ASA IKEv2 RA VPN con clientes VPN de Windows 7 o Android y configuración de autenticación de certificados

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Overview Configurar autoridad de certificados Generar un certificado de cliente Instalación del certificado de identidad en el equipo cliente de Windows 7 Cómo instalar el certificado de identidad en el dispositivo móvil Android Configuración de la cabecera ASA para RA VPN con IKEv2 Configurar cliente integrado de Windows 7 Configuración del cliente VPN nativo de Android Verificación Troubleshoot

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) versión 9.7.1 y posteriores para permitir que los clientes VPN nativos de Windows 7 y Android (red privada virtual) establezcan una conexión VPN RA (acceso remoto) con el uso de Internet Key Exchange Protocol (IKEv2) y Certificates como método de autenticación.

Colaboración de David Rivera y Cesar Lopez Zamarripa, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autoridad de certificación (CA)
- Public Key Infrastructure (PKI)
- VPN RA con IKEv2 en ASA
- Cliente VPN incorporado de Windows 7
- Cliente VPN nativo de Android

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CISCO1921/K9 15.5(3)M4a como servidor IOS CA
- ASA5506X 9.7(1) como cabecera VPN
- Windows 7 como equipo cliente
- Galaxy J5 Android 6.0.1 como cliente móvil

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Overview

Estos son los pasos para configurar los clientes VPN nativos de Windows 7 y Android para conectarse a una cabecera ASA:

Configurar autoridad de certificados

La CA permite incrustar el uso de clave extendida (EKU) requerido en el certificado. Para la cabecera ASA, se requiere certificado Server Auth EKU, mientras que el certificado del cliente necesita Client Auth EKU.

Se puede utilizar una variedad de servidores CA, como:

- servidor CA de Cisco IOS
- servidor OpenSSL CA
- servidor CA de Microsoft
- 3rd CA de parte

El servidor de CA del IOS se utiliza para este ejemplo de configuración.

Esta sección describe la configuración básica para que un CISCO1921/K9 con la versión 15.5(3)M4a funcione como servidor de CA.

Paso 1. Asegúrese de que el dispositivo y la versión sean compatibles con el 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

Paso 2. Habilite el servidor HTTP en el router.

IOS-CA(config)#ip http server
Paso 3. Genere un par de claves RSA exportable.

IOS-CA(config)# crypto key generate rsa modulus 2048 label <HeadEnd> exportable
The name for the keys will be: HeadEnd
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds)

Paso 4. Configure un punto de confianza.

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: La dirección IP para el comando enrollment es una de las direcciones IP configuradas del router para una interfaz accesible.

Paso 5. Autentique el punto de confianza (Obtener el certificado de 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.
Paso 6. Inscriba el punto de confianza (obtenga el certificado de identidad).
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
```

```
Paso 7. Verifique los certificados.
```

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
```

Paso 8. Exporte el punto de confianza de HeadEnd al terminal en formato PKCS12 para obtener el certificado de identidad. El certificado de CA y la clave privada se agregan en un solo archivo.

<cisco123>

Exported pkcs12 follows:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAqqs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPqJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pqpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/1X1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIzEzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+qnNZLWs3eU1n84rryZq5Pjw3MRTu2yXDvr799qvx7NIZH5yUZyV11T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg VbYsR+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M1O4K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/0 lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbq0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3H1HCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L01CeUcVDM8aQfy 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 BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhqdme56tVV0Vq ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD51+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrFOh9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyq6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZSOSjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHIsA92pp1S7VFrAWP65wrhs4X0f4YSF1M89Sn4

GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp2lMps5jVKoFfpPJCie3F2FB3ecS+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.

Paso 9. Cree un punto de confianza vacío en el ASA.

ASA(config)# crypto ca trustpoint <HeadEnd> DRIVERAP(config-ca-trustpoint)# exit Paso 10. Importe el archivo PKCS12.

ASA(config)#crypto ca import <HeadEnd> pkcs12 <cisco123>

Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uB0tAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/1X1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyV11T70b 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 yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD51+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948op1YFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZSOSjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB01peC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4X0f4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8qczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAgIEAA==

INFO: Import PKCS12 operation completed successfully **Paso 11. Verifique la información del certificado**.

quit

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

Generar un certificado de cliente

Paso 1. Genere un par de claves RSA exportable.

