# ASA IKEv2 RA VPN con client VPN Windows 7 o Android e configurazione dell'autenticazione del certificato

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Panoramica Configura Autorità di certificazione Genera un certificato client Installare il certificato di identità sul computer client Windows 7 Come installare il certificato di identità sul dispositivo mobile Android Configurare l'headend ASA per la VPN ASA con IKEv2 Configura client predefinito di Windows 7 Configura client VPN nativo Android Verifica Risoluzione dei problemi

# Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) versione 9.7.1 e successive per consentire ai client VPN Windows 7 e Android nativi (Virtual Private Network) di stabilire una connessione VPN (Remote Access) per RA con l'utilizzo di IKEv2 (Internet Key Exchange Protocol) e certificati come metodo di autenticazione.

Contributo di David Rivera e Cesar Lopez Zamarripa, Cisco TAC Engineers.

# Prerequisiti

# Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CA (Certification Authority)
- PKI (Public Key Infrastructure)
- RSA VPN con IKEv2 su ASA
- Client VPN incorporato di Windows 7
- Client VPN nativo Android

# Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- CISCO 1921/K9 15.5(3)M4a come server CA IOS
- ASA5506X 9.7(1) come headend VPN
- Windows 7 come computer client
- Galaxy J5 Android 6.0.1 come client mobile

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

# Panoramica

Di seguito viene riportata la procedura per configurare i client VPN nativi di Windows 7 e Android per la connessione a un headend ASA:

# Configura Autorità di certificazione

L'autorità di certificazione consente di incorporare l'utilizzo chiavi avanzato (EKU) richiesto nel certificato. Per l'headend ASA, è necessario l'utilizzo chiavi avanzato di autenticazione server certificati, mentre per il certificato client è necessario l'utilizzo chiavi avanzato di autenticazione client.

Èpossibile utilizzare diversi server CA, ad esempio:

- Server CA Cisco IOS
- Server CA OpenSSL
- Server CA Microsoft
- 3<sup>rd</sup> CA parte

Per questo esempio di configurazione viene utilizzato IOS CA Server.

In questa sezione viene descritta la configurazione di base per far funzionare un CISCO 1921/K9 con versione 15.5(3)M4a come server CA.

Passaggio 1. Verificare che il dispositivo e la versione supportino il comando eku.

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

Passaggio 2. Abilitare il server HTTP sul router.

Passaggio 3. Generare una coppia di chiavi RSA esportabile.

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)
Passaggio 4. Configurare un trust point.

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>

**Nota:** L'indirizzo IP per il comando enrollment è uno degli indirizzi IP configurati dal router per un'interfaccia raggiungibile.

Passaggio 5. Autenticare il trust point (ottenere il certificato CA).

```
IOS-CA(config)#crypto pki authenticate <HeadEnd>
Certificate has the following attributes:
       Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
      Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Passaggio 6. Registrare il trust point (ottenere il certificato di identità).
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
Passaggio 7. Verificare i certificati.
```

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: 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
```

Passaggio 8. Esportare il trust point HeadEnd in un terminale in formato PKCS12 per ottenere il certificato di identità. Il certificato CA e la chiave privata vengono aggiunti in un unico file.

<cisco123>

Exported pkcs12 follows: MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/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/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs y155wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd12lHurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eg1sBLs1wPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfnlAbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX  ${\tt AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp}$ kuauRzQ8/pwszaZuPh/5rE77z8zMut3+OE5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB01peC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68aOyZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+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. Passaggio 9. Creare un trust point vuoto sull'appliance ASA.

ASA(config)# crypto ca trustpoint <HeadEnd> DRIVERAP(config-ca-trustpoint)# exit Passaggio 10. Importare il file PKCS12.

ASA(config)#crypto ca import <HeadEnd> pkcs12 <cisco123> Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself: MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH  ${\tt BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz}$ Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/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/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAilrYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd12lHurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt

xkJ0qaE645ihTnLqk4eqlsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NB1SbvCfn1AbisKrbbqCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/clNsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZSOSjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5Cs1B9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8qsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvqNAeakqr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHISA92pplS7VFrAWP65wrhs4X0f4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAgIEAA==

quit

INFO: Import PKCS12 operation completed successfully

Passaggio 11. Verificare le informazioni sul certificato.

