

# Configure el ASA como el gateway SSL para los clientes de AnyConnect que usan la autenticación basada certificado múltiple

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Limitaciones](#)

[Selección del certificado en las Plataformas del no Windows de Windows v/s](#)

[Flujo de la conexión para la autenticación del certificado múltiple](#)

[Configurar](#)

[Autenticación del certificado múltiple de la configuración vía el ASDM](#)

[Configuración ASA para la autenticación del certificado múltiple vía el CLI](#)

[Verificación](#)

[Vea los Certificados instalados en el ASA vía el CLI](#)

[Vea los Certificados instalados en el cliente](#)

[Certificado de la máquina](#)

[Certificado de usuario](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar un dispositivo de seguridad adaptante (ASA) como el gateway de Secure Sockets Layer (SSL) para los Clientes de movilidad Cisco AnyConnect Secure que utiliza la autenticación basada certificado múltiple.

## Prerequisites

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración CLI ASA y de la configuración VPN SSL
- Conocimiento básico de los Certificados X509

## Componentes Utilizados

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

- Software adaptante del dispositivo de seguridad de Cisco (ASA), versión 9.7(1) y posterior
- Windows 10 con el Cliente de movilidad Cisco AnyConnect Secure 4.4

**Note:** Descargue el paquete de AnyConnect VPN Client (anyconnect-win\*.pkg) de [Descarga de Cisco Software \(sólo clientes registrados\)](#). Copie el AnyConnect VPN client en la memoria flash ASA, que será descargada a los equipos de los usuarios remotos para establecer la conexión SSL VPN con el ASA. Consulte la sección [Instalación de AnyConnect Client de la](#) guía de configuración ASA para obtener más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Antecedentes

Antes de la versión de software 9.7(1), los soportes ASA escogen el certificado basado la autenticación, que significa que el usuario o la máquina puede ser autenticado pero no ambas, para una tentativa de la sola conexión.

La autenticación basada certificado múltiple da la capacidad de hacer que el ASA valide la máquina o el certificado del dispositivo, asegurar el dispositivo es un dispositivo corporativo-publicado, además de autenticar el certificado de identidad del usuario para permitir el acceso VPN.

## Limitaciones

- La autenticación del certificado múltiple limita actualmente el número de Certificados a exactamente dos.
- El cliente de AnyConnect debe indicar el soporte para la autenticación del certificado múltiple. Si ése no es el caso entonces que el gateway utiliza uno de los métodos de autenticación de la herencia o falle la conexión. La versión 4.4.04030 o posterior de AnyConnect soporta la autenticación basada Multi-certificado.
- Para la plataforma de Windows, el certificado de la máquina se envía durante el contacto SSL inicial seguido por el Certificado de usuario bajo protocolo global del auth. Dos Certificados del almacén de la máquina de Windows no se soportan.
- La autenticación del certificado múltiple ignora las preferencias **automáticas de la selección del certificado del permiso** bajo perfil XML que significa que el cliente intenta todas las combinaciones para autenticar ambos los Certificados hasta que falle. Esto puede introducir el considerable retardo mientras que Anyconnect intenta conectar. Por lo tanto, se recomienda para utilizar el certificado que corresponde con en caso del usuario múltiple/del certificado de la máquina en la máquina del cliente.
- Los soportes de Anyconnect SSL VPN solamente RSA-basaron los Certificados.

- Solamente SHA256, SHA384, y el certificado basado SHA512 se soportan durante el auth global.