IOS-CA(config)# crypto key generate rsa modulus 2048 label <Win7_PC> exportable
The name for the keys will be: Win7_PC
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds

Paso 2. Configure un punto de confianza.

```
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>
Dasa 2 Autoptique of pupto do configured configured (Obtoper of Content of Conten
```

Paso 3. Autentique el punto de confianza configurado (Obtener el certificado de 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.
```

Paso 4. Inscriba el punto de confianza autenticado (obtenga el certificado de identidad).

```
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
Paso 5. Verifique la información de los certificados.
```

```
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
```

Instalación del certificado de identidad en el equipo cliente de Windows 7

Paso 1. Exporte el punto de confianza Win7_PC con nombre a un servidor FTP/TFTP (instalado en su equipo Windows 7) en formato PKCS12 (.p12) para obtener el certificado de identidad, el certificado CA y la clave privada en un solo archivo.

```
!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.

Así es como se ve el archivo exportado en un equipo cliente.

Search Re	esults in TFTP-Root 🕨			✓ ✓ Win7_PC		×
Organize 🔻 Save sear	ch			G	•	0
★ Favorites	Win7_PC C:\TFTP-Root		Type: Personal Information Exch	Date modified: 7/13/2017 9:01 AM Size: 2.97 KB	l	
Downloads	Search again in: 😭 Libraries 🛛 👰 Computer	F Custom 🌔 Internet	File Contents			
 □ Libraries □ Documents □ Music □ Pictures □ Videos 1[™] Computer □ os (C:) ○ Network 						
↓ 1 item						

Paso 2. Presione Ctrl + R y escriba mmc para abrir Microsoft Management Console (MMC).

📨 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	mmc
	OK Cancel <u>B</u> rowse

Paso 3. Seleccione OK.

🚡 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
		here are no items to show in this view. Actions Console Root More Actions	

Paso 4. Vaya a Archivo>Agregar o quitar complemento.

🚡 Console1 - [Console Root]			
🖀 File Action View Favorites Window 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 se extensible snap-ins, you can configure which extensions are enabled.	et of snap-ins. For	Console Root	^
Available snap-ins: Selected snap-ins:		More Actions	,
Snap-in Vendor Console Root	Edit Extensions		
ActiveX Control Microsoft Cor	Remove		
Certificates Microsoft Cor	Maria Un		
Component Services Microsoft Cor	Move Up		
Device Manager Microsoft Cor Add >	Move Down		
Sisk Management Microsoft and			
Folder Microsoft Cor			
Group Policy Object Microsoft Cor			
IP Security Monitor Microsoft Cor IP Security Policy M Microsoft Cor			
Link to Web Address Microsoft Cor 🛫	Advanced		
Decription			
The ActiveX Control snap-in enables you to add an MMC node with a results view containing an ActiveX con	ntrol.		
	OK Cancel		
		11	

Paso 5. Seleccione Certificados > Add > Computer Account.

Console1 - [Console Root]		
File Action View Favorites Window Help		_ 8 ×
Console Root Name		Actions
		Console Root 🔺
Add or Remove Snap-ins	8	More Actions
You can select snap-ins for this console from those available on your computer and configure the selected se extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Selected snap-ins:	ertificates snap-in	
Snap-in Vendor Console Root	Muurer segurt	
ActiveX Control Microsoft Cor	My user account Service account Computer account	
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service,	Cancel	Next > Cancel

Paso 6. Seleccione Siguiente,

Consolel - [Console Root] File Action View Favorites Window Help	Actions Console Root More Articops
You can select snap-ins for this console from those available on your computer and configure the select extensible snap-ins; Selected snap-ins: Available snap-ins: Selected snap-ins: Snap-in Vendor ActiveX Control Microsoft Cor Certificates Microsoft Cor Device Manager Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Polider Microsoft Cor Folder Microsoft Cor Polider Microsoft Cor Folder Microsoft Cor Exercition: Microsoft Cor Exercition: Microsoft Cor Exercition: Microsoft Cor Exercition: Microsoft Cor E	Select Computer Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: the computer this console is running on) Another computer: Alow the selected computer to be changed when launching from the command line. This only applies if you save the console. CK Cancel

Paso 7. Terminen.

Console1 - [Console Root]							
🚡 File Action View Favorites Wir	ndow Help						- 8 ×
Concels Baset	1	1					
Console Root	Name					Actions	
	Add or Remove Snap-ins				×	Console Root	^
	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		

Paso 8. Seleccione OK.

