RAVPN에 대해 FTD에서 다중 인증서 인증 구성

목차

소개

이 문서에서는 FMC에서 관리하는 FTD(Firepower Threat Defense)에서 Secure Client에 대해 다중 인증서 인증을 사용하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RAVPN(Remote Access VPN)에 대한 기본적인 이해
- FMC(Firepower 관리 센터) 경험
- X509 인증서에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 11(Cisco Secure Client 5.1.4.74 포함)

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

배경 정보

소프트웨어 버전 7.0 이전의 FTD는 단일 인증서 기반 인증을 지원합니다. 즉, 단일 연결 시도에서 사용자 또는 머신 중 하나만 인증할 수 있습니다.

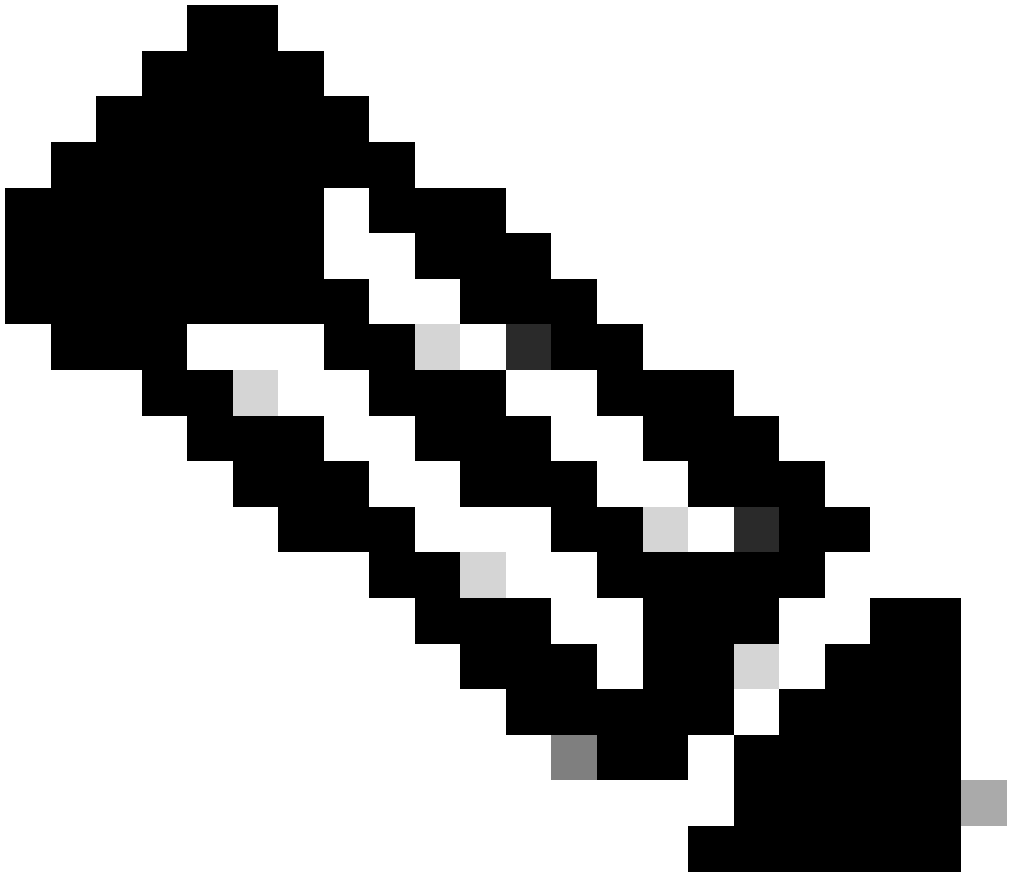
다중 인증서 기반 인증은 SSL 또는 IKEv2 EAP 단계에서 Secure Clientfor VPN 액세스를 허용하기 위해 사용자 ID 인증서를 인증하는 것 외에도 위협 방어가 머신 또는 디바이스 인증서를 검증하여 디바이스가 기업에서 발급한 디바이스인지 확인하는 기능을 제공합니다.

다중 인증서 인증은 현재 인증서 수를 2개로 제한합니다. 보안 클라이언트는 다중 인증서 인증에 대한 지원을 나타내야 합니다. 그렇지 않으면 게이트웨이가 레거시 인증 방법 중 하나를 사용하거나 연결에 실패합니다.Secure Clientversion 4.4.04030 이상은 다중 인증서 기반 인증을 지원합니다.

