

다중 인증서 기반 인증을 사용하여 ASA를 AnyConnect 클라이언트에 대한 SSL 게이트웨이로 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[제한 사항](#)

[Windows v/s 비 Windows 플랫폼에서 인증서 선택](#)

[다중 인증서 인증을 위한 연결 흐름](#)

[구성](#)

[ASDM을 통한 다중 인증서 인증 구성](#)

[CLI를 통한 다중 인증서 인증을 위해 ASA 구성](#)

[다음을 확인합니다.](#)

[CLI를 통해 ASA에 설치된 인증서 보기](#)

[클라이언트에 설치된 인증서 보기](#)

[머신 인증서](#)

[사용자 인증서](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 ASA(Adaptive Security Appliance)를 다중 인증서 기반 인증을 사용하는 Cisco AnyConnect Secure Mobility Client용 SSL(Secure Sockets Layer) 게이트웨이로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항


다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA CLI 컨피그레이션 및 SSL VPN 컨피그레이션에 대한 기본 지식
- X509 인증서에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 소프트웨어, 버전 9.7(1) 이상
- Windows 10(Cisco AnyConnect Secure Mobility Client 4.4 포함)

 참고: Cisco [Software Download](#)([등록된](#) 고객만)에서 AnyConnect VPN 클라이언트 패키지 (anyconnect-win*.pkg)를 다운로드합니다. ASA와의 SSL VPN 연결을 설정하기 위해 원격 사용자 컴퓨터에 다운로드할 ASA의 플래시 메모리에 AnyConnect VPN 클라이언트를 복사합니다. 자세한 내용은 ASA [컨피그레이션 가이드](#)의 Installing the AnyConnect Client(AnyConnect 클라이언트 설치) 섹션을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

소프트웨어 버전 9.7(1) 이전에는 ASA가 단일 인증서 기반 인증을 지원하므로 단일 연결 시도에 대해 사용자 또는 머신 중 하나만 인증할 수 있습니다.

다중 인증서 기반 인증은 VPN 액세스를 허용하기 위해 사용자의 ID 인증서를 인증하는 것 외에도 ASA에서 머신 또는 디바이스 인증서를 검증하여 디바이스가 기업 발급 디바이스인지 확인하는 기능을 제공합니다.

제한 사항

- 여러 인증서 인증은 현재 인증서 수를 정확히 2개로 제한합니다.
- AnyConnect 클라이언트는 여러 인증서 인증에 대한 지원을 나타내야 합니다. 그렇지 않으면 게이트웨이가 레거시 인증 방법 중 하나를 사용하거나 연결에 실패합니다. AnyConnect 버전 4.4.04030 이상은 다중 인증서 기반 인증을 지원합니다.
- Windows 플랫폼의 경우 초기 SSL 핸드셰이크 중에 머신 인증서가 전송되며 그 뒤에 Aggregate auth 프로토콜 아래의 User Certificate가 옵니다.Windows Machine Store의 두 인증서는 지원되지 않습니다.
- 다중 인증서 인증에서는 XML 프로파일 아래의 Enable automatic Certificate Selection(자동 인증서 선택 활성화) 환경 설정을 무시합니다. 즉, 클라이언트가 실패할 때까지 모든 조합을 시도하여 두 인증서를 모두 인증합니다. 이로 인해 Anyconnect가 연결을 시도하는 동안 상당한 지연이 발생할 수 있습니다. 따라서 클라이언트 컴퓨터에 여러 사용자/머신 인증서가 있는 경우 인증서 일치를 사용하는 것이 좋습니다.
- Anyconnect SSL VPN은 RSA 기반 인증서만 지원합니다.
- 집계 인증 중에는 SHA256, SHA384 및 SHA512 기반 인증서만 지원됩니다.

