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

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Übersicht Zertifizierungsstelle konfigurieren Erstellen eines Clientzertifikats Installieren des Identitätszertifikats auf dem Windows 7-Client-Computer So installieren Sie das Identitätszertifikat auf Ihrem Android-Mobilgerät ASA-Headend für RA VPN mit IKEv2 konfigurieren Integrierten Windows 7-Client konfigurieren Konfigurieren des nativen Android-VPN-Clients Überprüfen Fehlerbehebung

# 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<sup>Standard</sup> 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>
8
% 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: Uberprüfen 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: A000000
     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: 8600000
     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.

#### <cisco123>

Exported pkcs12 follows:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEqquGMIILqjCCC34GCSqGSIb3DQEH BqCCC28wqqtrAqEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74qYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+qnNZLWs3eU1n84rryZq5Pjw3MRTu2yXDvr799qvx7NIZH5yUZyV11T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg VbYsR+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3H1HCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L01CeUcVDM8aQfy HJSPk/VmfQ01XwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs y155wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfqrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948op1YFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eg1sBLs1wPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9qnMqMJmikP2qhqOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX290aDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmL1SbVIvGq1H9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHISA92pplS7VFrAWP65wrhs4XOf4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwM1AkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/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  ${\tt BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz}$ Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/1X1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg Vbysr+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3H1HCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L0lCeUcVDM8aQfy HJSPk/VmfQ01XwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs y155wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/X0kEvp3Sq0kLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD51+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9qnMqMJmikP2qhqOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDji5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGqX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6eqZS0SjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4X0f4YSF1M89Sn4 GD/yEsGVJzwGrxqCNnOZkLIKsFbI0jp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAqIEAA==

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: A000000
     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: 8600000
     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.

Console1 - [Console Root]					
File Action View Favorites Wind	low Help		- 8 ×		
Console Root	Name		Actions		
	There are no items to show in this view.	Console Root 🔺			
			More Actions		

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

Console1 - [Console Root]		
🚡 File Action View Favorites Windo	ow Help	- 8 ×
🦛 🔿 🔲 🖬 🔒 🖬 🖬		
Console Root	Add or Remove Snap-ins Actions	
	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.	<b>^</b>
	Available snap-ins: Selected snap-ins:	•
	Snap-in Vendor Console Root Edit Extensions	
	Remove	
	Certificates Microsoft Cor	
	Component Services Microsoft Cor     Microsoft Cor	
	Device Manager Microsoft Cor	
	Disk Management Microsoft and	
	Grosoft Cor     Folder Microsoft Cor	
	Group Policy Object Microsoft Cor	
	B P Security Monitor 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.	
	OK Cancel	

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

Console1 - [Console Root]	
	<u> </u>
Console Root Name	Actions
	Console Root
Add or Remove Snap-ins	More Actions
You can select snap-ins for this console from those available on your computer and configure the selected services by you can configure which extensions are enabled.       Certificates snap-in         Available snap-ins:       Selected snap-ins:       This snap-in will always manage certificates for:         Active X Control       Microsoft Cor       Console Root       My user account         Computer Manager       Microsoft Cor       Add >       Selected snap-ins:       This snap-in will always manage certificates for:         Device Manager       Microsoft Cor       Add >       Computer Microsoft Cor       Or power account         Disk Management       Microsoft Cor       Add >       Computer account       Computer account         Disk Management       Microsoft Cor       Add >       Computer account       Computer account         Disk Management       Microsoft Cor       Add >       Computer account       Computer account         Disk Management       Microsoft Cor       Add >       Computer account       Computer account         Disk Management       Microsoft Cor       Core policy Object       Microsoft Cor       Computer account         Disk Management       Microsoft Cor       Core policy Object       Microsoft Cor       Core object account         Description:       The Certificates snap-in allows you to br	Next > Cancel

### Schritt 6: Wählen Sie Weiter,

		Actions Console Root
Add of Kernove Snap-ins, for this console from those available on your correctensible snap-ins, you can configure which extensions eenabled.         Available snap-ins:       Select         Snap-in       Vendor         ActiveX Control       Microsoft Cor         ActiveX Control       Microsoft Cor         Component Services       Microsoft Cor         Device Manager       Microsoft Cor         Device Manager       Microsoft Cor         Device Manager       Microsoft Cor         Power Newer       Microsoft Cor         Power Newer       Microsoft Cor         Power New Microsoft Cor       Power Newer Microsoft Cor         P Security Policy Micro       Microsoft Cor         P Security Policy Micro       Microsoft Cor         P Security Policy Micro       Microsoft Cor         Wick Moderes       Microsoft Cor         Microsoft Cor       Micros	cate stores for yourself, a serv	n to manage. s console is running on) Changed when launching from the command line. This e. Changed when launching from the command line. This

Schritt 7: Beenden Sie.

