

將ASA配置為使用基於多證書的身份驗證的AnyConnect客戶端的SSL網關

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制](#)

[Windows v/s非Windows平台上的證書選擇](#)

[多證書身份驗證的連線流](#)

[設定](#)

[通過ASDM配置多證書身份驗證](#)

[通過CLI為多證書身份驗證配置ASA](#)

[驗證](#)

[通過CLI檢視ASA上安裝的證書](#)

[檢視客戶端上安裝的證書](#)

[電腦證書](#)

[使用者證書](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何將自適應安全裝置(ASA)配置為使用基於多證書身份驗證的Cisco AnyConnect安全移動客戶端的安全套接字層(SSL)網關。

必要條件

需求

思科建議您瞭解以下主題：

- ASA CLI配置和SSL VPN配置的基本知識
- X509證書的基本知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Adaptive Security Appliance(ASA)軟體9.7(1)版及更高版本
- 採用Cisco AnyConnect安全行動化使用者端的Windows 10 4.4

附註：從Cisco [Software Download](#) (僅限註冊客戶) 下載AnyConnect VPN客戶端軟體包 (anyconnect-win*.pkg)。將AnyConnect VPN客戶端複製到ASA的快閃記憶體，該快閃記憶體將下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。有關詳細資訊，請參閱ASA配置指南的[安裝AnyConnect客戶端](#)部分。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

在軟體版本9.7(1)之前，ASA支援基於單個證書的身份驗證，這意味著使用者或電腦可以進行身份驗證，但不能同時進行身份驗證，用於一次連線嘗試。

基於多重證書的身份驗證除了驗證使用者的身份證書以允許VPN訪問外，還能夠讓ASA驗證電腦或裝置證書，以確保裝置是公司頒發的裝置。

限制

- 多個證書身份驗證當前將證書數量限制為正好兩個。
- AnyConnect客戶端必須表示支援多證書身份驗證。如果情況並非如此，則網關使用傳統身份驗證方法之一或連線失敗。AnyConnect版本4.4.1或更04030版本支援基於多證書的身份驗證。
- 對於Windows平台，電腦證書在初始SSL握手期間傳送，隨後在聚合身份驗證協定下傳送使用者證書。不支援來自Windows電腦儲存區的兩個證書。
- 多證書身份驗證會忽略XML配置檔案下的**Enable automatic Certificate Selection**首選項，這意味著客戶端嘗試所有組合以驗證兩個證書，直到失敗。這可能會在Anyconnect嘗試連線時造成相當的延遲。因此，如果客戶端電腦上存在多個使用者/電腦證書，建議使用證書匹配。
- Anyconnect SSL VPN僅支援基於RSA的證書。
- 在彙總身份驗證期間，僅支援基於SHA256、SHA384和SHA512的證書。