Windows v/s 비 Windows 플랫폼에서 인증서 선택

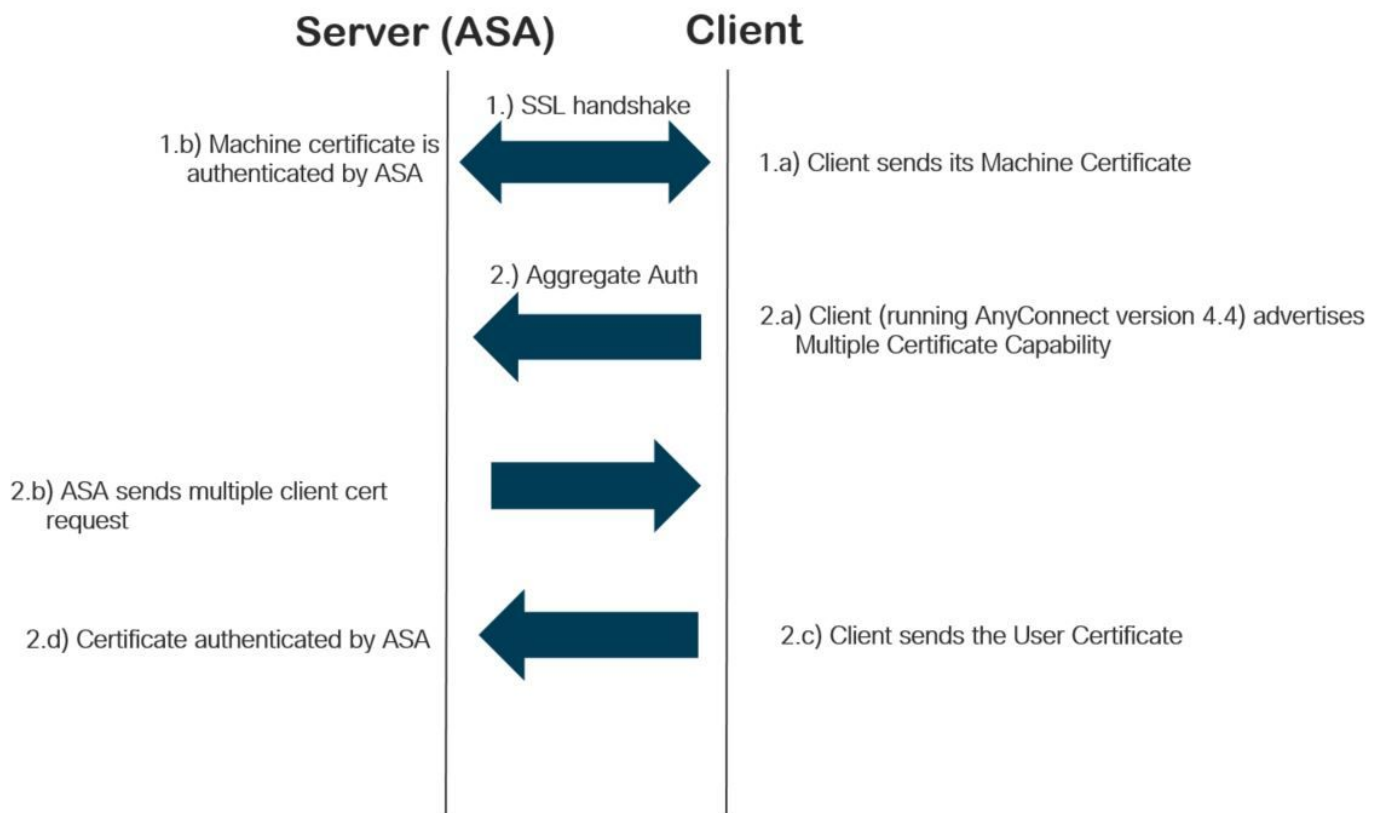
Windows의 AnyConnect는 컴퓨터 저장소(권한이 있는 프로세스에서만 액세스 가능)에서 검색된 인증서와 사용자 저장소(로그인한 사용자가 소유한 프로세스에서만 액세스 가능)를 구별합니다. Windows 이외의 플랫폼에서는 AnyConnect가 그러한 구분을 하지 않습니다.

ASA는 수신된 인증서의 실제 유형을 기반으로 ASA 관리자가 구성한 연결 정책을 시행하도록 선택할 수 있습니다. Windows의 경우 유형은 다음과 같을 수 있습니다.

- 단일 시스템 및 단일 사용자 또는
- 사용자 2명

비 Windows 플랫폼의 경우 표시는 항상 두 개의 사용자 인증서입니다.

다중 인증서 인증을 위한 연결 흐름



구성

ASDM을 통한 다중 인증서 인증 구성

이 섹션에서는 Cisco ASA를 다중 인증서 인증을 사용하는 AnyConnect 클라이언트에 대한 SSL 게이트웨이로 구성하는 방법에 대해 설명합니다.