```
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
```

### Genera un certificato client

Passaggio 1. Generare una coppia di chiavi RSA esportabile.

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
Passaggio 2. Configurare un trust point.

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>
Passaggio 3. Autenticare il trust point configurato (ottenere il certificato CA).

IOS-CA(config)#crypto pki authenticate <Win7\_PC>
Certificate has the following attributes:
 Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
 Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Passaggio 4. Registrare il trust point autenticato (ottenere il certificato di identità).

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 Passaggio 5. Verificare le informazioni relative ai certificati.

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

# Installare il certificato di identità sul computer client Windows 7

Passaggio 1. Esportare il trust point Win7\_PC denominato in un server FTP/TFTP (installato nel computer Windows 7) in formato PKCS12 (.p12) per ottenere il certificato di identità, il certificato CA e la chiave privata in un unico file.

IOS-CA(config)#crypto pki export <Win7\_PC> pkcs12 <tftp://10.152.206.175/ Win7\_PC.pl2> password
<ciscol23>
Address or name of remote host [10.152.206.175]?
Destination filename [Win7\_PC.pl2]?
!Writing pkcs12 file to tftp://10.152.206.175/Win7\_PC.pl2
!
CRYPTO\_PKI: Exported PKCS12 file successfully.

\*Jul 17 16:29:20.310: %PKI-6-PKCS12EXPORT\_SUCCESS: PKCS #12 Successfully Exported.

Questo è l'aspetto del file esportato su un computer client.

						E	- 0	×
Search Re	esults in TFTP-Root 🕨				▼ 4 Win7_PC			×
Organize 🔻 Save sear	ch						-	0
★ Favorites ₩ Recent Places ■ Desktop	Win7_PC C:\TFTP-Root			Type: Personal Information Exch	Date modified: <b>7/13/2017 9:01</b> Size: <b>2.97 KB</b>	AM		
〕 Downloads	Search again in: 😭 Libraries 🛛 👰 Computer	F Custom 🏮	Internet	File Contents				
<ul> <li>➢ Libraries</li> <li>➢ Documents</li> <li>ℳ Music</li> <li>➢ Pictures</li> <li>☑ Videos</li> <li>I Computer</li> <li>➢ os (C;)</li> <li>Network</li> </ul>								
↓ 1 item								

Passaggio 2. Premere Ctrl + R e digitare mmc per aprire Microsoft Management Console (MMC).



Passaggio 3. Selezionare OK.

Console1 - [Console Root]			
File Action View Favorites Wind	dow Help		_ & ×
Console Root	Name		Actions
		There are no items to show in this view.	Console Root

Passaggio 4. Passare a File>Aggiungi/Rimuovi snap-in.

🚡 Console1 - [Console Root]	
🜇 File Action View Favorites Window Help	_ 8 ×
Console Root Add or Remove Snap-ins	
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.	Root
Available snap-ins: Selected snap-ins: More	e Actions
Snap-in Vendor ^ Console Root Edit Extensions	
ActiveX Control Microsoft Cor      Remove      Remove	
Gertificates Microsoft Cor =	
Compare Services Microsoft Cor	
Add >	
Moragement Microsoft and	
Contraction Microsoft Contraction	
Group Policy Object Microsoft Cor	
Sub-Security Monitor Microsoft Cor	
Link to Web Address Microsoft Cor Advanced	
Description:	
The ActiveX Control snap-in enables you to add an MMC node with a results view containing an ActiveX control.	
OK Cancel	

Passaggio 5. Selezionare Certificati > Aggiungi > Account computer.

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       Selected snap-ins:       This snap-in will always manage certificates for:         Device Manager       Microsoft Cor       Add >       Computer Microsoft Cor       Or power anagement         Disk Managerent       Microsoft Cor       Add >       Computer Account       Computer account         Disk Managerent       Microsoft Cor       Add >       Computer account       Computer account         Disk Managerent       Microsoft Cor       Add >       Computer account       Computer account         Disk Managerent       Microsoft Cor       Add >       Computer account       Computer account         Disk Managerent       Microsoft Cor       Core policy Object       Microsoft Cor       Computer account         Unit to Web Address       Microsoft Cor       Core policy Object       Microsoft Cor       Core count         Description:       The Certificates snap-in allows you to browse the contents of the	Next > Cancel

Passaggio 6. Selezionare Avanti,

🚡 Console1 - [Console Root]	
File Action View Favorites Window Help	
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 to extensible snap-ins; you can configure which extensions are enabled.       Available snap-ins:       Stap-in:       Stap-in:	the select divide for the formula in the select Computer source is a server of the computer the select of the computer this console is running on)  Another computer:  Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.  self, a server the select of the computer to be changed when launching from the command line. This only applies if you save the console.
	OK Cancel

Passaggio 7. Fine.

Console1 - [Console Root]							
🚡 File Action View Favorites Wir	ndow Help						- 8 ×
Consels Baset	1	1					
Console Root	Name					Actions	
	Add or Remove Snap-ins				×	Console Root	<b>^</b>
	Add or Kemove Shap-ins You can select snap-ins for t extensible snap-ins; you can Available snap-ins; Snap-in ActiveX Control Authorization Manager Certificates Computer Manager Device Manager	Vendor  Microsoft Cor	available on your sions are enabled St Add >	computer and configure the selected : 	Edit Extensions         Remove         Move Up         Move Down	More Actions	,