Console1 - [Console Root]							
File Action View Favorites Win	dow Help						- 8 ×
	10.0					1	
Console Root	Name					Actions	
	Add or Remove Snap-ins				<b>—</b> ———————————————————————————————————	Console Root	<b>^</b>
	You can select snap-ins for extensible snap-ins, you can Available snap-ins:	this console from those in configure which exten	available on your nsions are enabled Se	computer and configure the selected elected snap-ins:	set of snap-ins. For	More Actions	,
	Snap-in	Vendor ^		Console Root	Edit Extensions		
	activeX Control	Microsoft Cor		Certificates (Local Computer)	Remove		
	Authorization Manager	Microsoft Cor			Kellove		
	Certificates	Microsoft Cor			Movello		
	Component Services	Microsoft Cor			Move op		
	Device Manager	Microsoft Cor			Move Down		
	Disk Management	Microsoft and	A00 >				
	Event Viewer	Microsoft Cor					
	Folder	Microsoft Cor					
	Group Policy Object	Microsoft Cor					
	IP Security Policy M	Microsoft Cor					
	Link to Web Address	Microsoft Cor			Advanced		
	Description:						
	The Certificates snap-in all	ows you to browse the	contents of the c	ertificate stores for yourself, a service	e, or a computer.		
				_			
					OK Cancel		
<u></u>	L						

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**:

🚡 Console1 - [Console Root\Certificates (Loc	al Computer)\Pe	ersonal\Certificates]						
🚡 File Action View Favorites Windo	ow Help							_ 8 ×
🗢 🤿 💋 🗊 📋 🙆 🛃 🗊								
Console Root	Issued To	*	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
Certificates (Local Computer)	DRIVERAP-6	KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	<b></b>
Personal							More Actions	•
Certificates	•	Request New	Certificate					
Enterprise		Import						
▷ ☐ Intermedia ▷ ☐ Trusted Pu New Window fro	m Here	Advanced Op	erations >					
▷ ☐ Untrusted ▷ ☐ Third-Party New Taskpad Vie	ew							
Trusted Per Refresh								
Other Peop Export List								
▷ Ams ▷ CanaryCert Help								
InjectorCertStore		-						
McAfee Trust     PolicyCertStore								
Remote Desktop								
Certificate Enrollment Requests								
Smart Card Trusted Roots								
⊳ SMS								
Trusted Devices								
	1							
Add a certificate to a store						,		

#### Certificate Import Wizard



# Welcome to the Certificate Import Wizard

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

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

To continue, click Next.

< Back Next > Cancel	

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

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
File name:	
C:\TFTP-Root\Win7_PC.p12 Browse	
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 <u>certificate file formats</u>	
< Back Next > Cano	el

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*.

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
<ul> <li>Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.</li> <li>Mark this key as exportable. This will allow you to back up or transport your keys at a later time.</li> </ul>
Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

Schritt 12: Wählen Sie Weiter aus.

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.
O Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Personal Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

Schritt 13: Wählen Sie noch einmal Weiter aus.



Schritt 14: Wählen Sie Fertig stellen aus.