## Selección del certificado en las Plataformas del no Windows de Windows v/s

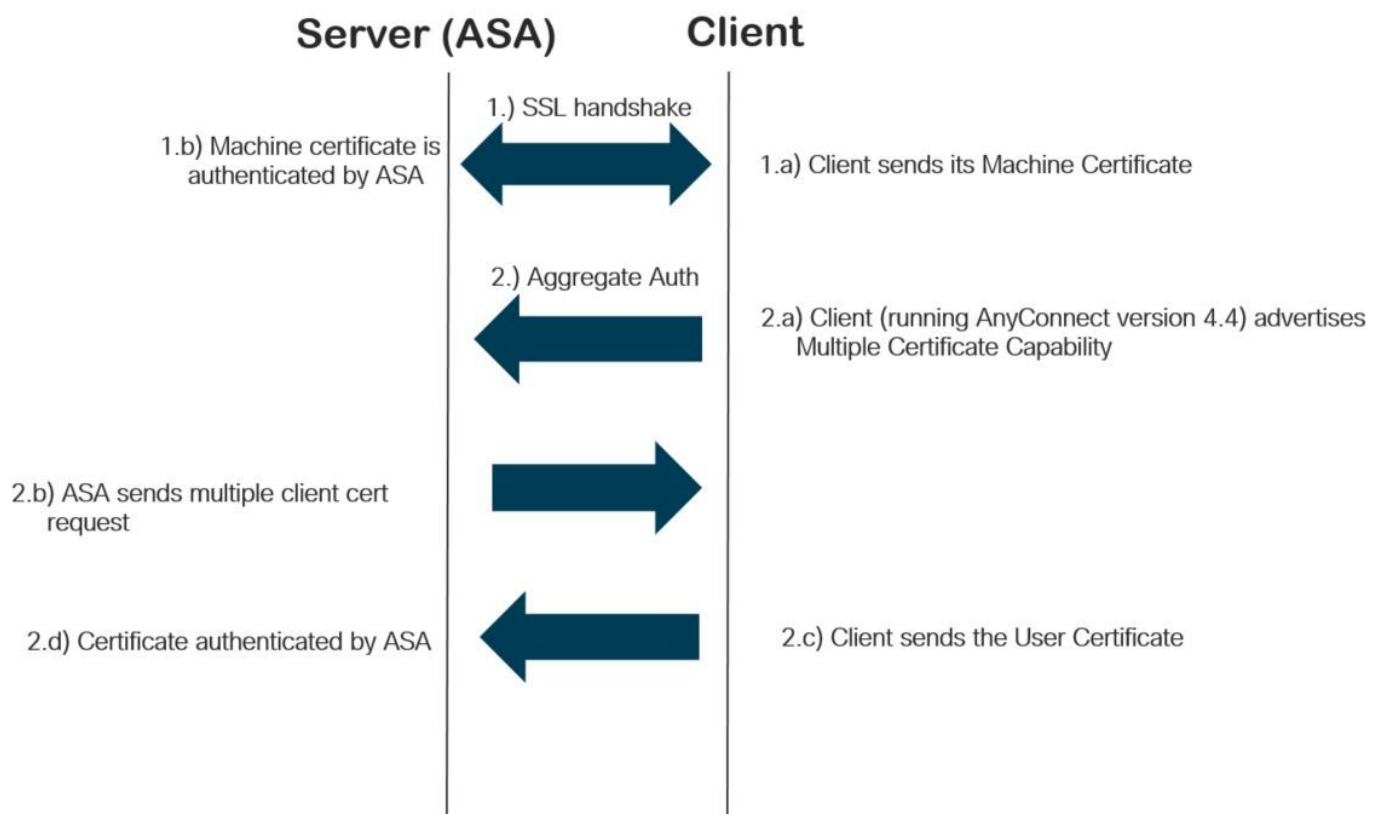
AnyConnect en Windows distingue entre los Certificados extraídos del almacén de la máquina (accesible solamente por los procesos privilegiados) y del almacén del usuario (accesible solamente por los procesos poseídos por el usuario conectado al sistema). No se hace ninguna tal distinción por AnyConnect en las Plataformas del no Windows.

El ASA puede elegir aplicar una directiva de la conexión, configurada por el administrador ASA, sobre la base de los tipos reales de Certificados recibidos. Para Windows, los tipos pueden ser:

- Una máquina y un usuario, o
- Usuario dos.

Para las Plataformas del no Windows, la indicación es siempre dos Certificados de usuario.

## Flujo de la conexión para la autenticación del certificado múltiple



## Configurar

### Autenticación del certificado múltiple de la configuración vía el ASDM

Esta sección describe cómo configurar Cisco ASA como el gateway SSL para los clientes de