	The Certificates span-in allo	ws you to browse the o	contents of the o	ertificate stores for yourself, a service	, or a computer.		
	the Ceruncates shap-in all	ms you to browse the c	uniterits or the o	e uncave stores for yoursen, à service	OK Cancel		

Passaggio 8. Selezionare OK.

Passaggio 9. Accedere a **Certificati (computer locale)>Personali>Certificati**, fare clic con il pulsante destro del mouse sulla cartella e selezionare **Tutte le attività>Importa**:

	C	BC IC -						
The console - (console Root) - (console Root) - (console - (console - (console Root)) - (console Root) - (co								
	и пер							
		•			1			
Console Root	ssued To	<u>^</u>	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
A Personal	DRIVERAP-6	UZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	-
Certificates							More Actions	•
Trusted Ro All Tasks	+	Request New	Certificate					
▷ Contemprise View	•	Import						
Intermedia     Trusted Pu     New Window from	Here	Advanced Op	erations +					
Untrusted      New Taskpad View     Third-Party								
Trusted Per Refresh								
Other Peop Export List								
CanaryCert Help								
InjectorCertStore		1						
Cafee Trust								
Poincycenstore     Pencycenstore     Pencycenstore								
Certificate Enrollment Requests								
Smart Card Trusted Roots								
b SMS								
Trusted Devices								
	(							
Add a certificate to a store						r		

# 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

Passaggio 10. Fare clic su Avanti. Indicare il percorso in cui è archiviato il file PKCS12.

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 format	s:			
Personal Information Exchange- PKCS #12 (.PFX,.P12)				
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)				
Microsoft Serialized Certificate Store (SST)				
Microsoft Senalized Certificate Store (.SST)				
Learn more about <u>certificate file formats</u>				
< Back Next > C	ancel			

Passaggio 11. Selezionare nuovamente **Avanti** e digitare la password immessa nel comando *crypto pki export <Win7\_PC> pkcs12 <tftp://10.152.206.175/ Win7\_PC.p12> password <cisco123>* 

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

Passaggio 12. Selezionare Avanti.

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

Passaggio 13. Selezionare ancora una volta Next.



Passaggio 14. Selezionare Fine.

Certificate Import Wizard
The import was successful.
ОК

Passaggio 15. Selezionare **OK**. Verranno ora visualizzati i certificati installati (sia il certificato CA che il certificato di identità).

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							
File Action View Favorites Wind	ow Help						_ & ×
Console Root     Certificates (Local Computer)     Personal     Certificates (Local Computer)     Personal     Certificates     Certificates     Trusted Root Certification Author     Enterprise Trust     D     Trusted Publishers     Untrusted Certificates     Trusted Publishers     Other People     Ams     CanaryCertStore     InjectorCertStore     McAfee Trust     PolicyCertStore     Remote Desktop     Certificate Enrollment Requests     Smart Card Trusted Roots     SMS     SPC     Trusted Devices	Issued To	Issued By 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=calo_ro <none> cn=Win7_P</none>	Actions Certificates More Actions	•
	< [	m			*		
Personal store contains 3 certificates.						J	

Passaggio 16. Trascinare e rilasciare il certificato CA da Certificati (Computer locale)>Personali>Certificati a Certificati (Computer locale)>Autorità di certificazione principale attendibile>Certificati.

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]							
🚡 File Action View Favorites Wind	ow Help						- 8 ×
🗢 🏟 🖄 🔚 🔏 🛸  😹	? 🗊						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly ^	Actions	
Certificates (Local Computer)     Personal	AddTrust External CA Root	AddTrust External CA Root Baltimore CyberTrust Root	5/30/2020 5/12/2025	Server Authenticati Server Authenticati	The USE DigiCert	Certificates More Actions	<u> </u>
<ul> <li>Certificates</li> <li>Trusted Root Certification Author</li> <li>Certificates</li> </ul>	Certum CA	calo_root Certum CA	7/12/2020 6/11/2027	<all> Server Authenticati</all>	cn=calo Certum	calo_root	- -
<ul> <li>Enterprise Trust</li> <li>Intermediate Certification Author</li> </ul>	Certum Trusted Network CA	Certum Trusted Network CA Cisco Root CA 2048	12/31/2029 5/14/2029	Server Authenticati <all></all>	Certum ≡ <none></none>	More Actions	•
Trusted Publishers     Gimen Untrusted Certificates     Gimen Third-Party Root Certification Aud	Cisco Root CA MI	Cisco Root CA MI Cisco Root CA MI Cisco Root CA M2	11/18/2033 11/18/2033 11/12/2037	<all> <all></all></all>	<none> <none></none></none>		
Trusted People     Other People	Cisco RXC-R2	Cisco RXC-R2 Class 3 Public Primary Certificatio	7/9/2034 8/1/2028	<all> Secure Email, Client</all>	<none> VeriSign</none>		
Ams     GanaryCertStore	COMODO RSA Certification Au	COMODO RSA Certification Auth Copyright (c) 1997 Microsoft Corp.	1/18/2038 12/30/1999	Server Authenticati Time Stamping	COMOE Microso		