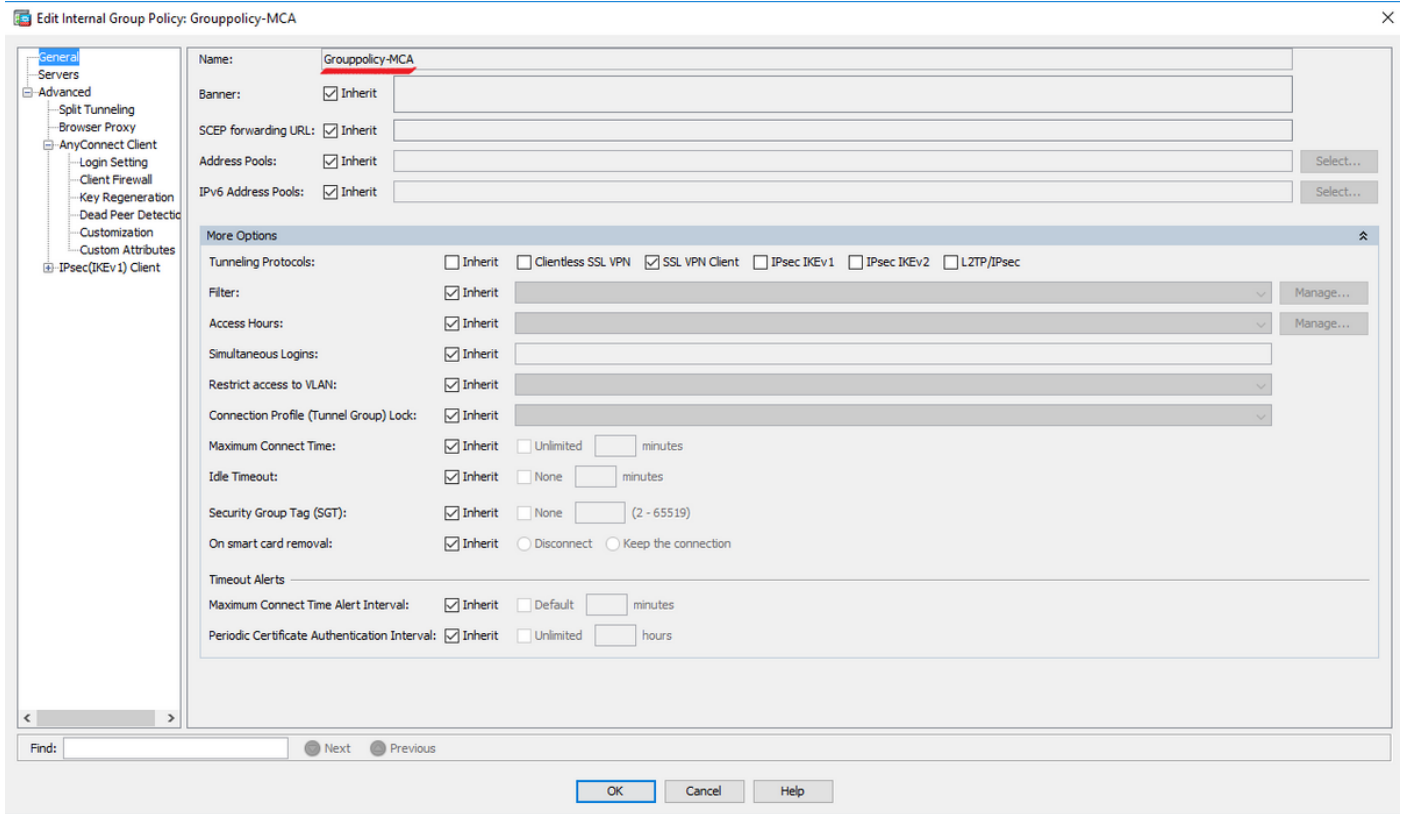
ASDM을 통해 다음 단계를 완료하여 다중 인증서 인증을 위한 Anyconnect 클라이언트를 설정합니

다.

1단계. ASA에 사용자 및 머신 인증서용 CA 인증서를 설치합니다.

인증서 설치에 대해서는 [ASA 구성: SSL 디지털 인증서 설치 및 갱신을 참조하십시오](#)

2단계. Configuration(컨피그레이션) > Remote Access(원격 액세스) > Group Policy(그룹 정책)로 이동하고 Group-Policy(그룹 정책)를 구성합니다.



3단계. 새 연결 프로파일을 구성하고 Authentication Method as Multiple Certificates를 선택하고 1단계에서 생성한 Group-Policy를 선택합니다.