Paso 9. Vaya a **Certificados (equipo local)>Personal>Certificados**, haga clic con el botón derecho del ratón en la carpeta y navegue hasta **Todas las tareas>Importar**:

🚡 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	
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

Paso 10. Haga clic en Next (Siguiente). Indique la ruta de acceso donde se almacena el archivo PKCS12.

Certificate Import Wizard	X
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 > Cance	2

Paso 11. Seleccione **Next** nuevamente y escriba la contraseña ingresada en el 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. Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

Paso 12. Seleccione Next.

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.	
Place all certificates in the following store Certificate store: Personal Browse	
Learn more about <u>certificate stores</u>	
< Back Next > Cancel	

Paso 13. Seleccione Siguiente una vez más.



Paso 14. Seleccione Finalizar.

Certificate Import Wizard	x
The import was successful.	
ОК	

Paso 15. Seleccione **OK**. Ahora verá los certificados instalados (tanto el certificado de CA como el certificado de identidad).

🚡 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							
🚡 File Action View Favorites Window Help							
← ⇒ 2 □ □ 0 ≥ 2 □							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
Certificates (Local Computer)	alo_root	calo_root	7/12/2020	<all></all>	cn=calo_ro	Certificates	^
Certificates	DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all> Secure Authentienti</all>	<none></none>	More Actions	•
Trusted Root Certification Author	En Win/_PC.david.com	calo_root	//15/2018	Server Authenticati	cn=win/_P		
Enterprise Trust Intermediate Certification Author							
 Trusted Publishers 							
Untrusted Certificates							
Third-Party Root Certification Aul Tructed People							
Other People							
Ams							
CanaryCertStore							
InjectorCertstore McAfee Trust							
PolicyCertStore							
Remote Desktop							
Certificate Enrollment Requests Smart Card Trusted Roots							
SMS							
⊳ SPC							
I rusted Devices							
	4				b		
Personal store contains 3 certificates.	, [F	1	

Paso 16. Arrastre y suelte el certificado CA desde Certificados (equipo local)>Personal>Certificados a Certificados (equipo local)>Autoridad de certificación raíz de confianza>Certificados.

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]						- • •	
a File Action View Favorites Window Help							- 6 ×
🗢 🔿 🖄 🔂 🖌 🖌 🖄 😹	? 🗊						
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	^
Personal Contification	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		
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	🔄 Cisco 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		
Remote 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>		
Smart Card Trusted Roots	🛱 DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com	1/12/2021	<all></all>	<none></none>		
	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
Districted Devicer	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
p in musted bevices	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	Enuifay Secure Certificate Auth	Equifay Secure Certificate Authority III	8/22/2018	Service Empil Serve	GenTrue		
Trusted Root Certification Authorities store co	ntains 60 certificates.						

🚡 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							- • •
🜇 File Action View Favorites Window 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							
Differ People							
CanaryCertStore							
▷ ☐ InjectorCertStore							
McAfee Trust							
PolicyCertStore							
Remote Desktop							
Smart Card Trusted Roots							
b ≦ SMS							
▷ C SPC							
Trusted Devices							
<	•				F		
Personal store contains 2 certificates.						,	

Cómo instalar el certificado de identidad en el dispositivo móvil Android

Nota: Android admite archivos de almacenamiento de claves PKCS#12 con extensión .pfx o .p12.

Nota: Android sólo admite certificados SSL X.509 codificados por DER.

Paso 1. Después de la exportación del certificado de cliente del servidor de CA del IOS en formato PKCS12 (.p12), envíe el archivo al dispositivo Android por correo electrónico. Una vez que lo tenga, toque el nombre del archivo para iniciar la instalación automática. (**No descargar el archivo**)

⊡ ⊟ ±		Ξ.	al 53%	8 7:24	PM
÷	1	•			÷
-					
					.
					1
					H
_					.
Androio	d_Smartphor	ne.p12	*	0	
*	~			*	
Reply	Reply	all	F	Forward	

Paso 2. Ingrese la contraseña utilizada para exportar el certificado, en este ejemplo, la contraseña es **cisco123**.

Extract certificate	
Enter the password to extrac certificates.	t the
CANO	EL OK

Paso 3. Seleccione **Aceptar** e introduzca un **nombre de certificado**. Puede ser cualquier palabra, en este ejemplo el nombre es **Certificado de ID de Android**.



Paso 4. Seleccione **OK** y aparecerá el mensaje "Android ID Cert installed" (Certificado de ID de Android instalado).