InjectorCertStore     McAfee Trust     PolicyCertStore	Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA	Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA	7/9/2019 11/9/2031	Secure Email, Serve Server Authenticati	Deutsch DigiCert DigiCert		
Gentificate Enrollment Requests	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root DRIVERAP-6KUZH	11/9/2031 11/9/2031 7/13/2022	Server Authenticati <all></all>	DigiCert <none></none>		
Smart Card Trusted Roots     SMS     SMC	DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com DST Root CA X3	1/12/2021 9/30/2021	<all> <all></all></all>	<none> <none></none></none>		
<ul> <li>SPC</li> <li>Trusted Devices</li> </ul>	DST Root CA X3	DST Root CA X3 Entrust Root Certification Authority	9/30/2021 11/27/2026	<all> Server Authenticati</all>	<none> Entrust</none>		
	Entrust Root Certification Auth	Entrust Root Certification Authori Entrust.net Certification Authority	12/7/2030 7/24/2029	Server Authenticati Server Authenticati	Entrust I		
•	Californita Secure Certificate Auth	III	*/////18	Servire Email Serve	1 A		
Trusted Root Certification Authorities store co	ntains 60 certificates.						

🚡 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							
🚡 File Action View Favorites Window Help							
🗢 🤿 🖄 🔂 📋 🙆 🔂 🖬							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
Certificates (Local Computer)	2 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	<b>^</b>
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 Intermediate Certification Author							
Trusted Publishers							
Untrusted Certificates							
Third-Party Root Certification Aut							
Trusted People							
Ams							
CanaryCertStore							
InjectorCertStore							
McAfee Trust							
PolicyCertStore							
Certificate Enrollment Requests							
Smart Card Trusted Roots							
SMS							
▷ C							
Trusted Devices							
<	•				۶.		
Personal store contains 2 certificates.							

# Come installare il certificato di identità sul dispositivo mobile Android

Nota: Android supporta i file dell'archivio chiavi PKCS#12 con estensione .pfx o .p12.

Nota: Android supporta solo certificati SSL X.509 con codifica DER.

Passaggio 1. Dopo l'esportazione del certificato client dal server CA IOS in formato PKCS12 (.p12), inviare il file al dispositivo Android tramite posta elettronica. Una volta ottenuto, toccare il nome del file per avviare l'installazione automatica. (**Non scaricare il file**)

⊡ B ±		7	<b>.d</b> 535	68 7:24	PM
÷		•		$\simeq$	÷
					.
					F.
			-	-	. 1
Andro	oid_Smartpho	one.p12	*	0	
*	<			+	
Reply	Reply	y all		Forward	

Passaggio 2. Immettere la password utilizzata per esportare il certificato. In questo esempio, la password è **cisco123**.

Extract certificate
Enter the password to extract the certificates.
CANCEL OK

Passaggio 3. Selezionare **OK** e immettere un **nome di certificato**. Può essere qualsiasi parola, in questo esempio il nome è **Android ID Cert**.



Passaggio 4. Selezionare OK e viene visualizzato il messaggio "Android ID Cert installed".

Passaggio 5. Per installare il certificato CA, estrarlo dal server CA IOS in formato base64 e salvarlo con estensione .crt. Inviare il file al dispositivo Android tramite e-mail. Questa volta è necessario scaricare il file incollandolo sulla freccia situata accanto al nome del file.

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

6:54 PM Tue, July 18	♦ ∨
🔶 🔍 🔹	⊗ 🛞
Wi-Fi Location Sound	Auto Bluetooth rotate
*•	Outdoors
calo_root.crt Download complete.	6:54 PM
NOTIFICATION SETTINGS	CLEAR
second second	
and the second se	
calo_root.crt	* \
Reply Reply all Emergency calls	Forward only

Passaggio 6. Passare a Impostazioni e schermata di blocco e protezione.



Passaggio 7. Selezionare Altre impostazioni di protezione.

#### 7 🛋 50% 🛢 6:57 PM

#### Lock screen and security

# Notifications on lock screen

Show content

#### Secure lock settings

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

Security

#### Find My Mobile

Locate and control your device remotely using your Samsung account.

#### Unknown sources

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

#### Encrypt device

Protect your device by encrypting its data.

#### Encrypt SD card No SD card inserted

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

#### Passaggio 8. Passare a Installa dallo storage del dispositivo.

#### 🖬 ±

#### 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.

Passaggio 9. Selezionare il file .crt e toccare Fatto.

Select file		DONE
•	calo_root-1.crt	

Passaggio 10. Immettere un **nome certificato**. Può essere una parola qualsiasi, in questo esempio il nome è **calo\_root-1**.



Passaggio 10. Selezionare OK per visualizzare il messaggio "calo\_root-1 installato".

Select file	
C calo_root-1.crt	
calo_root-1 installed.	

Passaggio 11. Per verificare che il certificato di identità sia installato, passare a Impostazioni/schermata di blocco e Protezione/Altro > Impostazioni protezione/Certificati utente/Scheda Sistema.

## 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

Passaggio 12. Per verificare che il certificato CA sia installato, passare a **Impostazioni/schermata** di blocco e protezione/Altre impostazioni di protezione/Visualizza certificati di protezione/scheda Utente.

## 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 🗆 ± ± 🖾 ±	\$° ⊿l 54% ≘ 7:45 PM					
← View security certificates						
SYSTEM	USER					