Certificate Import Wizard
The import was successful.
ОК

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

Console1 - [Console Root\Certificates (Lo	cal Computer)\Personal\Certificates]						
File Action View Favorites Wind	low Help						- 8 ×
Console Root Certificates (Local Computer) Personal Certificates (Local Computer) Personal Certificates Personal Certificates Personal Certificates Personal Trusted Root Certification Author Trusted Publishers Differ People Differ P	Issued To	Issued By calo_root DRIVERAP-6KUZH calo_root	Expiration Date 7/12/2020 7/13/2022 7/13/2018	Intended Purposes <all> <all> Server Authenticati</all></all>	Friendly Na cn=cal_roc <none> cn=Win7_P</none>	Actions Certificates More Actions	.,
×	<	III			4		
Personal store contains 3 certificates.						,	

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

Console1 - [Console Root) Certificates (Lo	cal Computer)\Trusted Root Certificati	on Authorities\Certificates]					
Eile Action View Envoriter Wind	low Help	an Additional Steel an editory					
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly ^	Actions	
Certificates (Local Computer)	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati	The USE	Certificates	<b></b>
a Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati	DigiCert	More Actions	•
Certificates	🙀 calo_root	calo_root	7/12/2020	<all></all>	cn=calo	more reality	
Certificates	Certum CA	Certum CA	6/11/2027	Server Authenticati	Certum	calo_root	-
Enterprise Trust	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati	Certum E	More Actions	•
Intermediate Certification Author	Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>		
Trusted Publishers	Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Untrusted Certificates	🔄 Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Third-Party Root Certification Aut	🔄 Cisco Root CA M2	Cisco Root CA M2	11/12/2037	<all></all>	<none></none>		
Trusted People	Gisco RXC-R2	Cisco RXC-R2	7/9/2034	<all></all>	<none></none>		
Other People	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Secure Email, Client	VeriSign		
Ams	COMODO RSA Certification Au	COMODO RSA Certification Auth	1/18/2038	Server Authenticati	COMOE		
CanaryCertStore	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microso		
InjectorCertStore	Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serve	Deutsch		
McAfee Trust	🔄 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati	DigiCert		
PolicyCertStore	DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati	DigiCert		
Kemote Desktop	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Server Authenticati	DigiCert		
Certificate Enrollment Requests	DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>		
	DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com	1/12/2021	<all></all>	<none></none>		
SPC	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
Trusted Devices	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></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.		
	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Server Authenticati	Entrust		
۰	CEEnuifay Secure Certificate Auth	Equifav Secure Certificate Authority III	8/22/2018	Servire Emsil Serve	GenTrue		
Trusted Root Certification Authorities store co	ontains 60 certificates.						

Console1 - [Console Root\Certificates (Lo	cal Computer)\Personal\Certificates]						- • •
🔚 File Action View Favorites Wind	low Help						- 8 ×
◆ ⇒   2 🗊 📋 🖻 🕞 🖉 🗊							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
Certificates (Local Computer)	🛱 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	
Certificates	Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati	cn=Win7_P	More Actions	•
a 📋 Trusted Root Certification Author							
Certificates							
Enterprise Trust							
Trusted Publishers							
Untrusted Certificates							
Third-Party Root Certification Aut							
Trusted People							
Other People							
Ams							
CanaryCertStore							
InjectorCertstore							
PolicyCertStore							
Remote Desktop							
Certificate Enrollment Requests							
Smart Card Trusted Roots							
▷ SMS							
SPC							
Finisted Devices							
۰	•	III			F.		
Personal store contains 2 certificates.							

## 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)

				PM
÷	•	ī	$\simeq$	÷
				Ы
Android_Sr	martphone.p12	<u>+</u>	≙	
Reply	Reply all		➡ Forward	

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

E	xtract certificate
Ei ci	nter the password to extract the ertificates.
	CANCEL OK

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.

⊟ ±		7 🛋 51	6:54	PI
-			$\simeq$	:
calo_ro	oot.crt	<u>+</u>	۵	
*	~		*	
Deplu	Reply all		Forward	

6:54 PM Tue, July 18	<b>\$</b> \to
🔶 🔍 🔹	⊗ 🛞
Wi-Fi Location Sound	Auto Bluetooth rotate
*•	Outdoors
calo_root.crt Download complete.	6:54 PM
NOTIFICATION SETTINGS	CLEAR
International Contents of	
the second se	
calo_root.crt	± 🛆
Reply Reply all Emergency calls	Forward only

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



Schritt 7: Wählen Sie Andere Sicherheitseinstellungen aus.

### 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.

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

#### 🖬 🛓

#### A 🗆 🖬 🛓

🕆 📶 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

#### Usage data access

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

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

Select file	DONE
e calo_root-1.crt	

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".