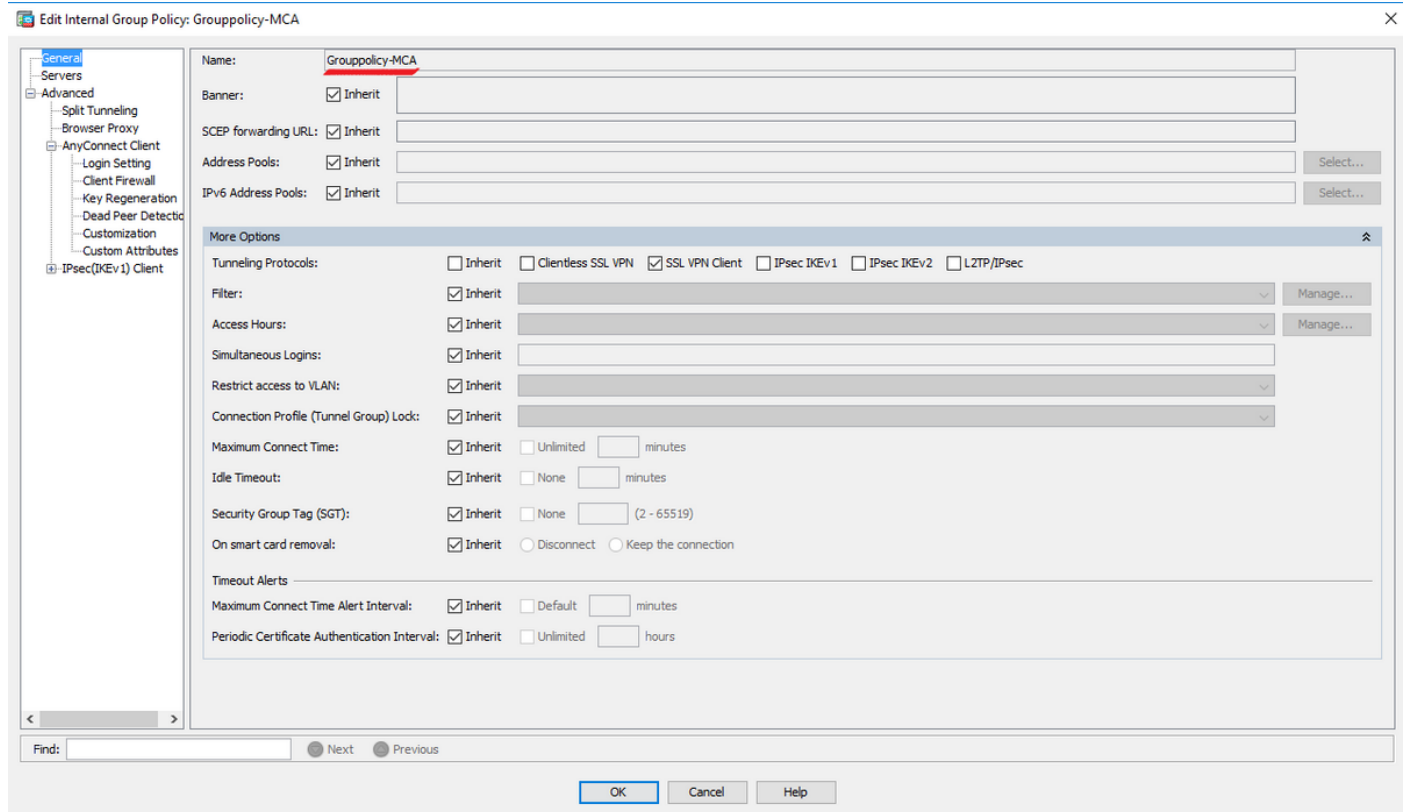
AnyConnect con la autenticación del certificado múltiple.

Complete estos pasos vía el ASDM para configurar a los clientes de Anyconnect para la autenticación del certificado múltiple:

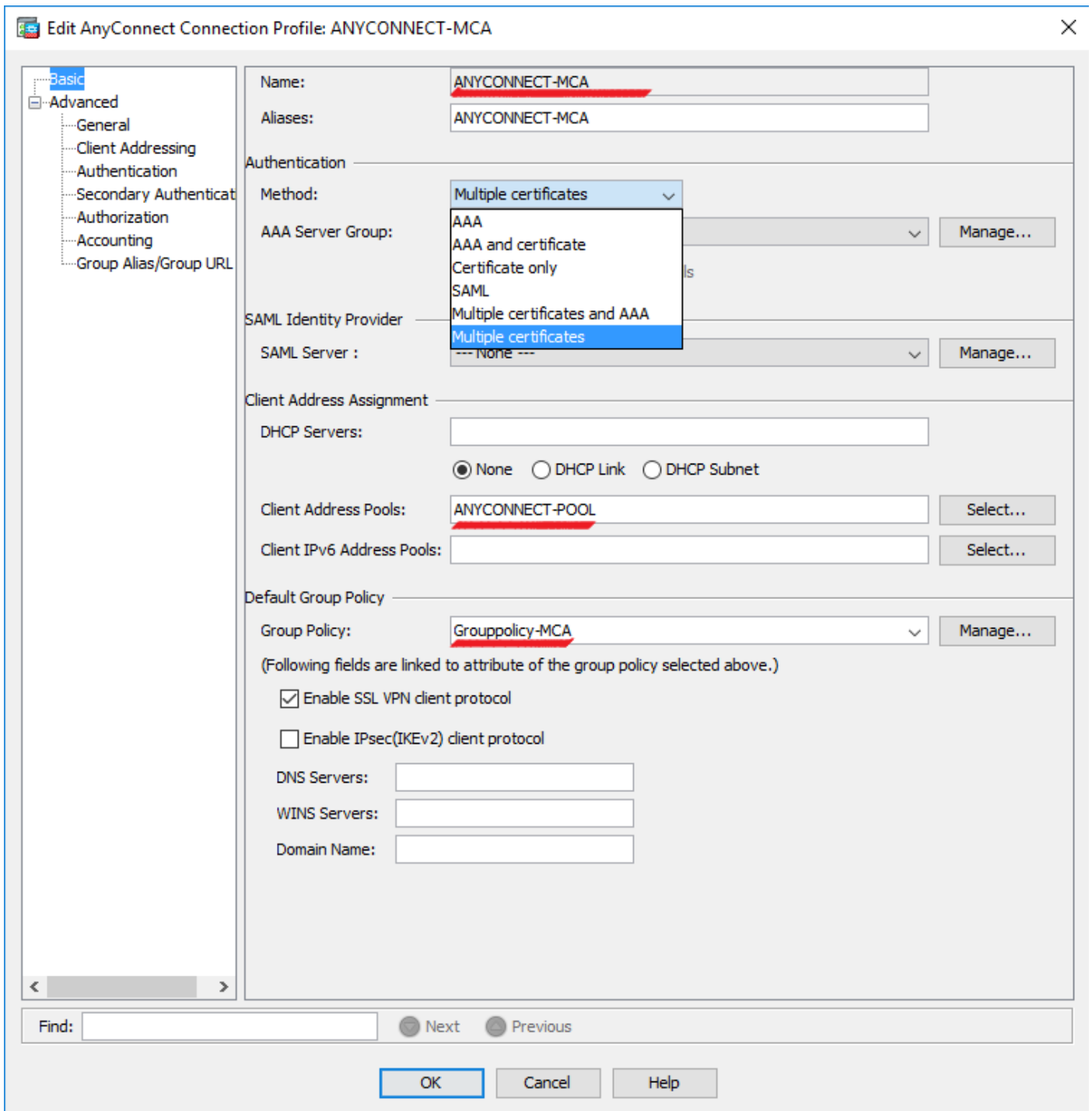
Paso 1. Instale el certificado de CA para el usuario y los certificados de la máquina en el ASA.

Para la instalación del certificado refiera a la [configuración ASA: Instalación y renovación del certificado digital SSL](#)

Paso 2. Navegue a la **directiva de la configuración > del Acceso Remoto > del grupo** y configure la Grupo-directiva.



Paso 3. Configure el perfil de la nueva conexión y el **método de autenticación** selecto como certificados múltiples y seleccione la Grupo-directiva creada en el paso 1.



Paso 4. Para la otra configuración detallada, [refiera el cliente del toVPN y el acceso al cliente de AnyConnect al ejemplo de configuración del LAN local](#)