Paso 5. Para instalar el certificado de CA, extráigalo del servidor de CA del IOS en el formato base64 y guárdelo con la extensión .crt. Envíe el archivo al dispositivo android por correo electrónico. Esta vez, debe descargar el archivo pulsando en la flecha situada junto al nombre del archivo.

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

6:54 PM Tue, July 18	۰ م
< 🛇 <	⊗ 🛞
Wi-Fi Location Sound	Auto Bluetooth rotate
*	Outdoors
calo_root.crt Download complete.	6:54 PM
NOTIFICATION SETTINGS	CLEAR
second second s	
the second se	
Calo_root.crt	± 🛆
Reply Reply all	IIII Forward

Paso 6. Navegue hasta Configuración y Bloquear pantalla y seguridad.



Paso 7. Seleccione Otros parámetros de seguridad.

⊡ ±		50% 🛢 6:57 PM
← Loc	k screen and secur	ity
Notificat Show control	tions on lock screen	í
Secure I Set your se and Lock in	ock settings cure lock functions, such a istantly with Power key.	s Auto lock
Security		
Find My Locate and Samsung a	Mobile control your device remote ccount.	ely using your
Unknow Allow insta other than r	n sources Ilation of apps from source the Play Store.	
Encrypt Protect you	device Ir device by encrypting its d	lata.
Encrypt No SD card	SD card Inserted	
Other se Change oth security up	curity settings er security settings, such a dates and credential storag	s those for le.

Paso 8. Vaya a Instalación desde el almacenamiento de dispositivos.

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.

Paso 9. Seleccione el archivo .crt y toque Finalizado.

Select file	DONE
ealo_root-1.crt	

Paso 10. Introduzca un **nombre de certificado**. Puede ser cualquier palabra, en este ejemplo, el nombre es **calo_root-1**.



Paso 10. Seleccione **OK** y verá el mensaje "calo_root-1 instalado".

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

Paso 11. Para verificar que el certificado de identidad está instalado, navegue a Settings/Lock Screen y Security/Other > Security Settings/User Certificates/System tab.

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

Paso 12. Para comprobar que el certificado de CA está instalado, vaya a **Configuración/Bloquear** pantalla y seguridad/Otros parámetros de seguridad/Ver certificados de seguridad/ficha Usuario.

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

	I 54% ≣ 7:45 PM						
← View security certificates							
SYSTEM	USER						
calo_root							

Configuración de la cabecera ASA para RA VPN con IKEv2

Paso 1. En ASDM, navegue hasta Configuration>Remote Access VPN > Network (client) Access> Anyconnect Connection Profiles. Marque la casilla IPSec (IKEv2), Permitir acceso en la interfaz que se encuentra frente a los clientes VPN (la opción Habilitar servicios de cliente no es necesaria).

Paso 2. Seleccione **Device Certificate** y quite la marca de verificación de **Use el mismo certificado** de dispositivo para SSL e IPSec IKEv2.

Paso 3. Seleccione el certificado de cabecera para la conexión IPSec y seleccione — Ninguno — para la conexión SSL.

Esta opción coloca el crypto ikev2, crypto ipsec, crypto dynamic-map y la configuración de crypto map.