calo_root						

# Configurare l'headend ASA per la VPN ASA con IKEv2

Passaggio 1. In ASDM, selezionare Configurazione>VPN ad accesso remoto > Accesso di rete (client)> Profili di connessione Anyconnect. Selezionare la casella Accesso IPSec (IKEv2), Consenti accesso sull'interfaccia rivolta ai client VPN (l'opzione Abilita servizi client non è necessaria).

Passaggio 2. Selezionare **Device Certificate** e rimuovere il segno di spunta da **Use the same device certificate for SSL and IPSec IKEv2**.

Passaggio 3. Selezionare il certificato headend per la connessione IPSec e scegliere Nessuno per la connessione SSL.

Questa opzione attiva la configurazione della mappa crittografica, ikev2, ipsec di crittografia, mappa dinamica e mappa crittografica.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254								- <b>-</b> X
File View Tools Wizards Window Help							Type topic to search G	° alatha
Home Configuration 😥 Monitoring 🔲 Sa	ave 🔇 Refresh 🕻	Back O Forward	1 🦓 Help					cisco
Remote Access VPN 🗗 🖗	Configuration >	Remote Access VPN	> Network (Client)	Access > AnyConnect	Connection Profiles			
Production     P	The security appl IPsec (IKEv2) tur Access Interfaces Enable Cisco SSL access must	ance automatically dep nel as well as SSL tunn AnyConnect VPN Client be enabled if you allow	loys the Cisco AnyCon el with Datagram Trans access on the interfac AnyConnect client to b	nnect VPN Client to remote sport Layer Security (DTLS ces selected in the table b be launched from a brows	users upon connection. ) tunneling options. Now r (Web Launch) .	The initial client deployment requires end-user admi	istrative rights. The Cisco AnyConnect VPN	Client supports
Group Policies		SSL Access		IPsec (IKEv2) Acces	s			
IPsec(IKEv2) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Service	es Device Certificate		
George Mobility Solution     Address Assignment	outside			2		Port Settings		
Advanced	inside							
Erefficate Management     Graduate Management	Login Page Setting Allow user to Shutdown po Connection Profiles Connection profi	select connection profil rtal login page. le (tunnel group) specifi dit <u>Delete</u> Find:	le on the login page. Nes how user is authen	ticated and other parame     So So Match Case	ers. You can configure t	he mapping from certificate to connection profile <u>the</u>	٤	
	Name	SSL Ena	bled	IPsec Enabled	Ali	ases Authentication Metho	d Group Policy	
	DefaultWEBVPN	Group			V V	AAA(LOCAL)	DfltGrpPolicy	
Device Setup						Specify Device Certificate Device certificate is a digital certificate that ide Use the same device certificate for SSL an	ntifies this ASA to the clients. d IPsec IKEv2	

Questo è l'aspetto della configurazione sull'interfaccia della riga di comando (CLI).

crypto ikev2 policy 1 encryption aes-256 integrity sha group 5 prf sha lifetime seconds 86400 crypto ikev2 enable outside crypto ikev2 remote-access trustpoint HeadEnd crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5 crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256 crypto map outside\_map 65535 ipsec-isakmp dynamic Anyconnect crypto map outside\_map interface outside

Passaggio 4. Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo per creare un criterio di gruppo

Fautra in ar		- / <b>/ 1</b>	
Add Internal Group Policy			
General	Name: GP_David		
⊕ Advanced	Banner: 👽 Inherit		
	SCEP forwarding LIBL : I Inherit		
			Colum
	Address Pools: V Inhent		Select
	IPv6 Address Pools: V Inherit		Select
	More Options		\$
	Tunneling Protocols:	inherit Clientiess SSL VPN SSL VPN Client IPsec IKEv1 V IPsec IKEv2 LZTP/IPsec	
	Filter:	☑ Inherit	Manage
	Access Hours:	✓ Inherit	Manage
	Simultaneous Logins:	✓ Inherit	
	Restrict access to VLAN:	🖉 Inherit 🗸 🗸	
	Connection Profile (Tunnel Group) Lock:	✓ Inherit	
	Maximum Connect Time:	Inherit Unlimited minutes	
	Idle Timeout:	Inherit None minutes	
	Security Group Tag (SCT):		
	Security group ray (501).		
	On smart card removal:		
	Periodic Certificate Authentication Interva	I: V Inherit Unimited hours	
Find:	Next Previou	S	
		OK Cancel Help	

Dalla CLI.

group-policy GP\_David internal
group-policy GP\_David attributes
vpn-tunnel-protocol ikev2

Passaggio 5. Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Pool di indirizzi e selezionare Aggiungi per creare un pool IPv4.

[5] Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File View Tools Wizards Window Help			Type topic to search Go	ahaha
Home 🗞 Configuration 🔯 Monitoring 🔚 Sav	ive 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help			CISCO
Remote Access VPN 🗗 🖗	Configuration > Remote Access VPN > Network (Client) Access :	> Address Assignment > Address Pools		
Predaction     Predactin     Predaction     Predaction     Predaction     Predaction     Pr	Configure named IP Address Pools. The IP Address Pools can dustering. Add - Cat Delete Pool Name Starting Address Acrool 192.169.50.1	be used in either a VPN [Psec[NEV1] Connection Profiles, AnyConnect Connection : Ending Address;Number of Addresses 192.168.50.100   [Edit [Pv4 Pool	sn Profiles, Group Policies configuration , or in Interfaces configuration	related to ASA
×		Apply Reset		

ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0

Passaggio 6. Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione IPSec(IKEv2) e selezionare Aggiungi per creare un nuovo gruppo di tunnel.