Windows v/s非Windows平台上的證書選擇

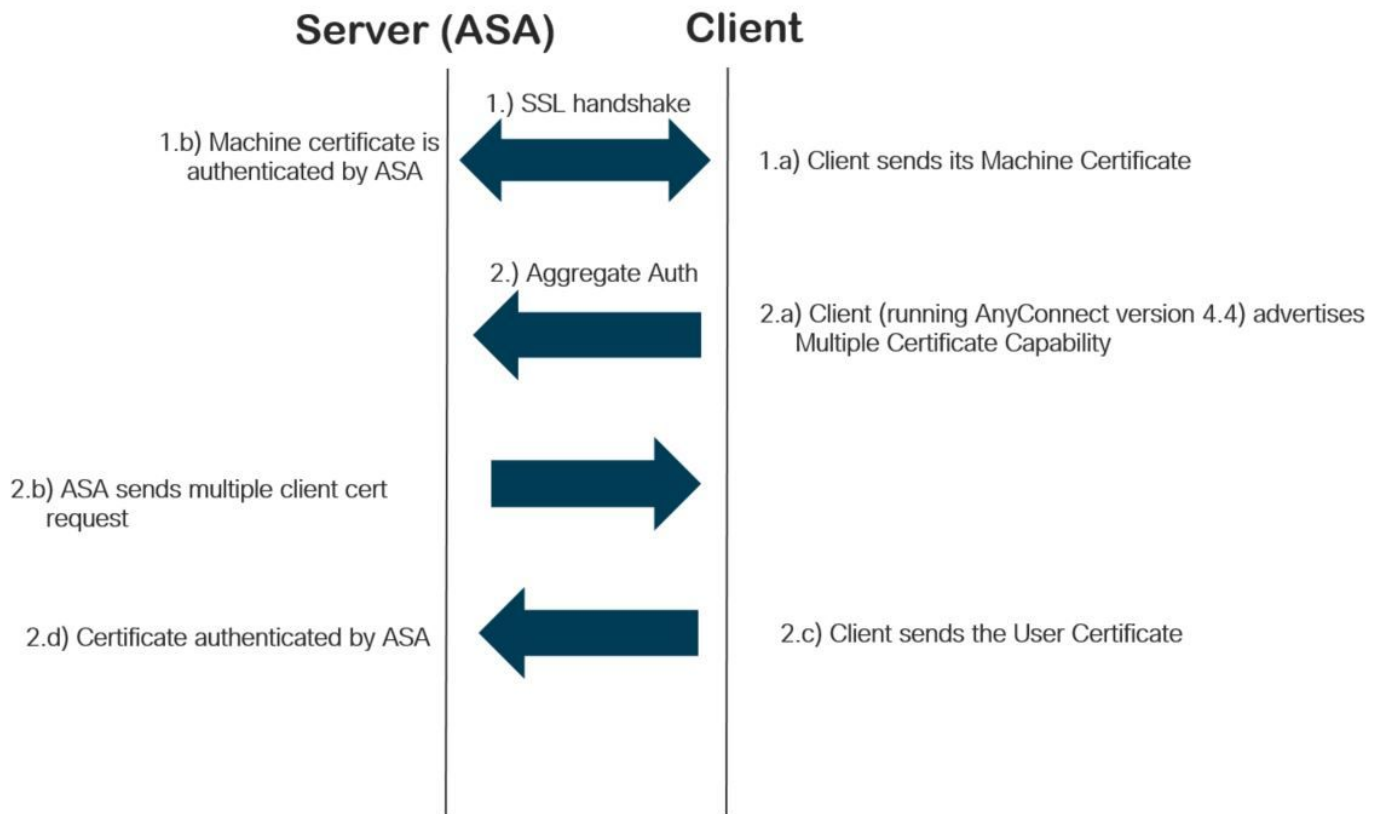
Windows上的AnyConnect區分從電腦儲存區 (只能由特權進程訪問) 和使用者儲存區 (只能由登入使用者擁有的進程訪問) 檢索的證書。非Windows平台上的AnyConnect沒有這種區別。