설정

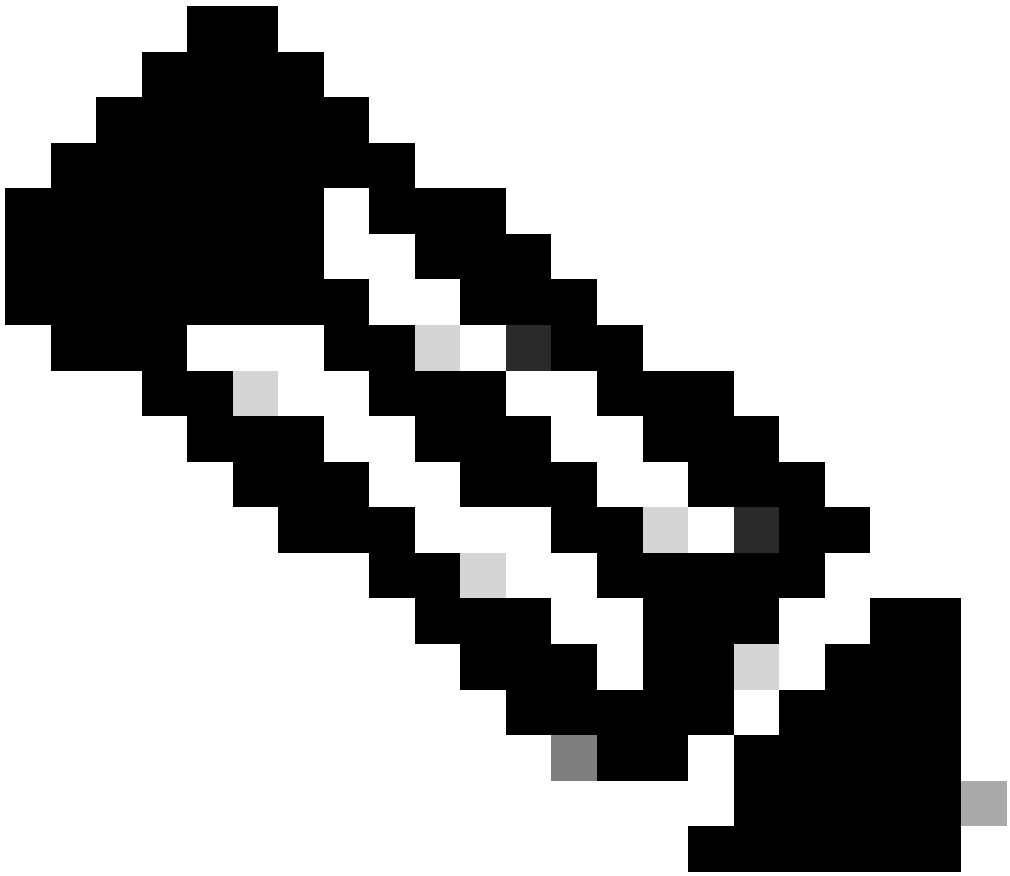
FTD의 컨피그레이션

1. Devices(디바이스) > VPN(VPN) > Remote Access(원격 액세스)로 이동합니다.
2. Remote Access VPN(원격 액세스 VPN) 정책을 선택하고 Edit(수정)를 클릭합니다.



참고: 원격 액세스 VPN을 구성하지 않은 경우 Add를 클릭하여 새 원격 액세스 VPN 정책을 만듭니다.

3. 여러 인증서 인증을 구성하려면 Connection Profile(연결 프로파일)을 선택하고 편집합니다.
4. AAA settings(AAA 설정)를 클릭하고 Authentication Method(인증 방법) as Client Certificate Only(클라이언트 인증서 전용) 또는 Client Certificate & AAA(클라이언트 인증서 및 AAA)를 선택합니다.