Select file	
C calo_root-1.crt	
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.

#### A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

#### 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

JII

Lloono data annon



Android\_Smartphone.david.com

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

#### A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

#### 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

JII

Lloono data annon

A = ± ± = ±	常 ⊿l 54% ≜ 7:45 PM						
← View security certificates							
SYSTEM	USER						
calo_root							

## 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.

								- 🗗 🔀
File View Tools Wizards Window Help							Type topic to search Go	alate
Home Configuration 🔯 Monitoring 🔲 Se	ave 💽 Refresh 🌘	Back O Forward	e de la composición de la composicinde la composición de la composición de la composición de la compos					cisco
Remote Access VPN	Configuration >	Remote Access VPN	> Network (Client)	Access > AnyConnect	Connection Profiles			
Production	The security app IPsec (IKEv2) tur Access Interfaces Enable Cisco SSL access must	iance automatically dep inel as well as SSL tunn AnyConnect VPN Client be enabled if you allow	loys the Cisco AnyCom el with Datagram Trans access on the interfac AnyConnect client to b	nect VPN Client to remote port Layer Security (DTLS es selected in the table b e launched from a brows	users upon connection. Th ) tunneling options. dow r (Web Launch) .	e initial client deployment requires end-user admin	istrative rights. The Cisco AnyConnect VPN Clie	nt supports
Group Policies		SSL Access		IPsec (IKEv2) Acces	s			
IPsec(IKEv2) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate		
George Mobility Solution     Address Assignment	outside					Port Settings		
Advanced	inside							
Cerfictaria     Cardination     Cardinati	Login Page Setting Allow user to Shutdown po Connection Profiles Connection profi	select connection profi rtal login page. le (tunnel group) specif dt m Delete	le on the login page. ( ies how user is authent	icated and other parame	ers. You can configure the	mapping from certificate to connection profile ( <u>her</u>	6	
	Name	SSL Ena	bled	IPsec Enabled	Alias	es Authentication Method	Group Policy	
	DefaultRAGroup	Group			V 7	AAA(LOCAL)	DittGroPolicy	
					¥	AAA(LOCAL)	DfltGrpPolicy	

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.

C Add Internal Group Policy	×
Add Internal Group Policy         Scheres         Banner:         Dhent         SCEP forwarding URL:         Di hent         SCEP forwarding URL:         Di hent         Divé Address Pools:         Di hent         IPv6 Address Pools:         Di hent         IPv6 Address Pools:         Di hent         IPv6 Address Pools:         Inhent         Clentess SSL VPN _ SSL VPN Clent         IPsec IKEv1         More Options         Turneling Protocols:         Inhent         Clentess SSL VPN _ SSL VPN Clent         IPsec IKEv1         Vinneling Protocols:         Inhent         Clentess SSL VPN _ SSL VPN Clent         IPsec IKEv1         Inhent         Clentess SSL VPN _ SSL VPN Clent         IPsec IKEv1         Inhent         Simultaneous Logins:         VInhent         Concetion Profile (Turnel Group) Lock:         VInhent         Nation Concert Time:         Inhent         Leinsted         Inhent         Concetion Profile (Turnel Group) Lock:         Vintent	
Maximum Connect Time:       I Inherit       Unlimited       minutes         Idle Timeout:       IV Inherit       None       minutes         Security Group Tag (SGT):       I Inherit       None       (2 - 65519)         On smart card removal:       I Inherit       Disconnect       Keep the connection         Periodic Certificate Authentication Interval:       Inherit       Unlimited       hours	
OK Cancel Help	

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.