## Configure el ASA para la autenticación del certificado múltiple vía el CLI

**Note:** Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

```
ASA Version 9.7(1)
!  
hostname GCE-ASA
```

```

!
! Configure the VPN Pool
ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 100
ip address 10.197.223.81 255.255.254.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
! Configure Objects
object network obj-AnyConnect_pool
subnet 192.168.100.0 255.255.255.0
object network obj-Local_Lan
subnet 192.168.1.0 255.255.255.0
!
! Configure Split-tunnel access-list
access-list split standard permit 192.168.1.0 255.255.255.0
!
! Configure Nat-Exemption for VPN traffic
nat (inside,outside) source static obj-Local_Lan obj-Local_Lan destination static obj-
AnyConnect_pool obj-AnyConnect_pool no-proxy-arp route-lookup
!
! TrustPoint for User CA certificate
crypto ca trustpoint UserCA
enrollment terminal
crl configure
!
! Trustpoint for Machine CA certificate
crypto ca trustpoint MachineCA
enrollment terminal
crl configure
!
!
crypto ca certificate chain UserCA
certificate ca 00ea473dc301c2fdc7
30820385 3082026d a0030201 02020900 ea473dc3 01c2fdc7 300d0609 2a864886
<snip>
3d57bea7 3e30c8f0 f391bab4 855562fd 8e21891f 4acb6a46 281af1f2 20eb0592
012d7d99 e87f6742 d5
quit

crypto ca certificate chain MachineCA
certificate ca 00ba27b1f331aea6fc
30820399 30820281 a0030201 02020900 ba27b1f3 31aea6fc 300d0609 2a864886
f70d0101 0b050030 63310b30 09060355 04061302 494e3112 30100603 5504080c
<snip>
2c214c7a 79eb8651 6ad1eabd ae1ffbbba d0750f3e 81ce5132 b5546f93 2c0d6ccf
606add30 2a73b927 7f4a73e5 2451a385 d9a96b50 6ebeba66 fc2e496b fa
quit
!
! Enable AnyConnect
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
!
! Configure Group-Policy

```

```
group-policy Grouppolicy-MCA internal
group-policy Grouppolicy-MCA attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
!
! Configure Tunnel-Group
tunnel-group ANYCONNECT-MCA type remote-access
tunnel-group ANYCONNECT-MCA general-attributes
address-pool ANYCONNECT-POOL
default-group-policy Grouppolicy-MCA
tunnel-group ANYCONNECT-MCA webvpn-attributes
authentication multiple-certificate
group-alias ANYCONNECT-MCA enable
group-url https://10.197.223.81/MCA enable
```

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

**Note:** [La herramienta del Output Interpreter \(clientes registrados solamente\)](#) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

## Vea los Certificados instalados en el ASA vía el CLI

### muestre el certificado Ca crypto

```
GCE-ASA(config)# show crypto ca certificate
```

```
CA Certificate
```

```
Status: Available
Certificate Serial Number: 00ea473dc301c2fdc7
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Subject Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Validity Date:
start date: 15:40:28 UTC Sep 30 2017
enddate: 15:40:28 UTC Jul202020
Storage: config
Associated Trustpoints: UserCA
```

## CA Certificate

Status: Available

Certificate Serial Number: 00ba27b1f331aea6fc

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA256 with RSA Encryption

Issuer Name:

cn=MachineCA.cisco.com

o=Cisco

l=Bangalore

st=Karnataka

c=IN

Subject Name:

cn=MachineCA.cisco.com

o=Cisco

l=Bangalore

st=Karnataka

c=IN

Validity Date:

start date: 15:29:23 UTC Sep 30 2017

enddate: 15:29:23 UTC Jul202020

Storage: config

Associated Trustpoints: MachineCA

## **Vea los Certificados instalados en el cliente**

Para verificar la instalación, utilice al Certificate Manager (certmgr.msc):

## **Certificado de la máquina**



File Action View Favorites Window Help

← → ↻ 📄 ✂ 📄 ✖ 📄 📄 ? 📄

Issued To	Issued By	Expiration Date	Intended Purposes
MachineID.cisco.com	MachineCA.cisco.com	2/13/2019	Server Authenticati...

