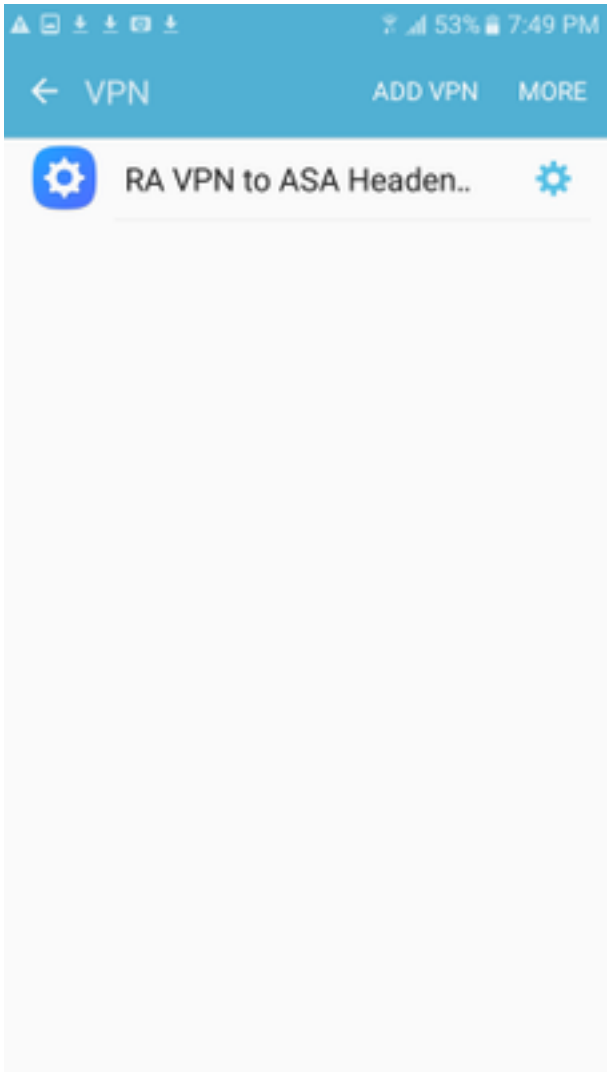
Konfigurieren des nativen Android-VPN-Clients

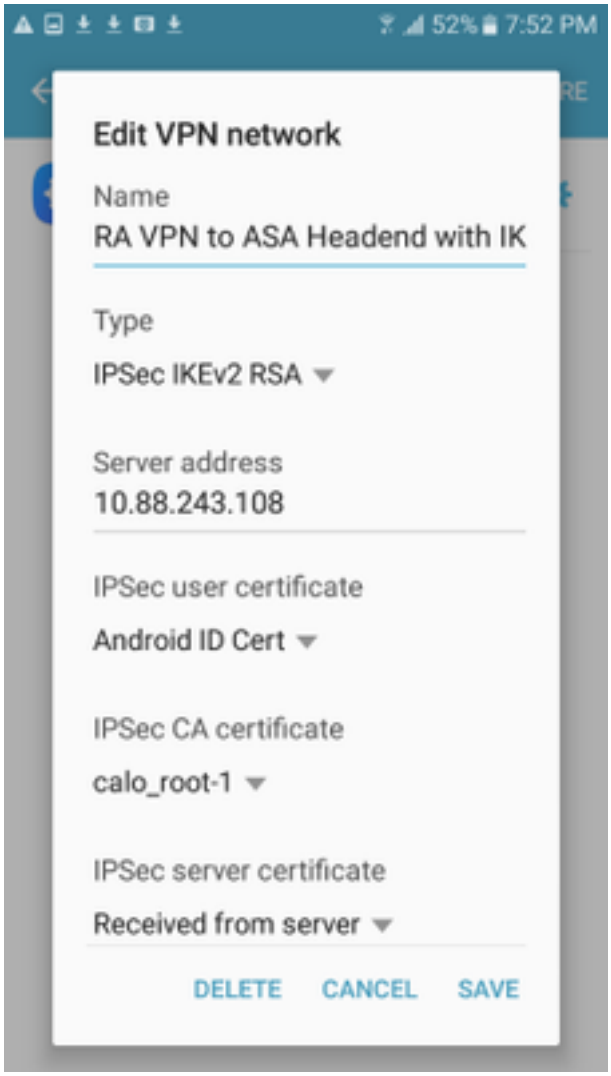
Schritt 1: Navigieren Sie zu **Einstellungen>Weitere Verbindungseinstellungen.**