```
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
```

Passaggio 7. Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Mappe del profilo certificato-connessione > Criteri e selezionare la casella Utilizza le regole configurate per associare un certificato a un profilo di connessione.





tunnel-group-map enable rules

Passaggio 8. Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Mappe profilo certificato-connessione > Regole e creare una nuova mappa certificati. Selezionare Aggiungi e associarla al gruppo di tunnel. Nell'esempio, il gruppo di tunnel è David.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254					- <b>-</b> X
File View Tools Wizards Window Help				Type topic to search Go	adradu
Home 🍇 Configuration 🔯 Monitoring 🛄 Save 🔇	Refresh 🔇 Back 🔘 Forward 🢡 Help				cisco
Remote Access VPN 🗗 🗜 Confid	iguration > Remote Access VPN > Network (C	lient) Access > Advanced > IPsec > Certificate to Co	onnection Profile Maps > Rules		
Introduction     Introduction     AnyConnect Connection Profiles     AnyConnect Connection Profiles     AnyConnect Contenziation(acaization     AnyConnect Client Profiles     AnyConnect Client Profiles     AnyConnect Client Profiles     Prese(TREV1) Connection Prof	fine rules to map certificates to desired AnyConnect o ficate to Connection Profile Maps	r dentiess SSL connection profiles (tunnel groups). Use the I	bottom table to configure certificate fields togethe Mapped to Connection Profile	r with their matching oriteria for the selected r	ule.
Address Assignment Mappin	ing Criteria				
Address Pools      Advanced      AnyConnect Custom Attributes      Field	Add Edit Add Certificate Matching Ru	ale g rule and associate it with a connection profile. The rule prio	rity uniquely identifies the Value		
□ AryConnect Custom Attribute Nam	certificate matching rule and as mapped will be ignored.	signs a priority to the rule with lower values having greater p	priority. Rules that are not		
- IHG Crypto Maps → IKE Policies = WE Parameters → ↓ IKE Parameters → ↓ ISec Proposals (Transform Set	Map:	Existing         DefaultCertificateMap +           Image: New         CERT_MAP			
Piece Pretragmentation Policies	Priority: Mapped to Connection Profile:	10 David • •			
ergr Upload Software → 2• Zone Labs Integrity Server gs] System Options gs] C. Manager		OK Cancel Help			
AAALocal Users					
Device Setup					
Remote Access VPN					
Site-to-Site VPN					
Device Management		Andy	Parat		
» *		Appry	Neaet		

Dalla CLI.

tunnel-group-map CERT\_MAP 10 David

Passaggio 9. Selezionare Aggiungi nella sezione Criteri di mapping e immettere questi valori.

### Campo: Emittente

Operatore: Contiene

Valore: calo\_radice

Cisco 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	ave 💽 Refresh 🚫 Back 🔘 Forward 🤌 Help CIS	co
Remote Access VPN	Configuration > Remote Access VPR > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules	
Remote Access VPH   Remote Access VPH   Remote Access VPH   Remote Access VPH   Remote Access VPH  Remote Accest Remote Access VPH  Remote Acce	Vertifiest       Vertifiest <td></td>	
Conc Labs Integrity Server     Conc Labs Integrity Server     Conc Labs Integrity Server     Conc Labs Integrity Server     Concentses SSU NPI Access     Concentses SU NPI Access     Concentses SUPI     Concentses	OK Cancel Hep	
» *	Apply Reset	

# Dalla CLI.

crypto ca certificate map CERT\_MAP 10 issuer-name co calo\_root

Passaggio 10. Creare un oggetto con la rete del pool IP da utilizzare per aggiungere una regola di esenzione NAT (Network Address Translation) in **Configurazione > Firewall > Oggetti > Oggetti/gruppi di rete> Aggiungi**.

Gisco A M 7.8(1)150 for ASA - 192.168.0.254 File View Tools Wizards Window Help						Type topic to searc	h Go	
Home 🖓 Configuration 🔯 Monitoring 🎧 Sa	ave 💽 Refresh 🚺 Back 🔘 Fo	orward						CISCO
Firewall 🗇 🖗	Configuration > Firewall > Obje	cts > Network Objects/Grou	<u>ps</u>					
Access Rules	🗣 Add 👻 🗹 Edit 📋 Delete 🛛 C	🖁 Where Used 🔍 Not Used						Eiter Clear
AAA Rules	^ 1	1 221	1					Filter [Clear]
Filter Rules	Name	IP Address	Netmask		Description	C	bject NAT Address	
Public Servers     Public S	<ul> <li>Network Objects</li> <li> <ul> <li></li></ul></li></ul>	10.88.243.0 50 192.155.50.0 192.168.0.0 224.0.0.251 224.0.0.252 ГСП Есії Networ Name: Туре: IP Version: IP Address: Netmask: Description: NAT	255.255.25 255.255.25 255.255.25 255.255.	5.128 5.0 .0_24 Zancel Help				
Remote Access VPN           Image: Site-to-Site VPN								
Device Management				Apply	set			

# Dalla CLI.

object network NETWORK\_OBJ\_192.168.50.0\_24 subnet 192.168.50.0 255.255.255.0

Passaggio 11. Passare a **Configurazione > Firewall > Regole NAT** e selezionare **Aggiungi** per creare la regola di esenzione NAT per il traffico VPN RA.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254							- # X
File View Tools Wizards Window Help						Type topic to search Go	de de
Home 🦓 Configuration 🔯 Monitoring 🔚 Save 🔇 Refin	resh 🔇 Back 😱 Forward 🦻 Help						cisco
Firewall 🗗 🖗 Configural	tion > Firewall > NAT Rules					Addresses Services	
Access Rules 💠 Add 🗸	Edit Edit NAT Rule			<b>—</b>		Addresses	Β₽×
E Q Service Policy Rules Mat	tch Criteri					💠 Add 👻 🎬 Edit 🏢 Delete 🔍 Where U	sed 🔍 Not Used
AAA Rules #	Match Criteria: Original Packet	[]		[]	Options	Filter:	Filter Clear
Filter Rules	Source Interface:	inside •	Destination Interface:	outside •	No Proxy	Name	
URL Filtering Servers "Networ	rk Object" N	any -	Destination Address:	COBJ_192.168.50.0_24		-Network Objects	
Threat Detection			Service:	any –			
	Action: Translated Packet					- any4	
Objects     Network Objects/Groups	Source NAT Type:	Static				inside-network/25	
Service Objects/Groups	Source Address:	Original	Destination Address:	Original		NETWORK_OBJ_192.168.50.0_24	
Local Users						- M outside-network/24	
Security Group Object Groups	Se one-to-one address transle	IDON					
Class Maps	PAT Pool Translated Address:		Service:	Original			
Regular Expressions	Round Robin						
TCP Maps	Extend PAT uniqueness to pe	er destination instead of per int	erface				
(intercarges     (intercarges     (intercarges	Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-102	3			
Advanced	Fall through to interface PAT						
	Use IPv6 for source interface P	AT	Use IPv6 for destin	nation interface PAT			
	Options						
	C Enable rule						
	Translate DNS replies that mate	ch this rule					
	Disable Proxy ARP on egress in	terface					
	Cookup route table to locate eg	ress interface					
Device Setup	Direction: Both 🗸						
	Description:						
Con Description Access (JDN)		OK Cancel	Help				
CENDLE ALLESS YFIT		Cancer	( nop				
Site-to-Site VPN	·						
Device Management					,		
30 *		Apply	et				

Dalla 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 Questa è la configurazione ASA completa utilizzata per l'esempio.