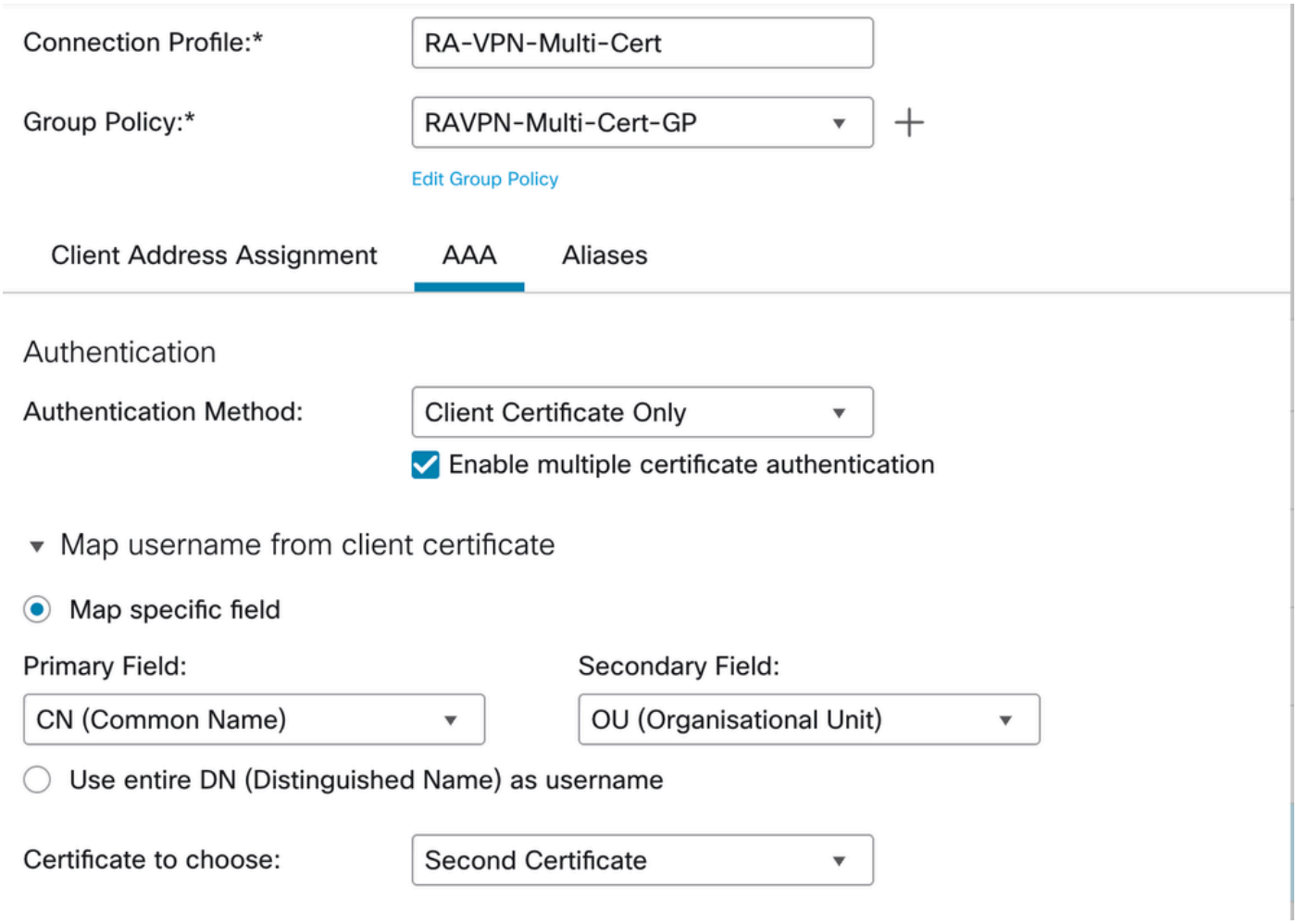
참고: 클라이언트 인증서 및 AAA 인증 방법을 선택한 경우 인증 서버를 선택합니다.

5. Enable multiple certificate authentication(다중 인증서 인증 활성화) 확인란을 선택합니다.
6. 클라이언트 인증서에서 사용자 이름을 매핑 할 인증서 중 하나를 선택 합니다.

- First Certificate(첫 번째 인증서) - VPN 클라이언트에서 보낸 머신 인증서의 사용자 이름을 매핑하려면 이 옵션을 선택합니다.
- Second Certificate(두 번째 인증서) - 클라이언트에서 보낸 사용자 인증서의 사용자 이름을 매핑하려면 이 옵션을 선택합니다.