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 🔚 S	ave 🔇 Refresh 🕻	Back 🔘 Forwar	rd 🦻 Help					CISCO
Remote Access VPN	Configuration >	Remote Access VPM	I > Network (Client)	Access > AnyConnect	Connection Profiles			
2 Introduction			dentities Care An Ca			***	Interface shakes The Class Are Connect 1001 C	
Part Retwork (Client) Access	IPsec (IKEv2) tur	nnel as well as SSL tunr	nel with Datagram Tran	sport Layer Security (DTLS) tunneling options.	me initial clent deployment requires end-user admin	is a sive rights. The cisco Anyconnect vervice	ient supports
AnyConnect Customization /Localization	Access Interfaces							
AnyConnect Client Profile	Enable Cisco	AnyConnect VPN Clien	nt access on the interfa	ces selected in the table b	wole			
AnyConnect Client Software Dynamic Access Policies	SSL access must	be enabled if you allow	v AnyConnect client to	be launched from a browse	r (Web Launch) .			
Group Policies		SSL Access		IPsec (IKEv2) Acces	s			
IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles	Interface	Allow Access	Enable DTI S	Allow Access	Enable Client Service	Device Certificate		
- Secure Mobility Solution	outside	Alloin Access	Endole Dites			Port Sattings		
Address Assignment	inside			m		For CSecongs		
Clientless SSL VPN Access								
Host Scan Image	Bypass interf	face access lists for inb	ound VPN sessions					
Secure Desktop Manager	Access lists from	group policy and user	policy always apply to	the traffic.				
Certificate Management Language Localization	Login Page Setting							
Load Balancing	Allow user to	select connection prof	file on the login page.	0				
DHCP Server	Shutdown po	rtal login page.						
Advanced	Connection Profiler							
	Connection prof	ile (tunnel aroun) speci	ifies how user is auther	nticated and other naramet	ers. You can configure th	he manning from certificate to connection profile he		
							<u>.</u>	
	Se Add	dit Delete Find:		Match Case				
	Name	SSL En	abled	IPsec Enabled	Alia	ases Authentication Metho	d Group Policy	
	DefaultRAGroup				V	AAA(LOCAL)	DfltGrpPolicy	
	DefaultWEBVPN	Group			√	AAA(LOCAL)	DfltGrpPolicy	
						Specify Device Certificate		— ×
Couries Setue						Device certificate is a digital certificate that ide	ntifies this ASA to the clients.	
Device Setup						Ise the same device certificate for SSI an	d IPsec IKEv2	
Firewall								
Remote Access VPN						Device Certificate for SSL Connection:	ne	•
						Device Certificate for IPsec Connection: Hear	dend:hostname=Connected_2_INET-B, cn=He	sadEnd.da 👻
Site-to-Site VPN	Let group UR	L take precedence if o	roup URL and certificat	e map match different con	nection profiles. Otherwis	54	Manage Certificates	
Device Management						ОК	Cancel Help	
»					Apply			

Así es como se ve la configuración en la interfaz de línea de comandos (CLI).

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 ikev2 policy 1

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

Paso 4. Vaya a Configuration > Remote Access VPN > Network (Client) Access > Group Policies para crear una política de grupo

Add Internal Group Policy			×
General Servers D-Advanced	Name: GP_David Banner: VI Inherit		
	SCEP forwarding URL: V Inherit		
	Address Pools: 📝 Inherit		Select
	IPv6 Address Pools: 📝 Inherit		Select
	More Options		*
	Tunneling Protocols:	Inherit Clientiess SSL VPN SSL VPN Client IPsec IKEv1 V IPsec IKEv2 LZTP/IPsec	
	Filter:	V Inherit	Manage
	Access Hours:	V Inherit	Manage
	Simultaneous Logins:	☑ Inherit	
	Restrict access to VLAN:	☑ Inherit v	
	Connection Profile (Tunnel Group) Lock:		
	Maximum Connect Time:		
	Maximum connect nine.		
	Idle Timeout:	V Inherit None minutes	
	Security Group Tag (SGT):	Inherit None (2 - 65519)	
	On smart card removal:	☑ Inherit O Disconnect O Keep the connection	
	Periodic Certificate Authentication Interval	☑ Inherit Unlimited hours	
Find:	Next Previous		
		OK Cancel Help	

En CLI.

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

Paso 5. Navegue hasta Configuration > Remote Access VPN > Network (Client) Access > Address Pools y seleccione Add para crear un Pool IPv4.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File View Tools Wizards Window Help			Type topic to search Go	ababa
Home Sconfiguration Annual Same	ive 🔇 Refresh 🔇 Back 🕥 Forward 🢡 Help			cisco
Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access	> Address Assignment > Address Pools		
Retmote Access Viria Retmote Access Viria Retmote Access Viria Retmote Access Viria Retmote Clamp AnyConnet Connection Profiles AnyConnet Clamp AnyConnet Profiles Part District Software Address Policies Secure Mobility Solution Address Assignment Address Assignment Address Solution Contecton Profiles Address Solution Contecton Profiles Contecton Profiles	Configure named IP Address Pools. The IP Address Pools can dustering. Add • C Edit Delete Pool Name Starting Address ACPool 192, 168,50,1	I be used in either a VPN [Decc[IXEV]] Connection Profiles, AnvConnect Conne Ise Ending Address, Number of Addresses IS2, 168, 50, 100 Edit IPv4 Pool Name: ACPool Starting IP Address: IS2, 168, 50, 1] Ending IP Address: IS2, 168, 50, 100	ection Profiles, Group Policies configuration , or in <u>Interfaces</u> configuration Subnet Mask/Prefix Length 255: 255: 0	related to ASA
Point Scan Image Point Scan Point Scan		Subnet Mask: 255.255.255.0 OK Cancel Help		
Device Management		Apply Reset		

ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0

Paso 6. Navegue hasta Configuration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles y seleccione Add para crear un nuevo grupo de túnel.





```
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
```

Paso 7. Navegue hasta Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy y marque la casilla Utilizando las reglas configuradas para matematizar un certificado en un Connection Profile.