ASA可以根據收到的實際證書型別選擇強制實施由ASA管理員配置的連線策略。對於Windows，型別可以是：

- 一台機器和一個使用者，或者
- 兩個使用者。

對於非Windows平台，指示始終為兩個使用者證書。

多證書身份驗證的連線流



設定

通過ASDM配置多證書身份驗證

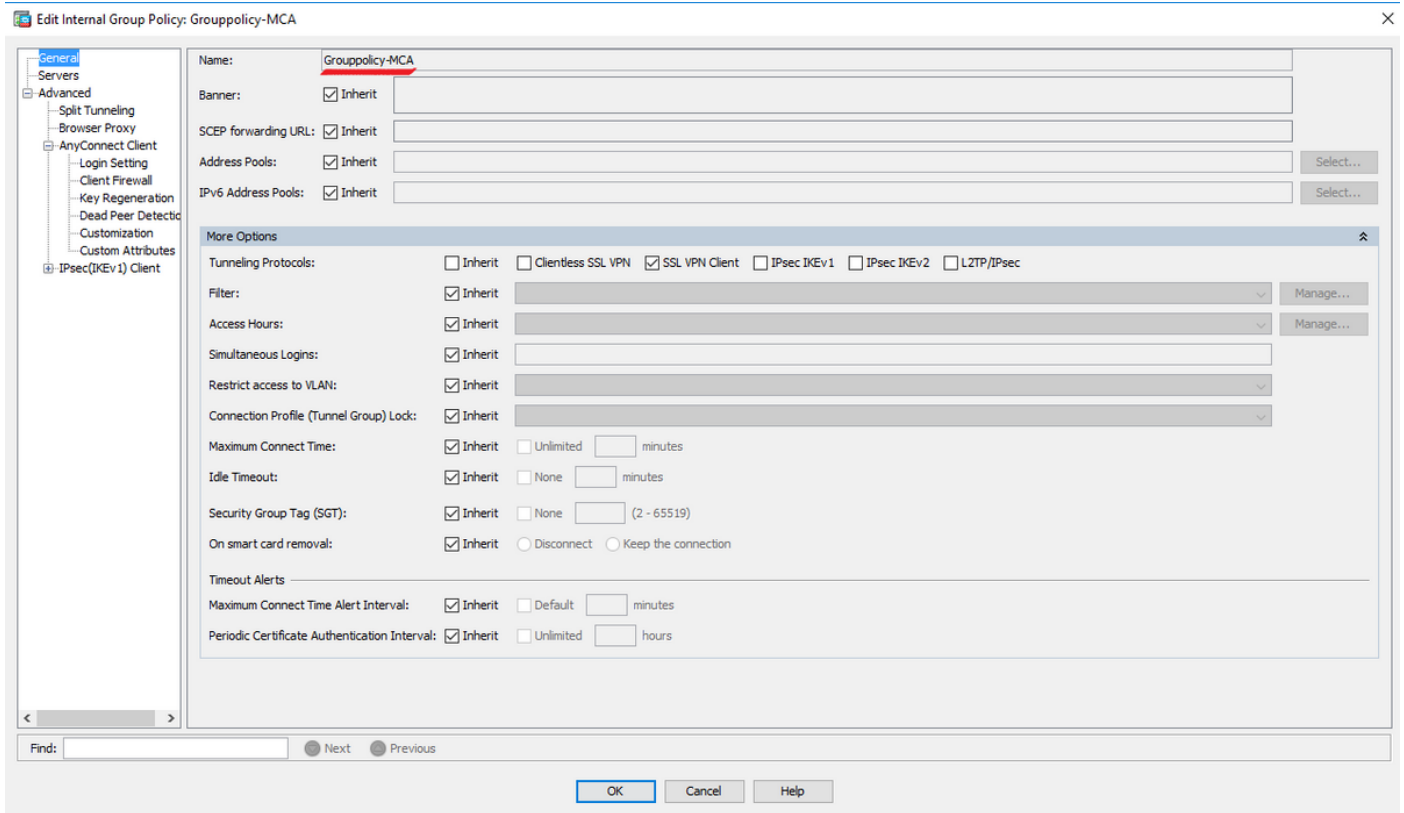
本節介紹如何將Cisco ASA配置為使用多證書身份驗證的AnyConnect客戶端的SSL網關。