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File View Tools Wizards Window Help			Type topic to search Go	alada
Home 🍪 Configuration 🔯 Monitoring 🔲 Sa	ave 🔇 Refresh 🔇 Back 🔘 Forward 🢡 Help			cisco
Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Ac	tess > Address Assignment > Address Pools		
Production     Production     Provent (Clent) Access     Provent Connection Profiles     Provent Connection Profiles     Provent Connect Constrainty AnyConnect Clent Profile     Provent Clent Software     Provent Software     ProventSoftware     Provent Software     P	Configure named IP Address Pools. The IP Address Pool dustering. Add - C Edt Delete Pool Name Starting A ACPool 192,160.5	I can be used in either a VPN (Psec(IKEv1) Connection Profiles, AnvConnect Connect Connect Connection Profiles, AnvConnect Con	ection Profiles, <u>Group Policies</u> configuration , or in <u>Interfaces</u> configuration Subnet Mask/Prefix Length 255-255-255-0	related to ASA
Secure Mobility Solution  Secure Mobility Solution  Address stagioment Policy  Address stagioment Policy  Contracts Pools  Contracts  Contracts Pools  Contracts  Co		Name: ACPool Starting IP Address: [92:168.50.1] Ending IP Address: [192:168.50.100 Subnet Mask: 255.255.0 • OK Cancel Help		
Device Management		Apply Reset		

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.

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File Niew Tools Wizards Window Help		T	ype topic to search	Go
Home Sconfiguration 🖗 Monitoring 🔜 Save 💽 Refresh	🔁 Back 🔘 Forward 🤣 Help			cisco
Remote Access VPN	note Access Connection Profile: David	×		
Introduction				
Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Localization     AnyConnect Client Profile	Name: David DE Peer Authentication			
AnyConnect Client Software	Preshared Key:			
Dynamic Access Policies	C Enable Certificate Authentication			
IPsec(IKEv 1) Connection Profiles      IPsec(IKEv 2) Connection Profiles	Enable peer authentication using EAP (If this is enabled, only Certificate is allowed for Local Authentication)			
- B Secure Mobility Solution	Send an EAP identity request to the dient			
Assignment Policy	IKE Local Authentication			
Address Pools     Advanced	C Enable local authentication			
AnyConnect Custom Attributes	Preshared Key:			
- ண일 AnyConnect Custom Attribute Nam - 타입 IPsec	Certificate: Headend:hostname=Connected_2_INET-B, cn=HeadEnd.da      Manage			
Crypto Maps	lear Authentization		Group Policy	
IKE Policies	Server Course	Magaza	DfltGrpPolicy	
DiPsec Proposals (Transform Set	Server group:	Manage	DfltGrpPolicy	
IPsec Prefragmentation Policies     Image: Image of the second seco	Falback: Use LOCAL if Server Group fails		GP_David	
Policy	Client Address Assignment			
Rules	DHCP Servers:			
A Operation String	None OHCP Link OHCP Subnet			
ACL Manager     Boundary     Clientless SSL VPN Access	Client Address Pools: ACPool	Select		
AAA/Local Users	Default Group Policy			
< III. •	Group Policy: GP_David	Manage		
A Device Setup	(Following field is an attribute of the group policy selected above.)			
🗊 Firewall				
Remote Access VPN Find:	Next Previous			
Site-to-Site VPN	OK Cancel Help			
Device Management			]	
» •	Apply Reset			

### 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.





#### 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**.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254					X
File View Tools Wizards Window Help				Type topic to search Go	ababa
Home 🖓 Configuration 🔯 Monitoring 🔲 Save	e 🔇 Refresh 🔇 Back 🔘 Forward  He	dp			cisco
Remote Access VPN	Configuration > Remote Access VPN > Networ	k (Client) Access > Advanced > IPsec > Certificate	to Connection Profile Maps > Rules		
Introduction     Introduction     AnyConnect Connection Profiles     AnyConnect Customzation, Acaization     AnyConnect Customzation, Acaization     AnyConnect Clear Profile     AnyConnect Clear Profile     Prace(TREV) I Connection Profiles     Proce(TREV) I Connection Profiles     Secure Mobility Solution     Secure Mobility Solution     Secure Mobility Solution	Define rules to map certificates to desired AnyConn Certificate to Connection Profile Maps	ect or clientiless SSL connection profiles (funnel groups). Us	e the bottom table to configure certificate fields tog Mapped to Connection Profile	ether with their matching criteria for the selected	rule.
Address Assignment Address Assignment Assignment Policy Address Pools  Any-Connect Custom Attributes Decerptore Address Decerptore Decerptore Address Decerptore Decer	Mapping Criteria  Add Certificate Matchin  Field  Field  Priority:  Mapped to Connection Pro	g Rule tring rule and associate it with a connection profile. The rul d assigns a priority to the rule with lower values having or Existing DefaultCertificateMap  New CERT_MAP  I0  OK Cencel Help  Antwo	le priority uniquely identifies the sater priority. Rules that are not		
*		white	Neset		