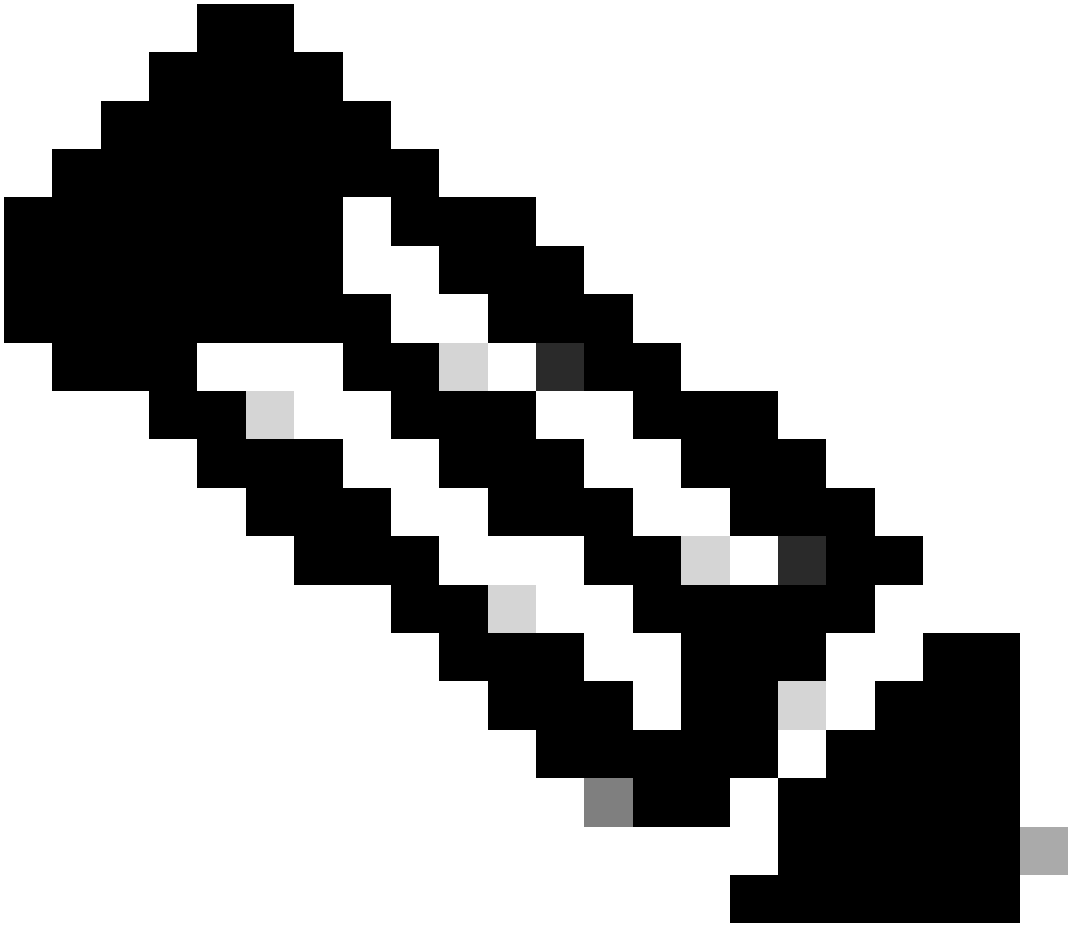
클라이언트에서 보낸 사용자 이름은 인증서 전용 인증이 활성화된 경우 VPN 세션 사용자 이름으로 사용됩니다. AAA 및 인증서 인증이 활성화된 경우 VPN 세션 사용자 이름은 Prefill 옵션을 기반으로 합니다.

7. 클라이언트 인증서의 사용자 이름을 포함하는 Map specific(특정 필드 매핑) 옵션을 선택하면 Primary(기본) 필드와 Secondary(보조) 필드에 기본값이 각각 CN(공용 이름)과 OU(조직 단위)로 표시됩니다.



연결 프로파일의 AAA 설정

8. Use entire Distinguished Name (DN) as usernameoption(전체 DN(고유 이름)을 usernameoption으로 사용)을 선택하면 시스템은 자동으로 사용자 ID를 검색합니다. DN은 사용자를 연결 프로파일에 일치시킬 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 고급 인증서 인증에 사용됩니다.



참고: Client Certificate & AAA authentication(클라이언트 인증서 및 AAA 인증)을 선택한 경우 Prefill username from certificate on user login window(사용자 로그인 창의 인증서에서 사용자 이름 미리 채우기) 옵션을 선택하여 사용자가 Cisco Secure Client의 Secure Client VPN 모듈을 통해 연결할 때 클라이언트 인증서에서 보조 사용자 이름을 미리 채웁니다.

로그인 창에서 사용자 이름 숨기기: 보조 사용자 이름은 클라이언트 인증서에서 미리 채워지지만 사용자가 미리 채워진 사용자 이름을 수정하지 않도록 사용자에게 숨겨집니다.