Certificate

General Details Certification Path

**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

---

**Issued to:** MachineID.cisco.com

**Issued by:** MachineCA.cisco.com

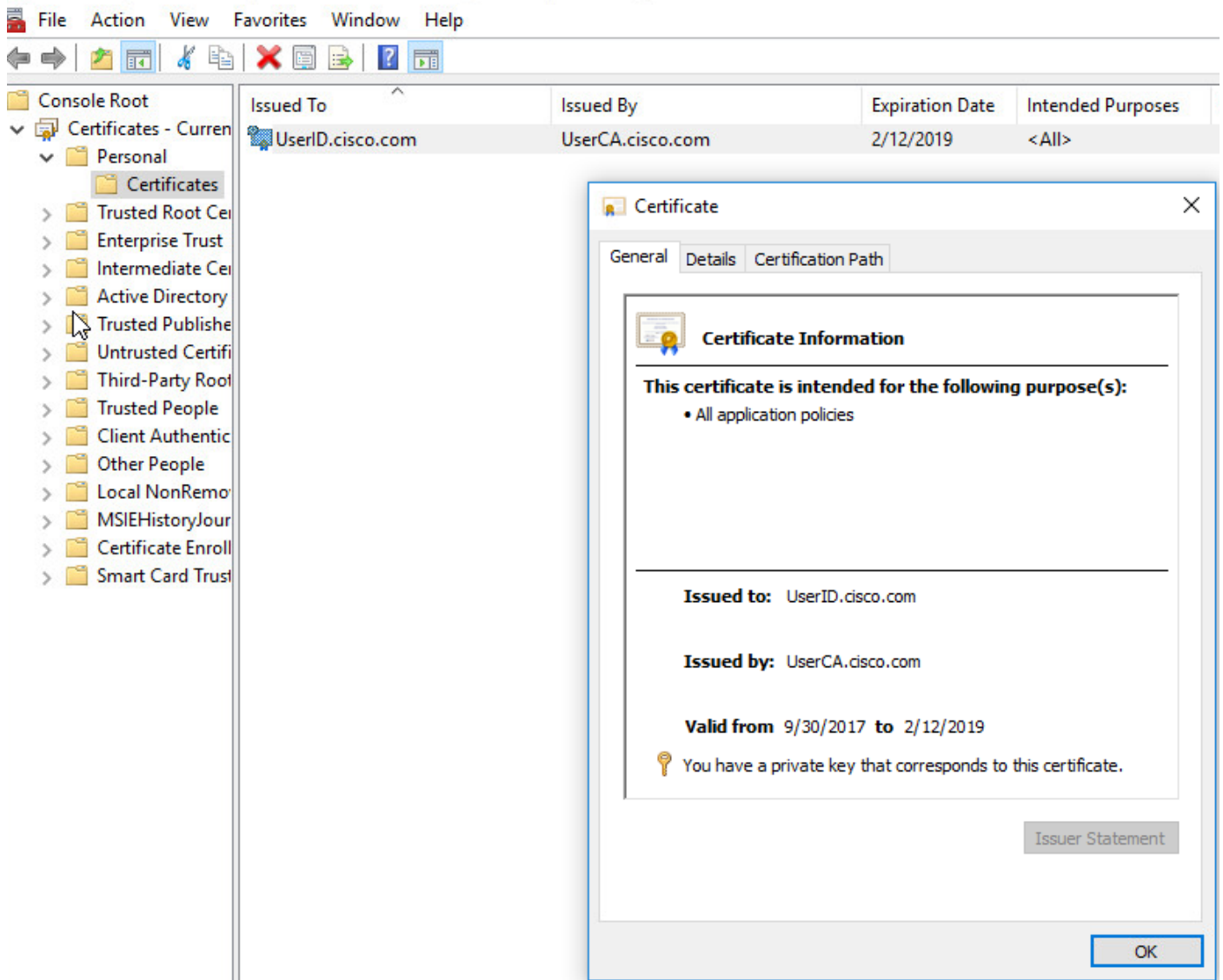
**Valid from** 10/1/2017 **to** 2/13/2019

🔑 You have a private key that corresponds to this certificate.