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

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254		2 23
File View Tools Wizards Window Help	Type topic to search Go	du
Home 🖓 Configuration 🔯 Monitoring 🔲 Sa	ve 🗞 Refresh 🖉 Back 🖉 Forward 🦻 Help CIS	co
Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules	
Remote Access VPI      Remote Access VPI      Introduction     Introduction     AnyConnect Conscitution Profiles     AnyConnect Conscitution Profiles     AnyConnect Conscitution Profiles     Prectificity Connection Profiles	Configuration > Remote Access VPI > Iletwork (Clent) Access > Advanced > IEsec > Certificate to Connection Profile Haps > Bules         Define rules to map certificates to desired AnyConnect or dendess SSL connection profiles (turnel groups). Use the bottom table to configure certificate fields together with their matching oriteria for the selected rule.         Certificate to Connection Profile Maps	
Prece Prefragmentation Policies     Certificate to Connection Policies     Vola Software     Vola	CK Cancel Help	
Site-to-Site VPN		
Device Management		
÷	Apply Reset	

### 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.

File View Tools Wizards Window Help						Type topic to search Go	
Home 🚱 Configuration 🔯 Monitoring 📳 Sa	we 🔇 Refresh 🔇 Back 🔘 Forwar	d 🢡 Help					CISCO
Firewall 🗗 🖓	Configuration > Firewall > Objects >	Network Objects/Grou	<u>ips</u>				
Access Rules	🗣 Add 🗸 🗹 Edit 📋 Delete 🛛 Q, Wr	nere Used 🔍 Not Used					
O Service Policy Rules	Filter						Filter Clear
AAA Rules	^1				-	20.000	r iter jeicer
Filter Rules	Name	IP Address	N	letmask	Description	Object NAT Address	
URL Eitering Servers	-Network Objects						
Threat Detection	- any						
	- Carly T						
Identity by TrustSec	- all inside-network	10.88.243.0	21	55.255.255.128			
Objects     Matwork Objects (Groups	METWORK OB1 192, 168, 50	. 192.158.50.0	2	55.255.255.0			
Service Objects/Groups	- a outside-network	192.168.0.0	2	55.255.255.0			
Local Users	224.0.0.251	224.0.0.251					
- A Local User Groups		224.0.0.252					
TCP Maps Time Ranges C fine Communications C Advanced		C Edit Network Name: Type: IP Version: IP Address: Netmask: Description:	rk Object NETWORK_083_1 Network @ IPv4 O IPv6 192.158.50.0 255.255.0	92.168.50.0_24	· ·		
A Device Setup			ОК	Cancel Help			
Firewall							
Remote Access VPN							
Site-to-Site VPN							
Device Management				Apply	iset		

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.

	Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254								
Fi	le View Tools Wizards Window Help							Type topic to search Go	de de
2	Home 🗞 Configuration 🔯 Monitoring 🗐 San	ve 🔇 Refresh 🔇 B	ack 😱 Forward 🢡 Help						cisco
	Firewall 🗗 🕀	Configuration > Firev	vall > NAT Rules					Addresses Services	
	Access Rules	🖶 Add 🗸 📝 Edit 1	C C C A MAT D . I.				)	Addresses	a t x
narks	NAT Rules		Calt NAT Rule					💠 Add 👻 🛒 Edit 🏢 Delete 🔍 Where U	Jsed 🔍 Not Used
look	AAA Rules	#	Match Criteria: Original Packet —				Options	Filter:	Filter Clear
	Filter Rules	Source Intf	Source Interface:	inside	<ul> <li>Destination Interface:</li> </ul>	outside 👻		Name	
	URL Filtering Servers	Network Object" N	Source Address:	any	Destination Address:	(_OBJ_192.168.50.0_24	No Proxy	-Network Objects	
	Threat Detection				Service:	any –		🏟 any	
								🧇 any4	
	E Objects		Action: Translated Packet	(a)				- 🍲 any6	
	Network Objects/Groups		Source NAT Type:	Static	•			NETWORK OBJ 192, 168, 50,0 24	
	Local Users		Source Address:	Original	Destination Address:	Original		outside-network/24	
	Local User Groups		Use one-to-one address transl	ation				- 3 224.0.0.251	
	Gass Maps		PAT Pool Translated Address:		Service:	Original			
	Inspect Maps     Regular Expressions		Round Robin						
	TCP Maps		Extend PAT uniqueness to p	er destination instead of per	interface				
	Time Ranges		Translate TCD and LDD parts	a late flat cases 1024 SEE2S		2			
	⊕ B Advanced		Translate TCP and CDP ports	s into hat range 1024-05555	Include range 1-102	2			
			Fall through to interface PAT						
			Use IPv6 for source interface P	PAT	Use IPv6 for desti	nation interface PAT			
			Options						
			Enable rule						
			Translate DNS replies that mat	ch this rule					
			Disable Proxy ARP on egress in	nterface					
	100100		Lookup route table to locate eg	gress interface					
	Device Setup		Direction: Both 👻						
	Frewall		Description:						
	Remote Access VPN			OK Cance	Help				
	Site-to-Site VPN						1		
	Device Management	•		m			Þ		
	ŝ			Apply	Reset				