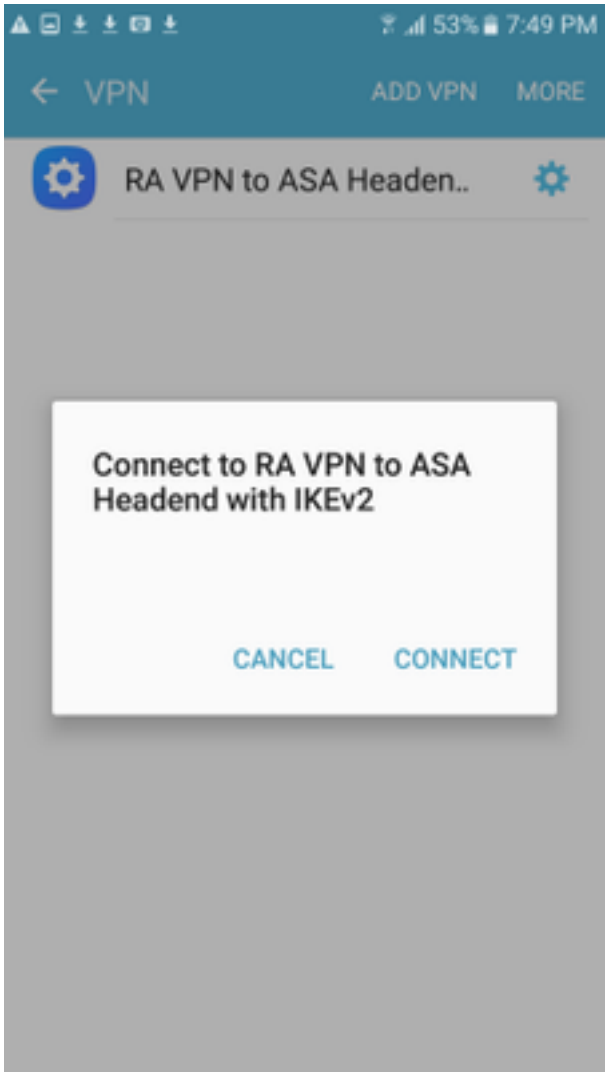
Schritt 2: **VPN** auswählen

Schritt 3: Wählen Sie **VPN hinzufügen aus**. Wenn die Verbindung bereits wie in diesem Beispiel erstellt wurde, tippen Sie auf das Modulsymbol, um sie zu bearbeiten. Geben Sie im Feld **Typ** IPSec IKEv2 RSA an. Die **Serveradresse** ist die IP-Adresse der IKEv2-fähigen ASA-Schnittstelle. Wählen Sie für das **IPSec-Benutzerzertifikat** und das **IPSec CA-Zertifikat** die Zertifikate aus, die durch Tippen auf die Dropdown-Menüs installiert wurden. Lassen Sie das **IPSec-Serverzertifikat** mit der Standardoption Received from server (Vom Server empfangen).

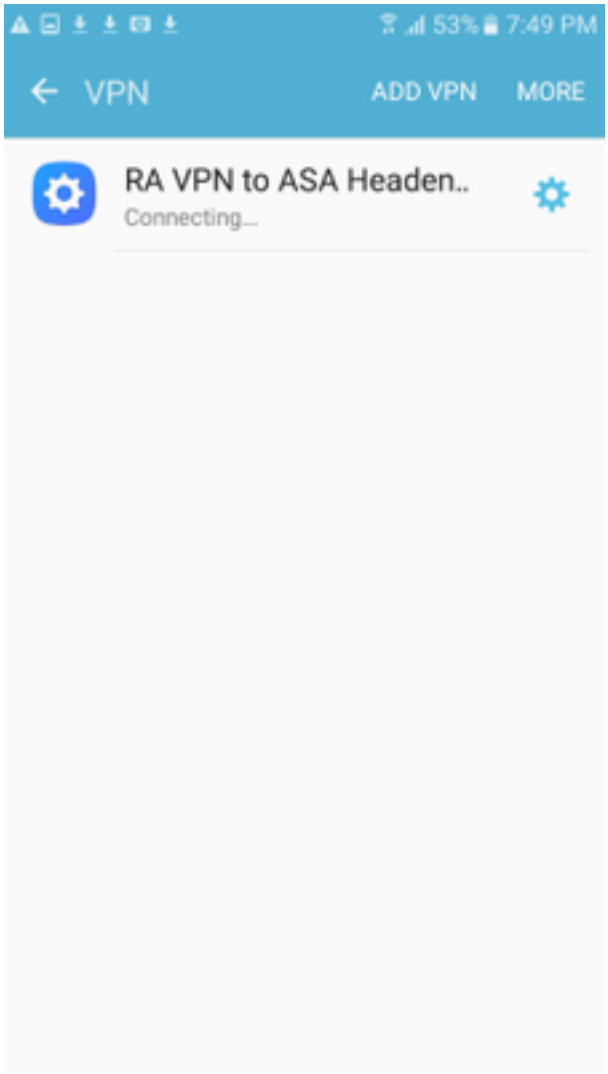

53% 7:49 PM
VPN
ADD VPN
MORE
RA VPN to ASA Headen..