En CLI.

tunnel-group-map enable rules

Paso 8. Vaya a Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules y cree un nuevo Certificate Map. Seleccione Add y asócielo al grupo de túnel. En este ejemplo, el grupo de túnel se llama 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	de de
Home 🗞 Configuration 🔯 Monitoring 📊 S	Save 🚱 Refresh 🔇 Back 💭 Forward 🤶 Help	cisco
Remote Access VPN	Configuration > Remote Access VPN > Hetwork (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules	
Introduction Introduction AnyConnect Connection Profiles AnyConnect Clent Profile AnyConnect Clent Profile AnyConnect Clent Profile AnyConnect Clent Profile Profiles Proce(IVEV) Connection Profiles Profiles Profiles Proce(IVEV) Connection Profiles Profiles	Define rules to map certificates to desired AnyConnect or clientiess SSL connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule certificate to Connection Profile Maps Add Add Add Rule Priority Mapped to Connection Profile Mapping Criteria	le.
Assignment Policy		
Clentes SSU VPI Acces Clentes SSU VPI Acces AAA/contect AnyConnect Custom Attributes AnyConnect Custom Attribut	Add ertificate Matching Rule Configure a critificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the critificate matching rule and associate it with ower values having greater priority. Rules that are not mapped will be ignored. Map: Existing DefaultCertificateMap Priority: 10 Mapped to Connection Profile: <u>Devid</u> Concellered Help	
Image: Prevail Image: P	e Apply Reset	

En CLI.

tunnel-group-map CERT_MAP 10 David

Paso 9. Seleccione Agregar en la sección Criterios de asignación e introduzca estos valores.

Campo: Emisor

Operador: Contiene

Valor: calo_root

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254		- F X
File View Tools Wizards Window Help	Type topic to search Go	ahaha
Home 🍪 Configuration 🔯 Monitoring 🎧 Sa	ave 💽 Refresh 🚫 Back 🔘 Forward 🦻 Help	CISCO
Remote Access VPN	Configuration > Remote Access VPII > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules	
Remote Access VPH P Partoduction P Partoduction <t< td=""><td>Configuration > Remote Access VPH > Hetwork (Clent) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules Define rules to map certificates to desired AnyConnect or denides SSL connection profiles (turnel groups). Use the bottom table to configure certificate fields together with their matching orteris for the selected or Certificate to Connection Profile Maps</td><td></td></t<>	Configuration > Remote Access VPH > Hetwork (Clent) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules Define rules to map certificates to desired AnyConnect or denides SSL connection profiles (turnel groups). Use the bottom table to configure certificate fields together with their matching orteris for the selected or Certificate to Connection Profile Maps	
Device Management	Apply Reset	

En CLI.

crypto ca certificate map CERT_MAP 10 issuer-name co calo_root

Paso 10. Cree un objeto con la red del conjunto IP que se utilizará para agregar una regla de exención de NAT (traducción de direcciones de red) en **Configuración > Firewall > Objetos > Objetos/Grupos de Red> Agregar**.

Cisco A DM 7.8(1)150 for ASA - 192.168.0.254					Type topic to caurch	
Home Configuration Monitoring S	ave 🔇 Refresh 🔇 Back 🕥 Fo	orward 🦻 Help			Type topic to search 00	cisco
Firewall 🗗 🖗	Configuration > Firewall > Obje	cts > Network Objects/Grou	<u>ps</u>			
Access Rules	💠 Add 👻 🗹 Edit 📋 Delete C	🖁 Where Used 🔍 Not Used				
G Service Policy Rules	Filter:					Filter Clear
Filter Rules	Name	IP Address	Netmask	Description	Object NAT Address	
Public Servers PRUR Filtering Servers PRUR Filtering Servers Prevent Detection Prevent Detection Prevent Detection Prevent Detection Prevent Pr	Network Objects 	10.88.243.0 50 192155.50.0 192.158.0.0 224.0.0.251 224.0.0.252	255.255.255.128 255.255.255.0 255.255.0 255.255.0 KODject NETWORK_08J_192.168.50.0_24 NETWORK_08J_192.168.50.0_24 192.158.50.0 255.255.255.0 CK Cancel			
Site-to-Site VPN	-					
Berne management			Apply	Reset		