The screenshot shows the 'Edit AnyConnect Connection Profile: ANYCONNECT-MCA' window. The left sidebar has 'Advanced' expanded, with 'Authentication' selected. The main area shows the following configuration:

- Name:** ANYCONNECT-MCA
- Aliases:** ANYCONNECT-MCA
- Authentication Method:** Multiple certificates (dropdown menu is open showing options: AAA, AAA and certificate, Certificate only, SAML, Multiple certificates and AAA, Multiple certificates, ---None---
- AAA Server Group:** [Empty] Manage...
- SAML Identity Provider:** Multiple certificates and AAA
- SAML Server:** ---None--- Manage...
- Client Address Assignment:**
 - DHCP Servers:** [Empty]
 - None** (selected), DHCP Link, DHCP Subnet
 - Client Address Pools:** ANYCONNECT-POOL Select...
 - Client IPv6 Address Pools:** [Empty] Select...
- Default Group Policy:**
 - Group Policy:** Grouppolicy-MCA Manage...
 - (Following fields are linked to attribute of the group policy selected above.)
 - Enable SSL VPN client protocol
 - Enable IPsec(IKEv2) client protocol
 - DNS Servers:** [Empty]
 - WINS Servers:** [Empty]
 - Domain Name:** [Empty]

At the bottom, there is a 'Find:' field, 'Next' and 'Previous' buttons, and 'OK', 'Cancel', and 'Help' buttons.

4단계. 기타 자세한 컨피그레이션은 로컬 [LAN 컨피그레이션에 대한 VPN 클라이언트 및 AnyConnect 클라이언트 액세스 예](#)를 참조하십시오

CLI를 통한 다중 인증서 인증을 위해 ASA 구성

참고: 이 섹션에서 사용된 [명령어](#)에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)(등록된 고객만 해당)을 사용하십시오.

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 out

!

!

TrustPoint for User CA certificate

crypto ca trustpoint UserCA

enrollment terminal

cr1 configure

!

!

Trustpoint for Machine CA certificate

crypto ca trustpoint MachineCA

enrollment terminal

cr1 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
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

 참고: Output [Interpreter Tool](#)([등록된](#) 고객만 해당)은 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

CLI를 통해 ASA에 설치된 인증서 보기

crypto ca 인증서 표시

<#root>

```
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

클라이언트에 설치된 인증서 보기

설치를 확인하려면 인증서 관리자(certmgr.msc)를 사용하십시오.

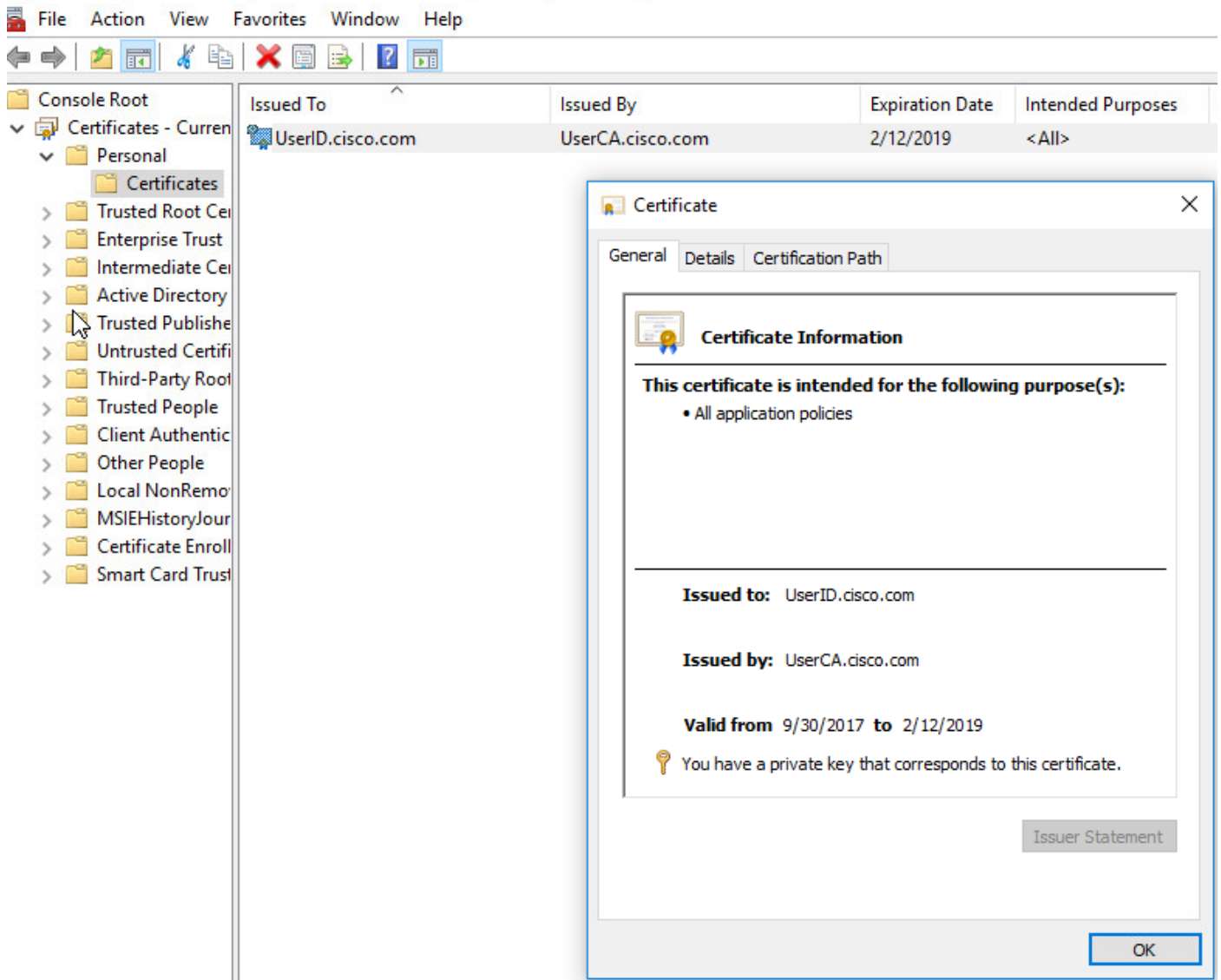
머신 인증서

The screenshot shows the Windows Certificate Manager console. The left pane displays the 'Certificates (Local Computer)' tree with 'Personal' > 'Certificates' selected. The main pane shows a table of certificates:

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

An 'Certificate' dialog box is open, showing the 'Details' tab. The 'Certificate Information' section states: 'This certificate is intended for the following purpose(s):' followed by a bulleted list: 'Ensures the identity of a remote computer' and 'Proves your identity to a remote computer'. Below this, it lists: 'Issued to: MachineID.cisco.com', 'Issued by: MachineCA.cisco.com', and 'Valid from 10/1/2017 to 2/13/2019'. A note at the bottom says: 'You have a private key that corresponds to this certificate.' There are 'Issuer Statement' and 'OK' buttons.

사용자 인증서



이 명령을 실행하여 연결을 확인합니다.

<#root>