通過ASDM完成以下步驟，為多證書身份驗證設定Anyconnect客戶端：

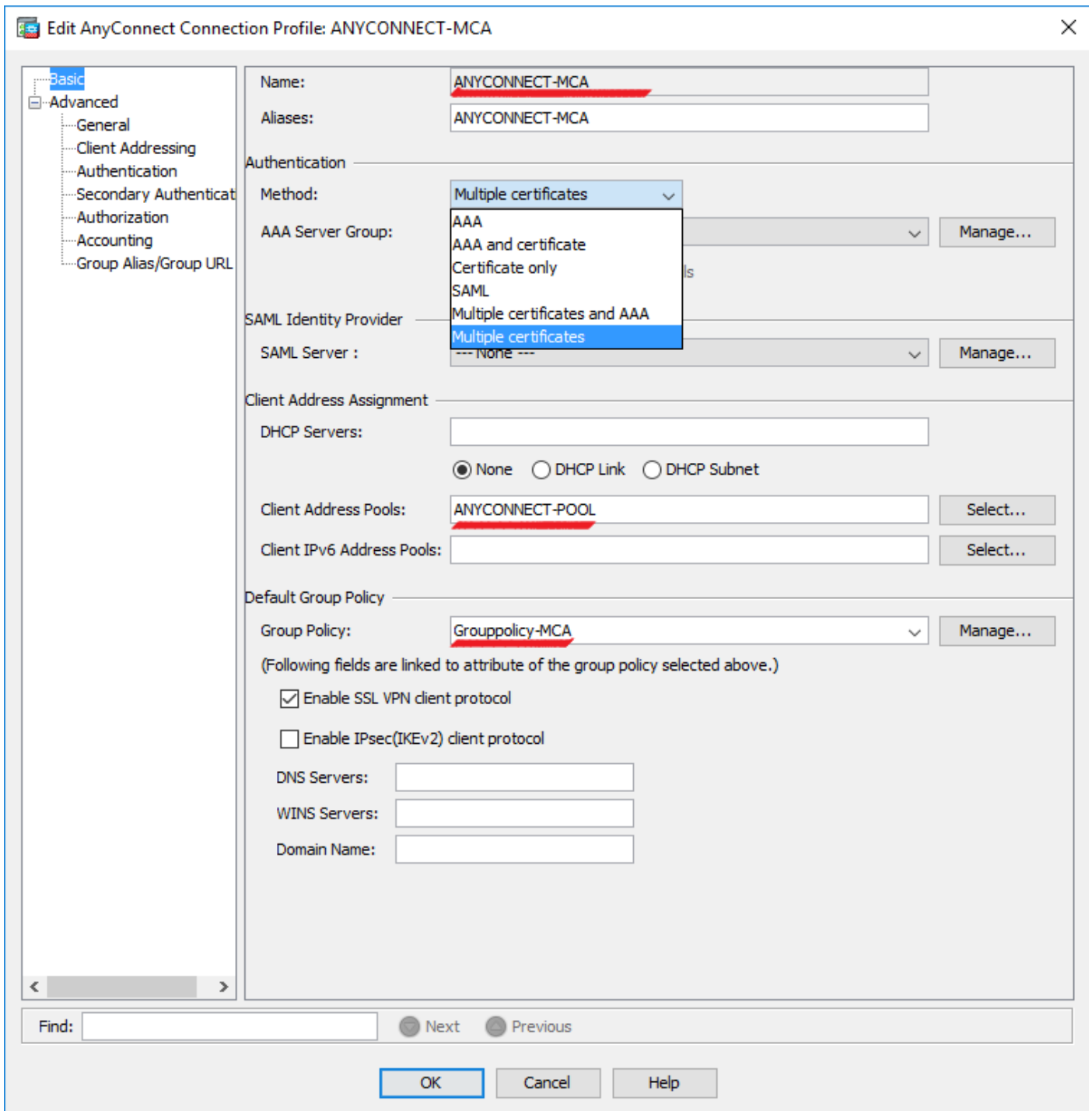
步驟1.在ASA上安裝使用者和電腦證書的CA證書。

有關證書的安裝，請參閱[配置ASA:安裝和更新 SSL 數位憑證](#)

步驟2.導航到Configuration > Remote Access > Group Policy並配置組策略。



步驟3. 配置新的連線配置檔案並選擇**Authentication Method**作為多個證書，然後選擇步驟1中建立的組策略。



步驟4.有關其他詳細配置，請參閱VPN客戶端和AnyConnect客戶端訪問本地LAN配置示例

通過CLI為多證書身份驗證配置ASA

附註：使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

附註： [輸出直譯器工具](#) (僅供已註冊客戶使用) 支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