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 \ {\tt 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**.

Control Panel	Network and Internet   Network and Sharing Center	← ← Search Control Panel	م
Control Panel Home	View your basic network information and s	et up connections	^ (§)
Manage wireless networks	🔍 ——— 🦫	See full map	
Change adapter settings	DRIVERAP-6KUZH cisco.com	Internet	
Change advanced sharing settings	(This computer) View your active networks	Connect or disconnect	
	cisco.com Domain network	Access type: Internet Connections: M Wireless Network Connection (blizzard)	E
	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.	
See also	📷 Connect to a network		
HomeGroup	Connect or reconnect to a wireless, wired, dial	-up, or VPN network connection.	
Internet Options Windows Firewall	Choose homegroup and sharing options Access files and printers located on other netw	vork computers, or change sharing settings.	-

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

🕎 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.	E
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.	-
Ne	xt Cane

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**.

		- • •
🚱 🌆 Connect to a Workplace		
Type the Internet addr	ess to connect to	
Your network administrator of	can give you this address.	
Internet address:	HeadEnd.david.com	
Destination name:	RA VPN to ASA with IKEv2	
<ul> <li>Use a smart card</li> <li>Image: Image: I</li></ul>	o use this connection yone with access to this computer to use this connection. ust set it up so I can connect later	
	Ne	t Cancel

Schritt 6: Wählen Sie Weiter aus.

🚱 🗽 Connect to a Workp	lace	
Type your user nar	me and password	
User name:	I	
Password:		
	Show characters Remember this password	
Domain (optional):		
		Create Cancel

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.

RA VPN to ASA with Disconnected	IKEv2		VirtualBox Host
🥂 🧊 WAN Miniport (IKEv2		Connect	
VMware Network Ad		Status	
Disabled VMware Virtual Ether		Set as Default Conn	ection
		Create Copy	
		Create Shortcut	
	۲	Delete	
	۲	Rename	
	0	Properties	

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.

📱 RA VPN	l to ASA v	vith IKEv.	2 Properties			×
General	Options	Security	Networking	Sharing		
Host nar 157.54.0	me or IP ad D.1 or 3ffe:	ldress of c 1234::111	destination (su 1):	ch as micro	osoft.com or	
HeadEr	nd.david.co	m				
- First co	onnect					_
Wind	lows can fi net, before	rst connec trying to e	ct to a public n establish this vi	ietwork, su irtual conne	ch as the ection.	
D	ial another	connectio	on first:		*	
See our informati	online <u>priv</u> on.	acy stater	nent for data c	ollection a	nd use	
				ОК	Cance	el

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**.