En CLI.

object network NETWORK_OBJ_192.168.50.0_24 subnet 192.168.50.0 255.255.255.0

Paso 11. Navegue hasta **Configuration > Firewall > NAT Rules** y seleccione **Add** para crear la regla de exención de NAT para el tráfico VPN RA.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254							
File View Tools Wizards Window Help						Type topic to search Go	de de
Home 🗞 Configuration 📴 Monitoring 🔲 Save 🔇 Refresh 🔇	Back R Forward ? Help						cisco
Firewall 🗗 🖓 Configuration > Firewall	ewall > NAT Rules					Addresses Services	
Access Rules 💠 Add - 🏹 Edit						Addresses	⊡ ₽ ×
The NAT Rules						💠 Add 👻 🛒 Edit 🏢 Delete 🔍 Where U	Ised 🔍 Not Used
AAA Rules #	Match Criteria: Original Packet —	,	7		Options	Filter:	Filter Clear
Source Intr	Source Interface:	inside 🗸	Destination Interface:	outside 🔹		Name	1
URL Filtering Servers "Network Object"	Source Address:	any -	Destination Address:	<_OBJ_192.168.50.0_24 -	NOPTOXY	-Network Objects	
Threat Detection			Service:	any –		🏟 any	
20 Identity Options						🧇 any4	
E-C Objects	Action: Translated Packet	Challe	r				
Network Objects/Groups Service Objects/Groups	Source NAT Type:	static				NETWORK OBJ 192.168.50.0 24	
G Local Users	Source Address:	Original	Destination Address:	Original		- add outside-network/24	
Local User Groups	Use one-to-one address trans	lation				- 3 224.0.0.251	
Gass Maps	PAT Pool Translated Address:		Service:	Original			
🕀 🔀 Inspect Maps	Round Robin						
Regular Expressions							
Time Ranges	Extend PAT uniqueness to p	er destination instead of per i	nterrace				
Communications Advanced	Translate TCP and UDP port	s into flat range 1024-65535	Include range 1-102	13			
	Fall through to interface PAT						
	Use IPv6 for source interface	PAT	Use IPv6 for desti	nation interface PAT			
	Options						
	Enable rule						
	Translate DNS replies that mat	tch this rule					
	Disable Proxy ARP on egress in	nterface					
	Lookup route table to locate e	gress interface					
Spevice Setup	Direction: Both +						
	Description:						
Contraction of the second seco							
Remote Access VPN		OK Cancel	Help				
Site-to-Site VPN							
Device Management		m) F		
		Apply	eset				

En 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

Esta es la configuración ASA completa utilizada para este ejemplo.

```
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
```