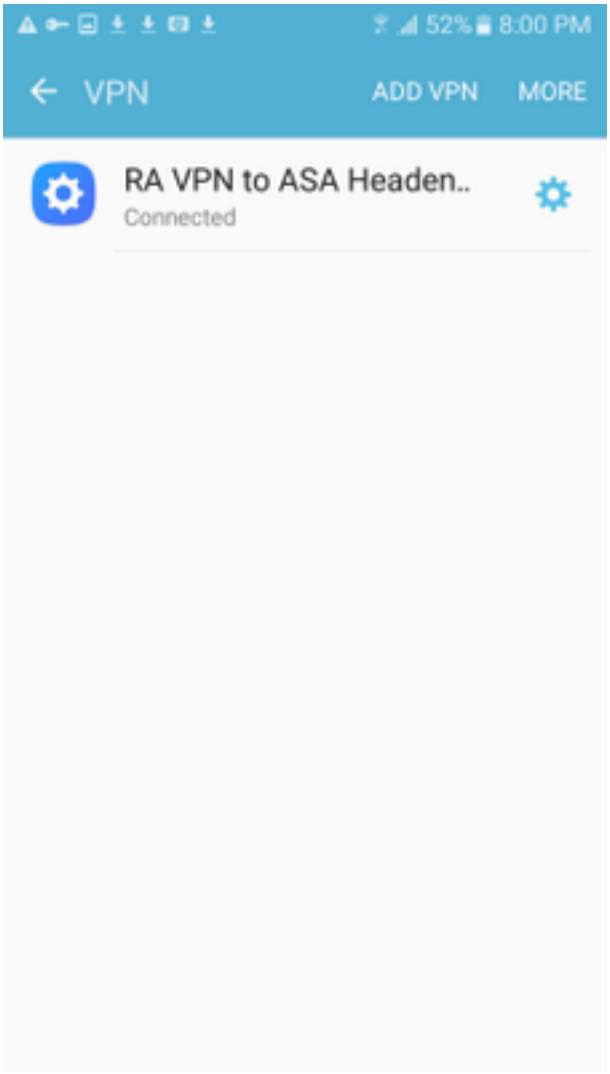


Schritt 4: Wählen Sie **Save (Speichern)** und tippen Sie dann auf den Namen der neuen VPN-Verbindung.

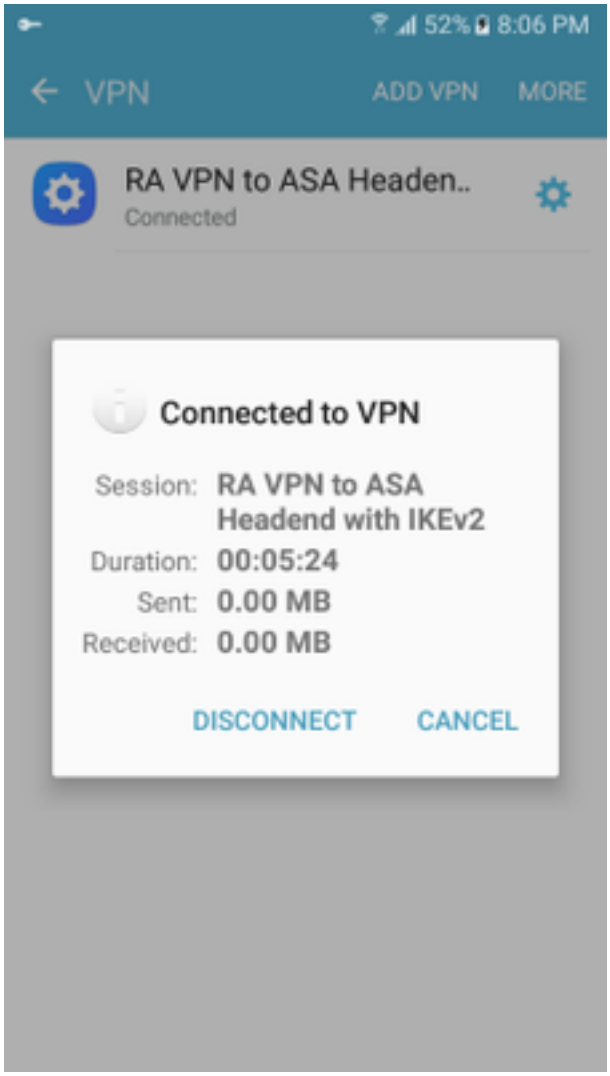


Schritt 5: Wählen Sie **Verbinden aus.**


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



Schritt 6: Geben Sie die VPN-Verbindung noch einmal ein, um den Status zu überprüfen. Es wird jetzt als **Verbunden** angezeigt.



Überprüfen

Überprüfungsbefehle auf ASA-Headend:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

> **Hinweis**: Weitere Informationen zu Debug-Befehlen finden Sie unter Wichtige Informationen, bevor Sie Debugbefehle verwenden.

> **Vorsicht**: Auf ASA können Sie verschiedene Debug-Level festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debugebene ändern, wird die Ausführlichkeit der Debuggen erhöht. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

- **Debug crypto ikev2 Protocol 15**
- **Debug crypto ikev2-Plattform 15**
- **Debug crypto ca 255**