```
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
```

# Configura client predefinito di Windows 7

Passaggio 1. Passare a **Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione**.

Control Panel	Network and Internet   Network and Sharing Center	← 4 Search Control Panel	٩
Control Panel Home	View your basic network information and s	set 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: #!!! 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	I-up, or VPN network connection.	
Internet Options	Choose homegroup and sharing options		
Windows Firewall	Access files and printers located on other network	vork computers, or change sharing settings.	-

Passaggio 2. Selezionare Configura nuova connessione o rete.

🖉 👰 Set Up a Connection or Network	
Choose a connection option	
<ul> <li>Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.</li> <li>Set up a new network Configure a new router or access point.</li> <li>Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.</li> <li>Connect to a workplace Set up a dial-up or VPN connection to your workplace.</li> <li>Set up a dial-up connection Connect to the Internet using a dial-up connection.</li> </ul>	
	Next Cancel

Passaggio 3. Selezionare Connetti a una rete aziendale e Avanti.



Passaggio 4. Selezionare No, crea una nuova connessione e Avanti.

📀 🔚 Connect to a Workplace	
How do you want to connect?	
Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.	
ing	
Dial directly Connect directly to a phone number without going through the Internet.	
What is a VPN connection?	
	Cancel

Passaggio 5. Selezionare **Use my Internet connection (VPN)** e aggiungere la stringa CN (Nome comune del certificato HeadEnd) nel campo **Indirizzo Internet**. Nel campo **Nome destinazione** digitare il nome della connessione. Può essere una stringa qualsiasi. Assicurarsi di controllare la casella di controllo **Non connettere ora; configuralo in modo da potermi collegare in seguito**.

		- • •
📀 🗽 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>Callow other people to This option allows an</li> <li>Don't connect now; j</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

Passaggio 6. Selezionare Avanti.

📀 🗽 Connect to a Workpl	ace	
Type your user nar	ne and password	
User name:	1	
Password:		
	Show characters	
Domain (optional):		
		Create Cancel

Passaggio 7. Selezionare Crea.



Passaggio 8. Selezionare **Chiudi** e selezionare **Pannello di controllo > Rete e Internet > Connessioni di rete**. Selezionare la connessione di rete creata e fare clic su di essa con il pulsante destro del mouse. Selezionare **Proprietà**.

RA VPN to ASA v Disconnected	vith IKEv2		VirtualBox Host
🧾 🥑 WAN Miniport (I	KEv2	Connect	
VMware Network	k Ad	Status	
Disabled VMware Virtual Ether	ther	Set as Default Conne	ection
		Create Copy	
		Create Shortcut	
	۲	Delete	
	۲	Rename	
	۲	Properties	

Passaggio 9. Nella scheda **General** è possibile verificare che il nome host appropriato per l'headend sia corretto. Il computer risolverà questo nome nell'indirizzo IP ASA usato per connettere gli utenti della VPN dell'appliance ASA.

📱 RA VPI	V to ASA	with IKEv.	2 Properties			x
General	Options	Security	Networking	Sharing		
Host na 157.54.	me or IP a 0.1 or 3ffe	ddress of a :1234::111	destination (su 1):	ch as micro	osoft.com o	r
HeadE	nd.david.c	om				
- First c	onnect					
Wind	dows can f net, before	irst conne trying to e	ct to a public r establish this vi	ietwork, su irtual conn	uch as the ection.	
	)ial anothe	r connectio	on first:		-	
See our informat	online <u>priv</u> ion.	vacy stater	<u>ment</u> for data o	collection a	nd use	
				ОК	Can	cel

Passaggio 10. Passare alla scheda **Sicurezza** e selezionare **IKEv2** come **tipo di VPN**. Nella sezione **Autenticazione** selezionare **Usa certificati computer**.

RA VPN to ASA with IKEv2 Properties	×
General Options Security Networking Si	haring
Type of VPN:	
IKEv2	•
Data encryption:	Advanced settings
Require encryption (disconnect if server decl	ines) 🔻
Authentication	
O Use Extensible Authentication Protocol (I	EAP)
	~
·	Properties
llas machine certificates	
Ose machine certificates	
0	K Cancel

Passaggio 11. Selezionare **OK** e passare a **C:\Windows\System32\drivers\etc**. Aprire il file **hosts** utilizzando un editor di testo. Configurare una voce per risolvere l'FQDN (Fully Qualified Domain Name) configurato nella connessione di rete sull'indirizzo IP dell'headend ASA (nell'esempio, l'interfaccia esterna).