```
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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

 참고: debug 명령을 사용하기 [전에 Debug 명령](#)에 대한 중요 정보를 참조하십시오.

 주의: ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

- Debug crypto ca messages(암호화 ca 메시지 디버그) 127
- Debug crypto ca transaction 127

<#root>

```
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=C
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name: cn=MachineID.ci
```

```
CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN" serial nu
```

```
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=C
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name: cn=MachineID.ci
```

```
CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN" serial number=00000000000000000000
```

```
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
```

```
CRYPTO_PKI(Cert Lookup) issuer="cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN" serial number=00A5A42E24A345E11A
```

```
CRYPTO_PKI: valid cert with warning.
```

```
CRYPTO_PKI:
```

```
valid cert status.
```

- 디버그 집계 인증 xml 127

```
<#root>
```

```
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<
```

```
<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## w  
    <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">FIYur1Dzb4VPTThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4
#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):
FIYur1Dzb4VPTThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJI9aWFqd1BbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
ABXv++cN71NWGHK91EAvNRcpCX4TdZ+6ZKpL4sClu8vZJew2jwGmPnYesG3sttrS
TFBRqg74+1TFSbUuIEzn8MLXZqHbOnA19B9gyXZJ on8eh3Z7cDspFiR0xKBu8iYH
L+ES84UNtDQjatIN4EiS8SD/5QPAunCyvAUBvK5FZ4c4TpnF6MIEPhjMwi6D0ygT
sm2218mstLDNK BouaTjB3A==
Successful Base64 signature decode, len 256
Loading cert into PKI
Waiting for certificate validation result
Verifying signature

Successfully verified signature

```

- 디버그 집계 인증 ssl 127

```
<#root>
```

```

/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_ATHENTICATE_CERT(1)
[462466710] Fiber waiting
Aggauth Message handler received message AGGAUTH_MSG_ATHENTICATE_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

관련 정보

- [Cisco ASA Series 릴리스 정보, 9.7\(x\)](#)
- [Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.4](#)

- [AnyConnect VPN 클라이언트 문제 해결 가이드 - 일반 문제](#)
- [기술 지원 및 문서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.