Configurar cliente integrado de Windows 7

Paso 1. Vaya a Panel de control > Red e Internet > Centro de redes y recursos compartidos.

~~~~~			
Control Panel 🕨	Network and Internet   Network and Sharing Center	✓  ✓  Search Control Panel	Q
Control Panel Home	View your basic network information and s	set up connections	<u>^</u>
Manage wireless networks	i i i i i i i i i i i i i i i i i i i	See full map	
Change adapter settings	DRIVERAP-6KUZH cisco.com	Internet	
Change advanced sharing	(This computer)		
secongs	View your active networks	Connect or disconnect	t
	cisco.com	Access type: Internet	
	Domain network	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	I-up, or VPN network connection.	
Internet Options	Choose homegroup and sharing options		
Windows Firewall	Access files and printers located on other netv	vork computers, or change sharing settings.	-

Paso 2. Seleccione Configurar una nueva conexión o red.

🖗 🐏 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>	
Nex	t Cancel

Paso 3. Seleccione Conectar a un lugar de trabajo y Siguiente.



Paso 4. Seleccione No, cree una nueva conexión y Siguiente.



Paso 5. Seleccione **Use my Internet connection (VPN)** y agregue la cadena HeadEnd certificate Common Name (CN) en el campo **Internet address**. En el campo **Nombre de destino**, escriba el nombre de la conexión. Puede ser cualquier cadena. Asegúrese de comprobar el mensaje **No conectar ahora; sólo debe configurarlo para poder conectarlo más adelante**.

		- • •
🚱 🌆 Connect to a Workplace	:	
Type the Internet add	ress to connect to	
Your network administrator	can give you this address	
Tour network administrator		
Internet address:	HeadEnd.david.com	
Destination name:	RA VPN to ASA with IKEv2	
Use a smart card		
😵 🕅 Allow other people t This option allows a	to use this connection nyone with access to this computer to use this connection.	
Don't connect now;	just set it up so I can connect later	
	Ne	t Cancel

Paso 6. Seleccione Next.

😋 🗽 Connect to a Workpla	ce	
Type your user nam	e and password	
User name:	1	]
Password:		]
	Show characters Remember this password	
Domain (optional):		]
		Create Cancel

Paso 7. Seleccione Crear.



Paso 8. Seleccione **Cerrar** y navegue hasta **Panel de control > Red e Internet > Conexiones de red**. Seleccione la conexión de red creada y haga clic con el botón derecho en ella. Seleccione Properties (Propiedades).

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

Paso 9. En la pestaña **General** puede verificar que el nombre de host adecuado para la cabecera sea correcto. El ordenador resolverá este nombre a la dirección IP de ASA utilizada para conectar usuarios de VPN de RA.

RA VPN to ASA with IKEv2 Properties									
General Options Security Networking Sharing									
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):									
HeadEnd.david.com									
First connect									
Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.									
Dial another connection first:									
See our online <u>privacy statement</u> for data collection and use information.									
OK Cancel									

Paso 10. Navegue hasta la pestaña **Seguridad** y seleccione **IKEv2** como el **Tipo de VPN**. En la sección **Autenticación** seleccione **Usar certificados de máquina**.

RA VPN to ASA with IKEv2 Properties	<b>×</b>
General Options Security Networking	Sharing
Type of VPN:	
IKEv2	•
Data encryption:	Advanced settings
Require encryption (disconnect if server d	eclines) 🔹
Authentication	
Use Extensible Authentication Protoco	ol (EAP)
	· ·
L	Properties
Use machine certificates	
	OK Cancel

Paso 11. Seleccione **OK** y navegue a **C:\Windows\System32\drivers\etc**. Abra el archivo **host** con un editor de texto. Configure una entrada para resolver el FQDN (Nombre de dominio completo) configurado en la conexión de red a la dirección IP de su cabecera ASA (en este ejemplo, la interfaz externa).

```
# 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

Paso 12. Vuelva al **Panel de control > Red e Internet > Conexiones de red**. Seleccione la conexión de red que ha creado. Haga clic con el botón derecho y seleccione **Connect (Conectar).** 

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	ıt		
	۲	Delete			
	۲	Rename			
	0	Properties			

Paso 13. El estado de la conexión de red pasa de Desconectado a Conectando y luego a Conectado. Por último, se muestra el nombre especificado para la conexión de red.



El ordenador está conectado a la cabecera VPN en este momento.

## Configuración del cliente VPN nativo de Android

Paso 1. Vaya a Settings>More connection Settings



Paso 2. Seleccione 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).

Paso 3. Seleccione Add VPN. Si la conexión ya se ha creado como en este ejemplo, pulse el icono del motor para editarla. Especifique IPSec IKEv2 RSA en el campo Type. La dirección del servidor es la dirección IP de la interfaz ASA habilitada para IKEv2. Para el certificado de usuario IPSec y el certificado de CA IPSec, seleccione los certificados instalados pulsando en los menús desplegables. Deje el certificado de servidor IPSec con la opción predeterminada, Recibido del servidor.



± ± 0 ±	¥ "∎ 52% 🛢 7:52 PM
Edit VPN networ	RE K
Name RA VPN to ASA H	leadend with IK
Туре	
IPSec IKEv2 RSA	· · · ·
Server address	
10.88.243.108	
IPSec user certific	ate
Android ID Cert 🔻	
IPSec CA certificat	te
calo_root-1 🔻	
IPSec server certif	icate
Received from ser	ver 🔻
DELETE	CANCEL SAVE

Paso 4. Seleccione **Save** y luego toque el nombre de la nueva conexión VPN.



Paso 5. Seleccione Connect (Conectar).





Paso 6. Escriba la conexión VPN una vez más para verificar el estado. Ahora se muestra como **Conectado**.



# Verificación

Comandos de verificación en la cabecera ASA:

```
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
           : 0
Pkts Tx
                                   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		

# Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Nota: Consulte Información Importante sobre los Comandos Debug antes de utilizar los comandos debug.

**Precaución**: En ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, la verbosidad de las depuraciones aumenta. Haga esto con precaución, especialmente en entornos de producción.

- Debug crypto ikev2 protocol 15
- Depurar la plataforma crypto ikev2 15
- Debug crypto ca 255