```
# 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

Passaggio 12. Tornare a **Pannello di controllo > Rete e Internet > Connessioni di rete**. Selezionare la connessione di rete creata. Fare clic con il pulsante destro del mouse e selezionare **Connetti.** 

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				

Passaggio 13. Lo stato della connessione di rete passa da Disconnesso a Connesso e quindi a Connesso. Viene infine visualizzato il nome specificato per la connessione di rete.



A questo punto, il computer è connesso all'headend VPN.

# Configura client VPN nativo Android

Passaggio 1. Passare a Impostazioni>Altre impostazioni di connessione



Passaggio 2. Selezionare VPN

#### A 🖬 🗄 🗖 🖬 🛓

🕆 🛣 🖬 54% 🖹 7:45 PN

More connection settings

# Nearby device scanning

On

Printing

Download booster

#### VPN

Set up and manage Virtual Private Networks (VPNs).

Passaggio 3. Selezionare Add VPN. Se la connessione è già stata creata come in questo esempio, toccare l'icona del motore per modificarla. Specificare IPSec IKEv2 RSA nel campo Tipo. L'indirizzo del server è l'indirizzo IP dell'interfaccia ASA abilitata per IKEv2. Per il certificato utente IPSec e il certificato CA IPSec selezionare i certificati installati toccando i menu a discesa. Lasciare il certificato del server IPSec con l'opzione predefinita, Ricevuto dal server.



▲ 🖂	± ± 🖬 ± 🔋 🛣 \$2% 🚔 7:52 PM
÷	RE Edit VPN network
6	Name RA VPN to ASA Headend with IK
	Type
l	Server address 10.88.243.108
l	IPSec user certificate
l	IPSec CA certificate
l	calo_root-1 ▼ IPSec server certificate
	Received from server   DELETE CANCEL SAVE

Passaggio 4. Selezionare **Save** e quindi toccare il nome della nuova connessione VPN.



Passaggio 5. Selezionare Connetti.





Passaggio 6. Digitare nuovamente la connessione VPN per verificare lo stato. Viene visualizzato come **Connesso**.



# Verifica

Comandi di verifica sull'headend ASA:

```
ASA#show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username : Win7_PC.david.com Index : 24
Assigned IP : 192.168.50.1
                                  Public IP : 10.152.206.175
Protocol : IKEv2 IPsec
License
           : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
           : 0
Bytes Tx
                                   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) 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: Oxffffffff Oxfffffff

outbound esp sas:							
spi: 0x76131476 (	1980961910	)	-				
transform: esp	-aes-256 e	sp-sha-	hmac :	no comp	pression	n	
in use setting	s ={RA, Tu	nnel, 1	KEV2,	}			
slot: 0, conn_1d: 98304, crypto-map: Anyconnect							
TV size: 16 by	tes	IIICUI		CC)• 20	5707		
replay detecti	on support	: Y					
Anti replay bi	tmap:	_					
0x000000000	00000001						
ASA#show vpn-sessiondb	license-su	mmary					
VPN Licenses and Config	Jured Limit	s Summa					
							· · · · · · · · · · · · · · · · · · ·
AnyConnect Premium		: ENAB	LED :		50 :	50	: NONE
AnyConnect Essentials		: DISAB	LED :		50 :	0	: NONE
Other VPN (Available by	r Default)	: ENAB	LED :		10 :	10	: NONE
Shared License Server		: DISAB	LED				
Shared License Particip	pant	: DISAB	LED				
AnyConnect for Mobile		: ENAB	LED (R	equires	s Premi	um or Esse	entials)
Advanced Endpoint Asses	sment	: ENAB	LED(R	equires	s Premi	um)	
AnyConnect for Cisco VE	N Phone	: ENAB	LED				
VPN-3DES-AES		: ENAB	LED				
VPN-DES		: ENAB	LED				
VPN Licenses Usage Summ	arv						
	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 won-sessiond	·						
	, 						
VPN Session Summary							
	Ac	tive :	Cumul	ative	Peak	Concur : :	Inactive
American cit cit							
Anyconnect Client	•	0:		11	•	1.	U
SSL/TLS/DTLS	:	0 :		1.0		1 :	0
IKEV2 IPsec	:	0 :		10		1 :	0
Generic IKEv2 Remote Ac	cess :	1:		14 :	:	1	
Total Active and Inacti	ve :	1		 To	otal Cu	mulative	: 25
Device Total VPN Capaci	ty :	50					
Device Load	:	2%					
Tunnels Summarv							
		·					
	Ac	tive :	Cumul	ative	Peak (	Concurrent	t

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		

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nota: consultare le <u>informazioni importanti sui</u> comandi di<u>debug</u> prima di usare i comandi di debug.

**Attenzione**: sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene utilizzato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug aumenta. Procedere con cautela, soprattutto negli ambienti di produzione.

- Debug del protocollo ikev2 di crittografia 15
- Debug della piattaforma crypto ikev2 15
- Debug della crittografia ca 255