---

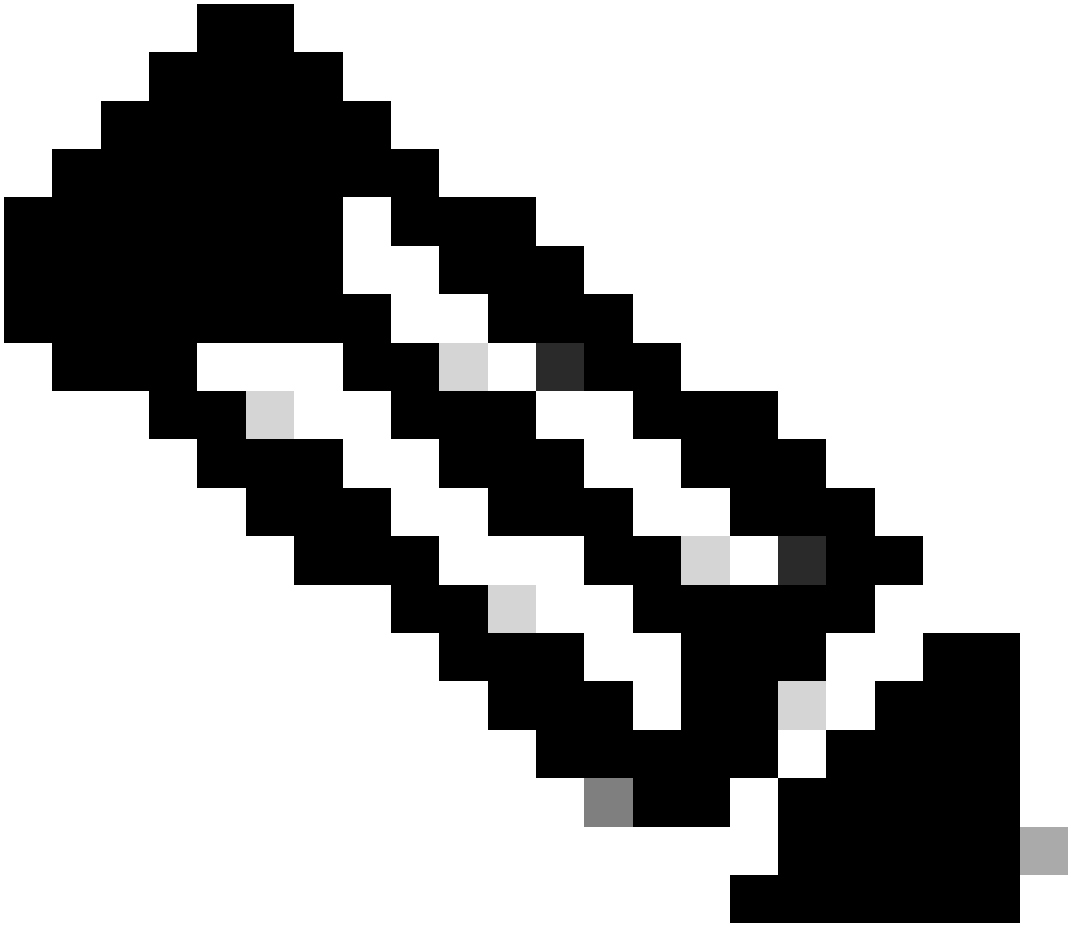
9. 기타 자세한 컨피그레이션은 FTD에서 보안 클라이언트(AnyConnect) 원격 액세스 VPN 구성을 참조하십시오.

10. 성공적인 검증을 위해 사용자 저장소 인증서 및 머신 저장소 인증서의 CA 인증서를 FTD에 업로드합니다. 이 시나리오에서는 사용자 저장소 인증서 및 머신 저장소 인증서가 동일한 CA에 의해 서명되므로 하나의 CA만 설치하면 됩니다. 사용자 저장소 인증서와 머신 저장소 인증서가 서로 다른 CA에 의해 서명된 경우 두 CA 인증서를 모두 FTD에 업로드해야 합니다.

CA Certificate

- Issued By :
  - CN : IdenTrust Commercial Root CA 1
  - O : IdenTrust
  - C : US
- Issued To :
  - CN : HydrantID Server CA O1
  - OU : HydrantID Trusted Certificate Service
  - O : IdenTrust
  - C : US
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : ftdha HydrantID-Server-CA-O1
- Valid From : 16:56:15 UTC December 12 2019
- Valid To : 16:56:15 UTC December 12 2029