Issuer Statement

OK

Certificado de usuario



Ejecute este comando de verificar la conexión:

```
GCE-ASA# sh vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : MachineID.cisco.com Index : 296
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11542 Bytes Rx : 2097
Pkts Tx : 8 Pkts Rx : 29
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Grouppolicy-MCA Tunnel Group : ANYCONNECT-MCA
Login Time : 22:26:27 UTC Sun Oct 1 2017
Duration : 0h:00m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5df510012800059d16b93
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

AnyConnect-Parent:  
Tunnel ID : 296.1  
Public IP : 10.197.223.235  
Encryption : none Hashing : none  
TCP Src Port : 51609 TCP Dst Port : 443  
**Auth Mode : Multiple-certificate**  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : win  
Client OS Ver: 10.0.14393  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054  
Bytes Tx : 5771 Bytes Rx : 0  
Pkts Tx : 4 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 296.2  
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235  
Encryption : AES128 Hashing : SHA1  
Ciphersuite : AES128-SHA  
Encapsulation: TLSv1.2 TCP Src Port : 51612  
TCP Dst Port : 443 Auth Mode : Multiple-certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054  
Bytes Tx : 5771 Bytes Rx : 446  
Pkts Tx : 4 Pkts Rx : 5  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
Tunnel ID : 296.3  
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235  
Encryption : AES256 Hashing : SHA1  
Ciphersuite : AES256-SHA  
Encapsulation: DTLSv1.0 UDP Src Port : 63385  
UDP Dst Port : 443 Auth Mode : Multiple-certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054  
Bytes Tx : 0 Bytes Rx : 1651  
Pkts Tx : 0 Pkts Rx : 24  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

## Troubleshooting

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

**Note:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

**Caution:** En el ASA, usted puede fijar los diversos niveles de debug; por abandono, se utiliza el nivel 1. Si usted cambia el nivel de debug, la verbosidad de los debugs pudo aumentar. Haga esto con cautela, especialmente en los entornos de producción.

- Mensajes 127 del debug crypto ca
- Transacción 127 del debug crypto ca

CRYPTO\_PKI: Begin sorted cert chain

-----Certificate-----:

Serial: 00B6D609E1D68B9334

Subject: **cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN**

Issuer: cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO\_PKI: End sorted cert chain

CRYPTO\_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use

CRYPTO\_PKI: List pruning is not necessary.

CRYPTO\_PKI: Sorted chain size is: 1

CRYPTO\_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:

cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO\_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:

cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer\_name:

cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO\_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"

serial number=00 b6 d6 09 e1 d6 8b 93 34 | .....4

CRYPTO\_PKI: valid cert with warning.

CRYPTO\_PKI: **valid cert status.**

CRYPTO\_PKI: Begin sorted cert chain

-----Certificate-----:

Serial: 00B6D609E1D68B9334

Subject: **cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN**

Issuer: cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO\_PKI: End sorted cert chain

CRYPTO\_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use

CRYPTO\_PKI: List pruning is not necessary.

CRYPTO\_PKI: Sorted chain size is: 1

CRYPTO\_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:

cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO\_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:

cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer\_name:

cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO\_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"

serial number=00 b6 d6 09 e1 d6 8b 93 34 | .....4

CRYPTO\_PKI: valid cert with warning.

CRYPTO\_PKI: **valid cert status.**

CRYPTO\_PKI: Begin sorted cert chain

-----Certificate-----:

Serial: 00A5A42E24A345E11A

Subject: **cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN**

Issuer: cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN

CRYPTO\_PKI: End sorted cert chain

CRYPTO\_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use

CRYPTO\_PKI: List pruning is not necessary.

CRYPTO\_PKI: Sorted chain size is: 1

CRYPTO\_PKI: Found ID cert. serial number: 00A5A42E24A345E11A, subject name:

cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN

CRYPTO\_PKI: Verifying certificate with serial number: 00A5A42E24A345E11A, subject name:

```
cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN, issuer_name:
cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN, signature alg: SHA256/RSA.
```

```
CRYPTO_PKI(Cert Lookup) issuer="cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN" serial
number=00 a5 a4 2e 24 a3 45 e1 1a | ....$.E..
```

CRYPTO\_PKI: valid cert with warning.

CRYPTO\_PKI: **valid cert status.**

- **Xml 127 del agregado-auth del debug**

```
Received XML message below from the client <?xml version="1.0" encoding="UTF-8"?> <config-auth
client="vpn" type="init" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
#snip# win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<group-select>ANYCONNECT-MCA</group-select>
<group-access>https://10.197.223.81/MCA</group-access>
<capabilities>
<auth-method>single-sign-on</auth-method>
<auth-method>multiple-cert</auth-method></capabilities>
</config-auth>
```

Generated XML message below

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request" aggregate-auth-version="2">
<opaque is-for="sg">
<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>136775778</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash>
</opaque>
<multiple-client-cert-request>
<hash-algorithm>sha256</hash-algorithm>
<hash-algorithm>sha384</hash-algorithm>
<hash-algorithm>sha512</hash-algorithm>
</multiple-client-cert-request>
<random>FA4003BD87436B227####snip####C138A08FF724F0100015B863F750914839EE79C86DFE8F0B9A0199E2</r
andom>
</config-auth>
```

Received XML message below from the client

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-reply" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
##snip## win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<session-token></session-token>
<session-id></session-id>
<opaque is-for="sg">
<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>608423386</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash></opaque>
```