通過CLI檢視ASA上安裝的證書

show crypto ca certificate

```
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

檢視客戶端上安裝的證書

若要驗證安裝，請使用憑證管理員(certmgr.msc):

電腦證書

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...

Console Root

- Certificates (Local C)
 - Personal
 - Certificates
 - Trusted Root Certificates
 - Enterprise Trust
 - Intermediate Certificates
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certificates
 - Trusted People
 - Client Authentication
 - Preview Build Root Certificates
 - AAD Token Issuers
 - Other People
 - Homegroup Master Keys
 - Local Non-Removable Certificates
 - MSIEHistoryJournals
 - Remote Desktop
 - Certificate Enrollment
 - Smart Card Trust
 - Trusted Devices
 - Windows Live ID

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

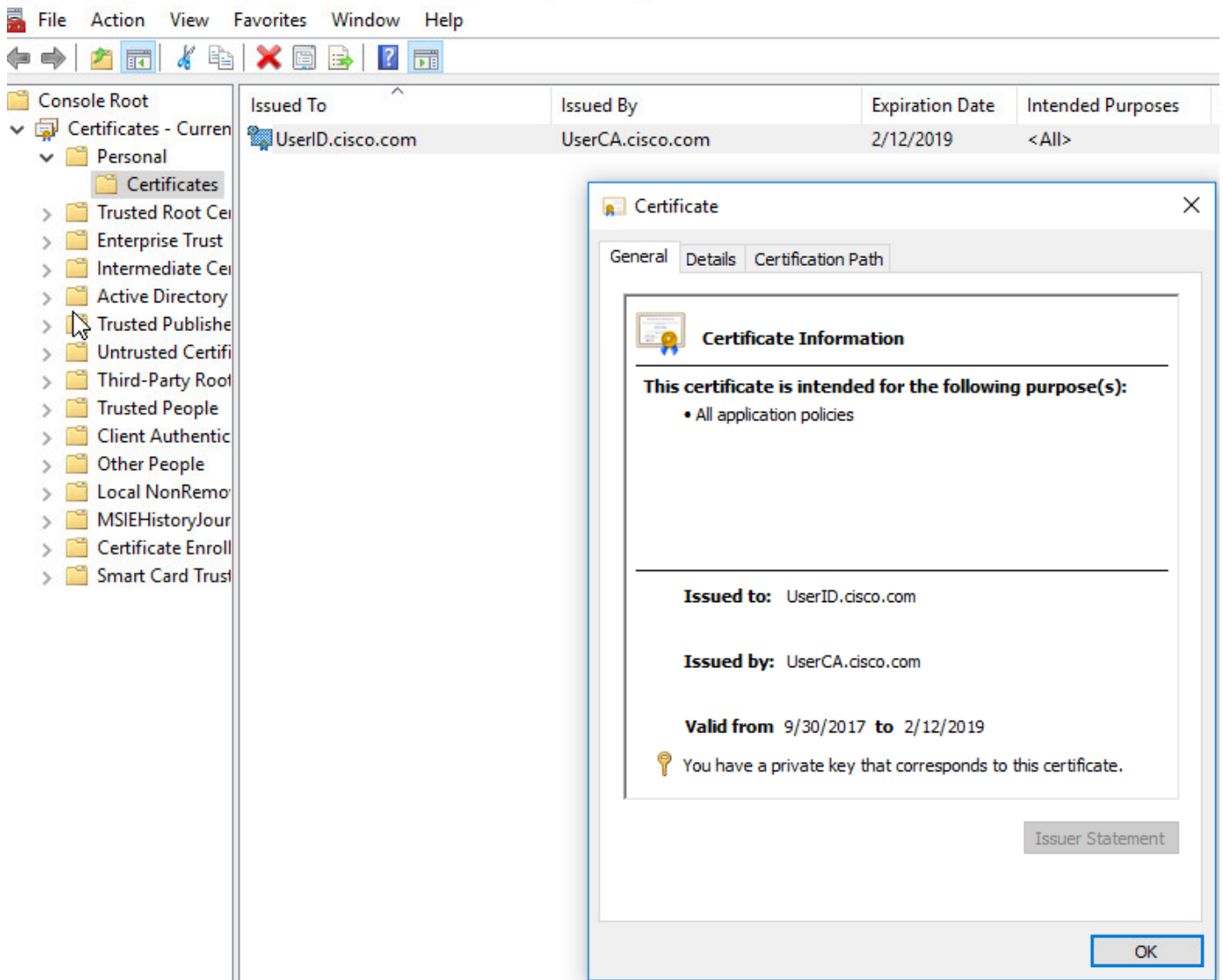
Valid from 10/1/2017 **to** 2/13/2019

 You have a private key that corresponds to this certificate.

Issuer Statement

OK

使用者證書



執行以下命令驗證連線：

```
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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

注意：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中。

- Debug crypto ca messages 127

• Debug crypto ca transaction 127

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.**

• Debug aggregate-auth xml 127

```
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</random>
</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
yTCCAzwggIkAgkApaQuJKNF4RowDQYJKoZIhvcNAQELBQAwWTELMakGA1UEBhMC
#Snip#
gSCx8Luo9V76nPjDI8PORurSFVWL9jiGJH0rLakYoGv
</client-cert>
<client-cert-auth-signature hash-algorithm-
chosen="sha512">FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJ
#snip#
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQnjMwi6D0ygT=</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+G5u2Phr4fJI9aWFqd1BbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
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

- **Debug aggregate-auth ssl 127**

```
/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
```

相關資訊

- [Cisco ASA系列9.7\(x\)版本說明](#)
- [Cisco AnyConnect安全移動客戶端管理員指南4.4版](#)
- [AnyConnect VPN客戶端故障排除指南 — 常見問題](#)
- [技術支援與檔案](#)