FMC에서 FTD에 CA 인증서 설치

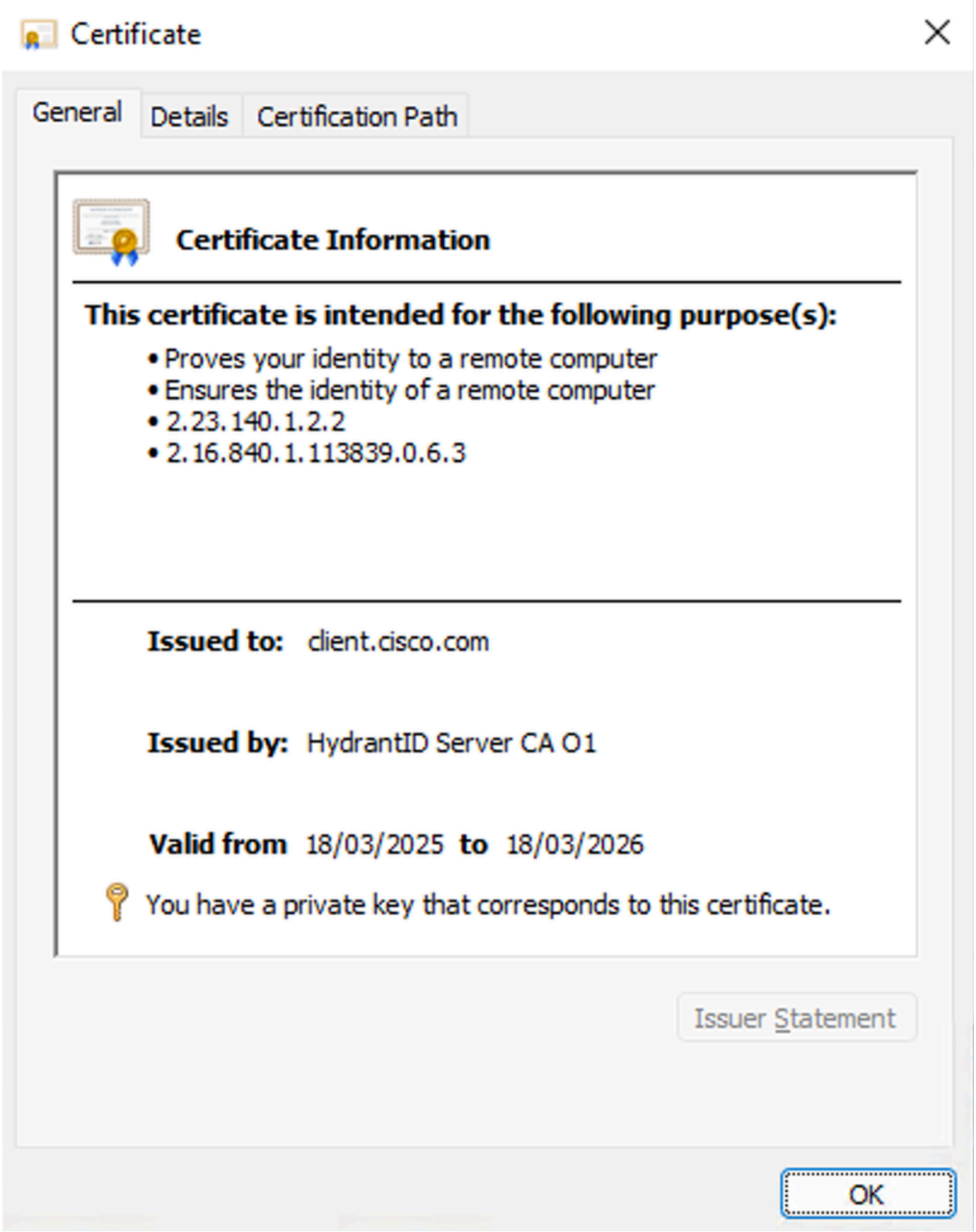


참고: AnyConnect 클라이언트 프로파일에는 CertificateStore가 All로 설정되어야 하며, 사용자에게 관리자 권한이 없는 경우 CertificateStoreOverride가 true로 설정되어야 합니다.