```
<auth>
<client-cert-chain cert-store="1M">
<client-cert-sent-via-protocol></client-cert-sent-via-protocol></client-cert-chain>
<client-cert-chain cert-store="1U">
<client-cert cert-format="pkcs7">MIIG+AYJKoZIhvcNAQcCoIIG6TCCBuU
yTCCAzwwgIkAgkApaQuJKNF4RowDQYJKoZIhvcNAQELBQAwWTELMakGAlUEBhMC
#Snip#
gSCx8Luo9V76nPjDI8PORurSFVWL9jiGJH0rLakYoGv
</client-cert>
<client-cert-auth-signature hash-algorithm-
chosen="sha512">FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJ
#snip#
EYt4G2hQ4hySySYqD4L4iV9luCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQnjMwi6D0ygT=</client-cert-auth-
signature>
</client-cert-chain>
</auth>
</config-auth>
```

Received attribute hash-algorithm-chosen in XML message from client  
Base64 Signature (len=349):

```
FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJI9aWFqdlBbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV9luCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
ABXv++cN71NwGHK91EAvNRcpCX4TdZ+6ZKpL4sClu8vZJew2jwGmPnYesG3sttrS
TFBRqg74+1TFSbUuIEzn8MLXZqHbOnA19B9gyXZJon8eh3Z7cDspFir0xKBu8iYH
L+ES84UNTdQjatIN4Eis8SD/5QPAunCyvAUBvK5FZ4c4TpnF6MIEPhjMwi6D0ygT
sm2218mstLDNKBouaTjB3A==
```

Successful Base64 signature decode, len 256

Loading cert into PKI

Waiting for certificate validation result

Verifying signature

**Successfully verified signature**

- **SSL 127 del agregado-auth del debug**

```
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-no-cert: Client has not sent a certificate
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-no-cert: Resolve tunnel group (ANYCONNECT-MCA) alias (NULL) Cert or URL mapped YES
INIT-no-cert: Client advertised multi-cert authentication support
[332565382] Created auth info for client 10.197.223.235
[332565382] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-no-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
[332565382] Generating multiple certificate request
[332565382] Saved message of len 699 to verify signature
rcode from handler = 0
Sending response
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-cert: Client has certificate, groupSelect ANYCONNECT-MCA
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-cert: Found tunnel group (ANYCONNECT-MCA) alias (NULL) url or certmap YES
INIT-cert: Client advertised multi-cert authentication support
[462466710] Created auth info for client 10.197.223.235
[462466710] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
Resetting FCADB entry
[462466710] Generating multiple certificate request
[462466710] Saved message of len 741 to verify signature
rcode from handler = 0
```

Sending response  
/CSCOSSLC/config-auth  
Processing client request  
XML successfully parsed  
Processing request (auth-reply)  
auth-reply:[462466710] searching for authinfo  
[462466710] Found auth info for client 10.197.223.235, update expire timer (3 mins)  
Found tunnel group (ANYCONNECT-MCA) alias ANYCONNECT-MCA  
[462466710] Multi cert authentication  
[462466710] **First cert came in SSL protocol, len 891**  
[462466710] Success loading cert into PKI  
[462466710] **Authenticating second cert**  
[462466710] Sending Message AGGAUTH\_MSG\_AUTHENTICATE\_CERT(1)  
[462466710] Fiber waiting  
Aggauth Message handler received message AGGAUTH\_MSG\_AUTHENTICATE\_CERT  
[462466710] Process certificate authentication request  
[462466710] Waiting for async certificate verification  
[462466710] Verify cert callback  
[462466710] **Certificate Authentication success - verifying signature**  
[462466710] Signature verify success  
[462466710] Signalling fiber  
[462466710] Fiber continuing  
[462466710] Found auth info  
[462466710] Resolved tunnel group (ANYCONNECT-MCA), Cert or URL mapped YES  
Resetting FCADB entry  
Attempting cert only login  
Authorization username = MachineID.cisco.com  
Opened AAA handle 335892526  
Making AAA request  
AAA request finished  
Send auth complete  
rcode from handler = 0  
Sending response  
Closing AAA handle 335892526  
[462466710] Destroy auth info for 10.197.223.235  
[462466710] Free auth info for 10.197.223.235

## Información Relacionada

- [Release Note para la serie de Cisco ASA, 9.7\(x\)](#)
- [Guía del administrador del Cliente de movilidad Cisco AnyConnect Secure, versión 4.4](#)
- [Guía de Troubleshooting del cliente VPN de AnyConnect - Problemas comunes](#)
- [Soporte técnico y documentación](#)