RA VPN to ASA with IKEv2 Properties
General Options Security Networking Sharing
Type of VPN:
IKEv2 ▼
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Ouse Extensible Authentication Protocol (EAP)
· · · · · · · · · · · · · · · · · · ·
Properties
Ose machine certificates
OK Cancel

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
# 38.25.63.10 x.acme.com
10.88.243.108 HeadEnd.david.com
```

```
# source server
# x client host
```

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.** 

RA VPN to ASA with IKEv2			VirtualBox Host-Only	
Disconnected WAN Miniport (IKEv2)		Connect		
VMware Network Adapter Disabled VMware Virtual Ethernet A		Status		
		Set as Default Connection		
		Create Copy		
		Create Shortcu	ut	
	۲	Delete		
	۲	Rename		
	0	Properties		

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

#### A 🖬 🗄 🗄 🖬 🛓

🕆 🗐 54% 🛢 7:45 PM

More connection settings

# Nearby device scanning

On

Printing

Download booster

#### VPN

Set up and manage Virtual Private Networks (VPNs).

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).



▲ 🖃	± ± 🗉 ± 🛛 🕺 🕺 🕺 🛱 ± 🕅 🕄 ± 🕅 ±
÷	RE Edit VPN network
6	Name RA VPN to ASA Headend with IK
l	Type
l	Server address
l	IPSec user certificate
l	Android ID Cert 🔻
l	calo_root-1 👻
l	IPSec server certificate Received from server v
I.	DELETE CANCEL SAVE

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



Schritt 5: Wählen Sie Verbinden aus.





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

![](_page_58_Picture_0.jpeg)

# 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
                                  Public IP : 10.152.206.175
Assigned IP : 192.168.50.1
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 : TPsec: : 24.2 Tunnel ID Local Addr : 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 Left(T): 28778 Seconds Rekey Int (T): 28800 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 Remote Status Tunnel-id Local Role READY RESPONDER 2119549341 10.88.243.108/4500 10.152.206.175/4500 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: Oxfffffff Oxfffffff

outbound esp sas:									
spi: 0x76131476 (1	98096191	.0)							
transform: esp-a	aes-256	esp-sh	a-hma	ac no co	ompre	ession			
in use settings	={RA, 7	unnel,	IKE	v2, }					
slot: 0, conn_i	d: 98304	, cryp	to-ma	ap: Anyo	conne	ect			
sa timing: rema	ining ke	ey life	time	(sec):	2876	7			
IV size: 16 byte	es								
replay detection	n suppor	rt: Y							
Anti replay bit	map:								
0x00000000 0x0	000001								
ASA#show vpn-sessiondb 1	icense-s	ummary							
VPN Licenses and Configu	red Limi	ts Sum	mary						
		S	tatu	s : Capa	acity	r : In	stalle	ed :	Limit
Jure Course at Decemium									
Anyconnect Premium		: EN.	ABLEI		50	:	5	0:	NONE
AnyConnect Essentials		: DIS.	ABLEI		50	:	1	0:	NONE
Other VPN (Available by )	Default)	: EN.	ABLEI		10	:	1	.0 :	NONE
Shared License Server		: DIS	ABLEI	D					
Shared License Participa	nt	: DIS	ABLEI	D					
AnyConnect for Mobile		: EN	ABLEI	D(Requi	res P	remiu	m or E	lsse	ntials)
Advanced Endpoint Assess	ment	: EN	ABLEI	D(Requi	res P	remiu	m)		
AnyConnect for Cisco VPN	Phone	: EN	ABLEI	D					
VPN-3DES-AES		: EN	ABLEI	D					
VPN-DES		: EN	ABLEI	D					
VPN Licenses Usage Summa:	ry								
	Local	: Shar	ed :	A11	:	Peak	: Eff	•	:
	In Use	: In U	se :	In Use	: In	u Use	: Lin	ιit	: 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									
	P	active	: Cur	mulative	e : P	Peak C	oncur	: I	nactive
AnyConnect Client		·		1	 1 .				
	•	0	:	. ⊥	⊥ ; 1 .		1	:	0
	•	0	•	-	1 : 0 :		1	•	0
IKEV2 IPSec	:	0	:	T (	•		1	:	0
Generic IKEV2 Remote Acc	ess : 	L 	:	14	4 : 		1 		
Total Active and Inactive	e :	1			Tota	l Cum	ulativ	re :	25
Device Total VPN Capacity	y :	50							
Device Load	:	2%							
Tunnels Summary									
<b></b>		ctive	: Cur	nulative	e : P	eak C	oncurr	ent	

IKEv2	:	1	:	<b>2</b> 5	:	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 <u>zu Debug-</u>Befehlen finden Sie<u>unter Wichtige Informationen</u>, 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