사용자 컴퓨터의 인증서

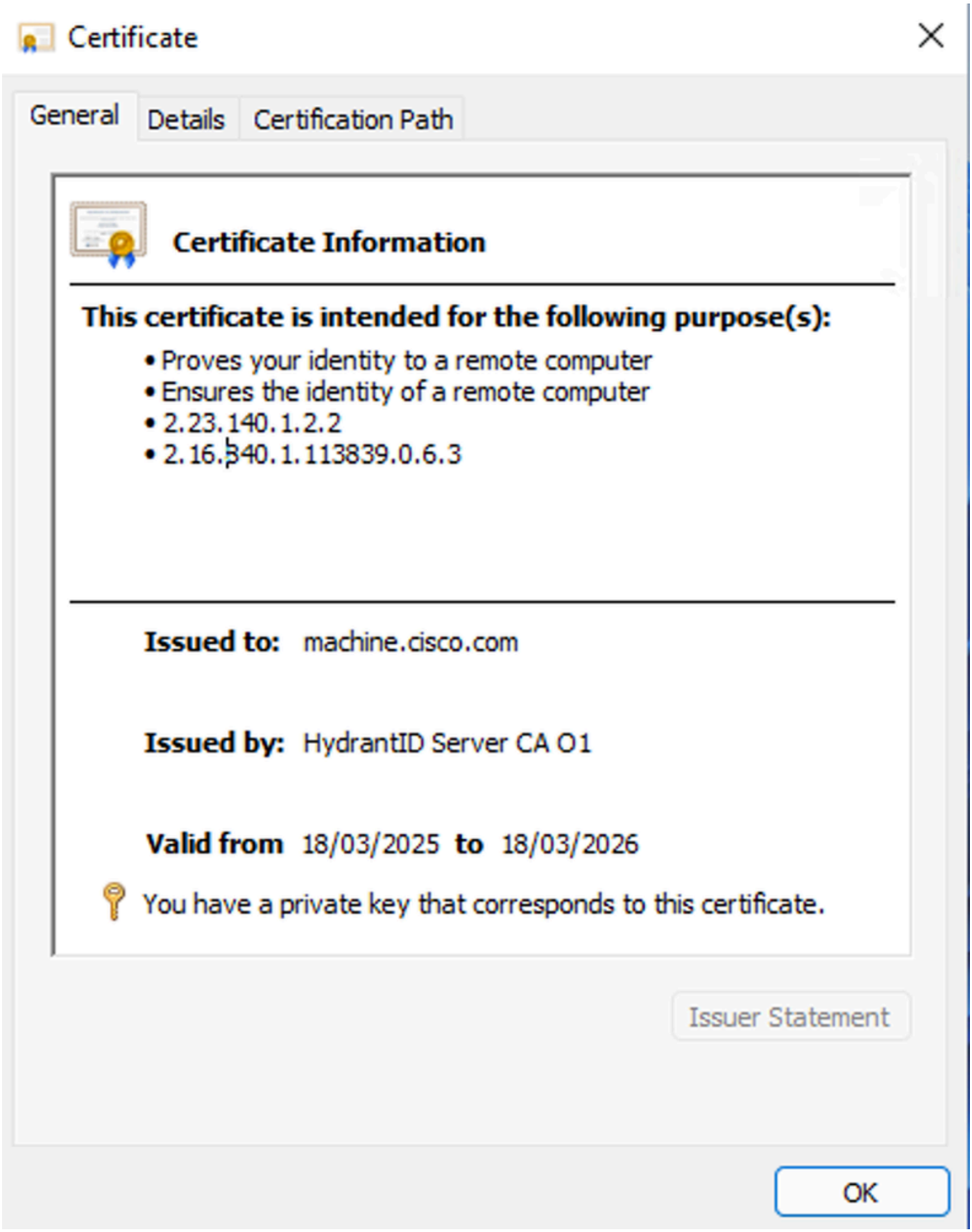
이 연결 프로파일에 연결해야 하는 사용자 컴퓨터에는 사용자 저장소 및 컴퓨터 저장소에 유효한 인증서가 설치되어 있어야 합니다.

사용자 저장소의 인증서:



사용자 저장소 인증서

컴퓨터 저장소의 인증서:



컴퓨터 저장소 인증서

다음을 확인합니다.

1. FTD CLI에서 연결 프로파일 컨피그레이션을 확인합니다.

<#root>

```
firepower# show run tunnel-group
tunnel-group RA-VPN-Multi-Cert type remote-access
tunnel-group RA-VPN-Multi-Cert general-attributes
 address-pool RAVPN-MultiCert-Pool
 default-group-policy RAVPN-Multi-Cert-GP
tunnel-group RA-VPN-Multi-Cert webvpn-attributes
```

authentication multiple-certificate

```
 group-alias RAVPN-MultiCert enable
```

2. 이 명령을 실행하여 연결을 확인합니다.

<#root>

```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

Username : client.cisco.com

```
       Index        : 28
Assigned IP  : 192.168.13.1           Public IP    : 10.106.56.89
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 19324                  Bytes Rx     : 134555
Pkts Tx      : 2                      Pkts Rx      : 1379
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : RAVPN-Multi-Cert-GP    Tunnel Group : RA-VPN-Multi-Cert
Login Time   : 07:18:53 UTC Wed Mar 19 2025
Duration     : 0h:21m:00s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a43590001c00067da6fdd
Security Grp : none                   Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 28.1
  Public IP    : 10.106.56.89
  Encryption   : none                   Hashing      : none
  TCP Src Port : 53927                  TCP Dst Port : 443
```

Auth Mode : Multiple-certificate

```
  Idle Time Out: 30 Minutes            Idle TO Left : 9 Minutes
  Client OS    : win
  Client OS Ver: 10.0.22000
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
  Bytes Tx     : 11581                 Bytes Rx     : 224
  Pkts Tx      : 1                     Pkts Rx      : 0
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 28.2
  Assigned IP  : 192.168.13.1          Public IP    : 10.106.56.89
  Encryption   : AES-GCM-128           Hashing      : SHA256
  Ciphersuite  : TLS_AES_128_GCM_SHA256
  Encapsulation: TLSv1.3               TCP Src Port : 53937
  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 5.1.4.74
  Bytes Tx     : 7743                  Bytes Rx     : 240
  Pkts Tx      : 1                     Pkts Rx      : 3
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 28.3
  Assigned IP  : 192.168.13.1          Public IP    : 10.106.56.89
  Encryption   : AES-GCM-256           Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2              UDP Src Port : 62975
  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 5.1.4.74
  Bytes Tx     : 0                     Bytes Rx     : 134091
  Pkts Tx      : 0                     Pkts Rx      : 1376
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

사용자 이름 client.cisco.com은 AAA 섹션에서 맵 사용자 이름 Second Certificate(두 번째 인증서의 맵 사용자 이름)가 선택되었으므로 사용자 저장소 인증서 CN에서 검색됩니다. First Certificate(첫 번째 인증서)를 선택하면 Machine store certificate(machine.cisco.com)에서 사용자 이름이 검색됩니다.

문제 해결

1. 유효한 인증서가 사용자 인증서 저장소와 머신 인증서 저장소에 있는지 확인합니다.
2. FTD에서 디버그를 수집하여 디버그 암호화 ca 14를 사용한 인증서 검증과 관련된 로그를 확

인합니다.

3. 사용자 시스템에서 DART를 검토합니다.

작업 시나리오의 DART 로그:

<#root>

```
****************************************

Date         : 03/19/2025
Time         : 00:18:50
Type         : Information
Source       : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 12100

[MCA] Multiple client cert auth requested by peer (via AggAuth)



****************************************

Date         : 03/19/2025
Time         : 00:18:50
Type         : Information
Source       : csc_vpnapi

Description : Function: ConnectMgr::nextClientCert
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 6774
Subject Name: C=US, ST=California, L=San Jose, O=Cisco Systems Inc.,

CN=machine.cisco.com


Issuer Name : C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA O1

Store : Microsoft Machine



****************************************

Date         : 03/19/2025
Time         : 00:18:50
Type         : Information
Source       : csc_vpnapi

Description : Function: CTransportCurlStatic::ClientCertRequestCB
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\CTransportCurlStatic.cpp
Line: 1358

Using client cert: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=machine.cisco.com



****************************************

Date         : 03/19/2025
Time         : 00:18:51
```

```
Type        : Information
Source      : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 12105
[MCA] Client certificate accepted at protocol level

*****************************************

Date        : 03/19/2025
Time        : 00:18:51
Type        : Information
Source      : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 12124
[MCA] Received and successfully parsed Multiple Certificate Authentication request from secure gateway.

*****************************************

Date        : 03/19/2025
Time        : 00:18:51
Type        : Information
Source      : csc_vpnapi

Description : Function: ConnectMgr::nextClientCert
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 6774
Subject Name: C=US, ST=California, L=San Jose, O=Cisco Systems Inc.,
CN=client.cisco.com

Issuer Name : C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA O1
Store : Microsoft User

*****************************************

Date        : 03/19/2025
Time        : 00:18:51
Type        : Information
Source      : csc_vpnapi

Description : Function: ConnectMgr::processIfcData
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 4129
[MCA] Second certificate for Multiple Certificate Authentication found - now sending 2nd certificate to

*****************************************

Date        : 03/19/2025
Time        : 00:18:51
Type        : Information
Source      : csc_vpnapi

Description : Function: ConnectMgr::userResponse
```

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 1690
Processing user response.

****

Date   : 03/19/2025
Time   : 00:18:52
Type   : Information
Source   : csc_vpnapi

Description : Function: ConnectMgr::createMultiCertAuthReplyXML
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 17127

[MCA] Successfully signed Multiple Certificate Authentication data with 2nd certificate

****

Date   : 03/19/2025
Time   : 00:18:52
Type   : Information
Source   : csc_vpnapi

Description : Function: ConnectMgr::sendResponse
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 6522
[MCA] Multiple Certificate Authentication response ready to send to secure gateway

****

Date   : 03/19/2025
Time   : 00:18:52
Type   : Information
Source   : csc_vpnapi

Description : Message type prompt sent to the user:
Your client certificate will be used for authentication

****

Date   : 03/19/2025
Time   : 00:18:53
Type   : Information
Source   : csc_vpnapi

Description : Function: CVpnApiShim::SaveUserPrompt
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\ApiShim\ApiShim.cpp
Line: 3538
User submitted response for host ftdha.cisco.com and tunnel group: RAVPN-MultiCert

****

Date   : 03/19/2025
Time   : 00:18:53
Type   : Information
Source   : csc_vpnapi

Description : Function: ConnectMgr::userResponse
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 1690

Processing user response.

****

Date   : 03/19/2025
Time   : 00:18:53
Type   : Information
Source   : csc_vpnapi

Description : Function: ConnectMgr::processIfcData
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 3815

Authentication succeeded

****

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.