在FTD上為RAVPN設定多重憑證驗證

目錄

簡介

本檔案介紹對FMC管理的Firepower威脅防禦(FTD)上的安全使用者端使用多重憑證驗證的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 對遠端訪問VPN(RAVPN)的基本瞭解
- 使用Firepower管理中心(FMC)的經驗
- X509證書的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科FTD - 7.6
- 思科FMC - 7.6
- Windows 11，帶Cisco安全客戶端5.1.4.74

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在軟體版本7.0之前，FTD支援單一憑證的驗證，這表示使用者或機器可以透過單一連線嘗試進行驗

證，但無法兩者均有。

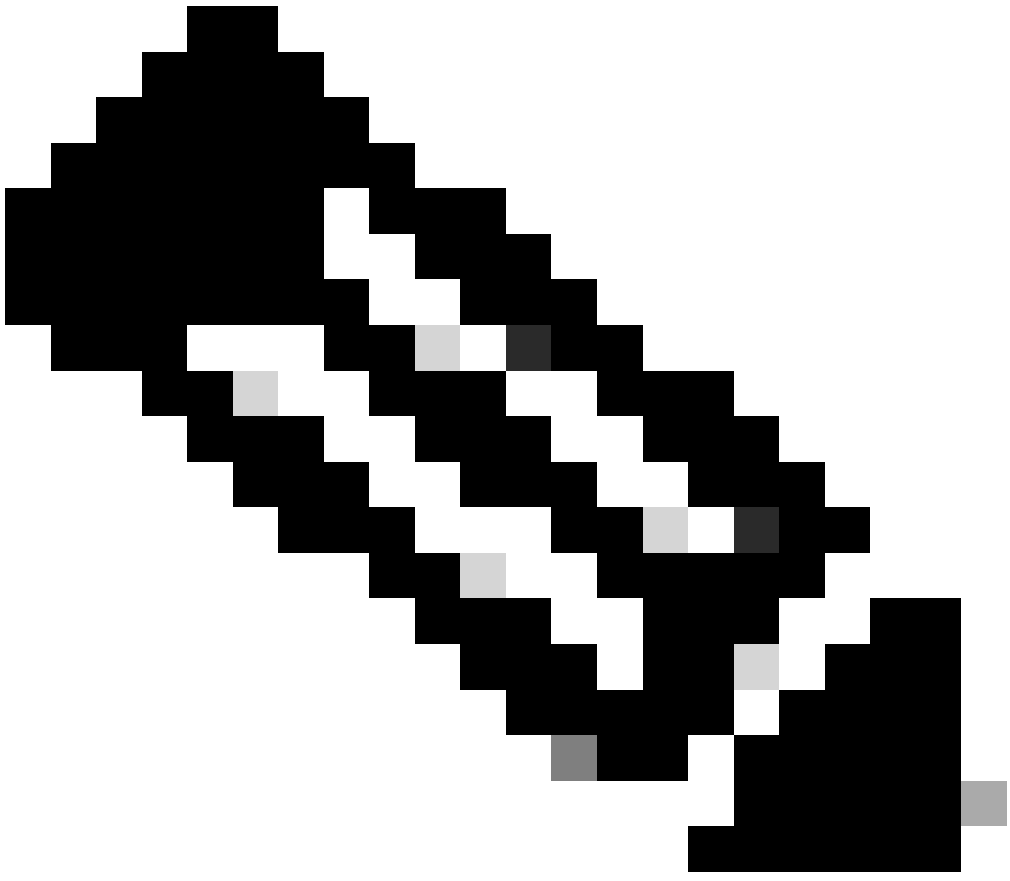
通過基於多個證書的身份驗證，可以使用threat防禦驗證電腦或裝置證書，以確保裝置是公司簽發的裝置，此外還可以驗證使用者身份證書，以便在SSL或IKEv2 EAP階段使用Secure Client進行VPN訪問。

多個證書身份驗證當前將證書數量限製為兩個。安全客戶端必須指示支援多個證書身份驗證。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。Secure Client 4.4.04030或更高版本支援基於多證書的身份驗證。

組態

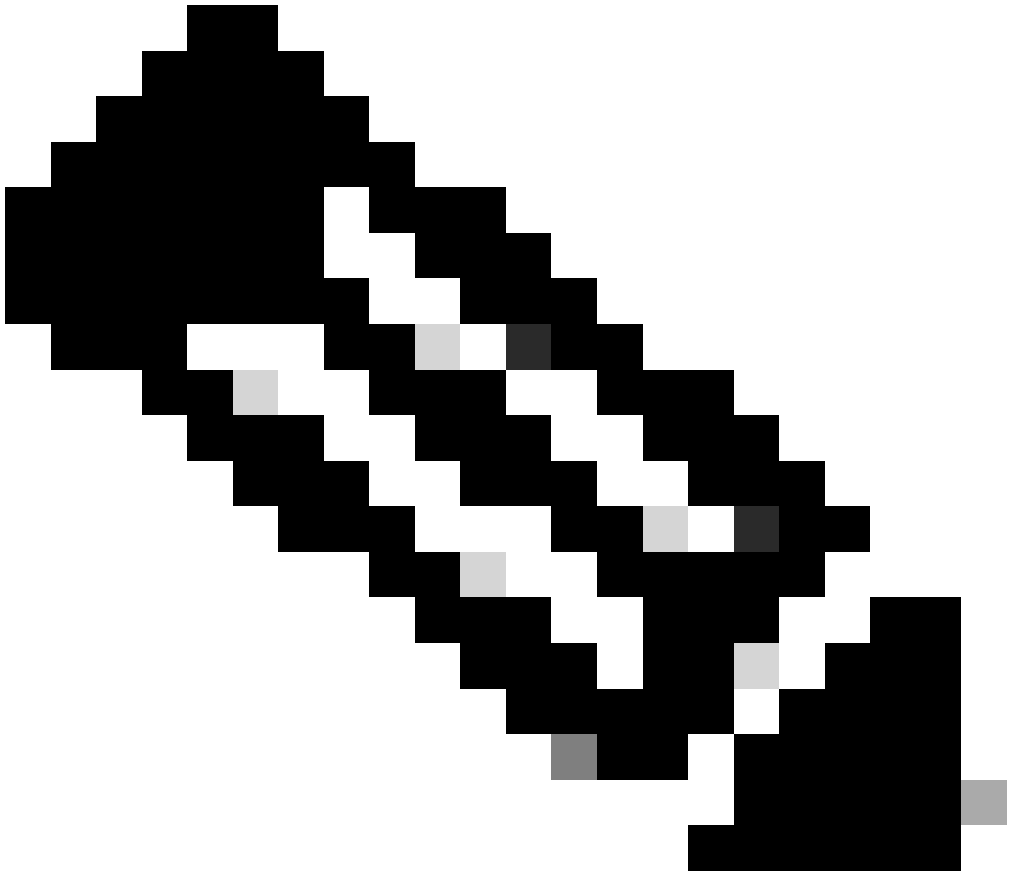
FTD上的組態

1. 導覽至Devices > VPN > Remote Access。
2. 選擇Remote Access VPN policy並按一下Edit。



附註：如果尚未配置遠端訪問VPN，請按一下Add建立新的遠端訪問VPN策略。

3. 選擇並編輯Connection Profile以配置多個證書身份驗證。
4. 按一下「AAA」，然後選擇「Authentication Method」作為「Client Certificate Only」或「Client Certificate & AAA」。



附註：如果您已選擇Client Certificate & AAA authentication method，請選擇Authentication Server。

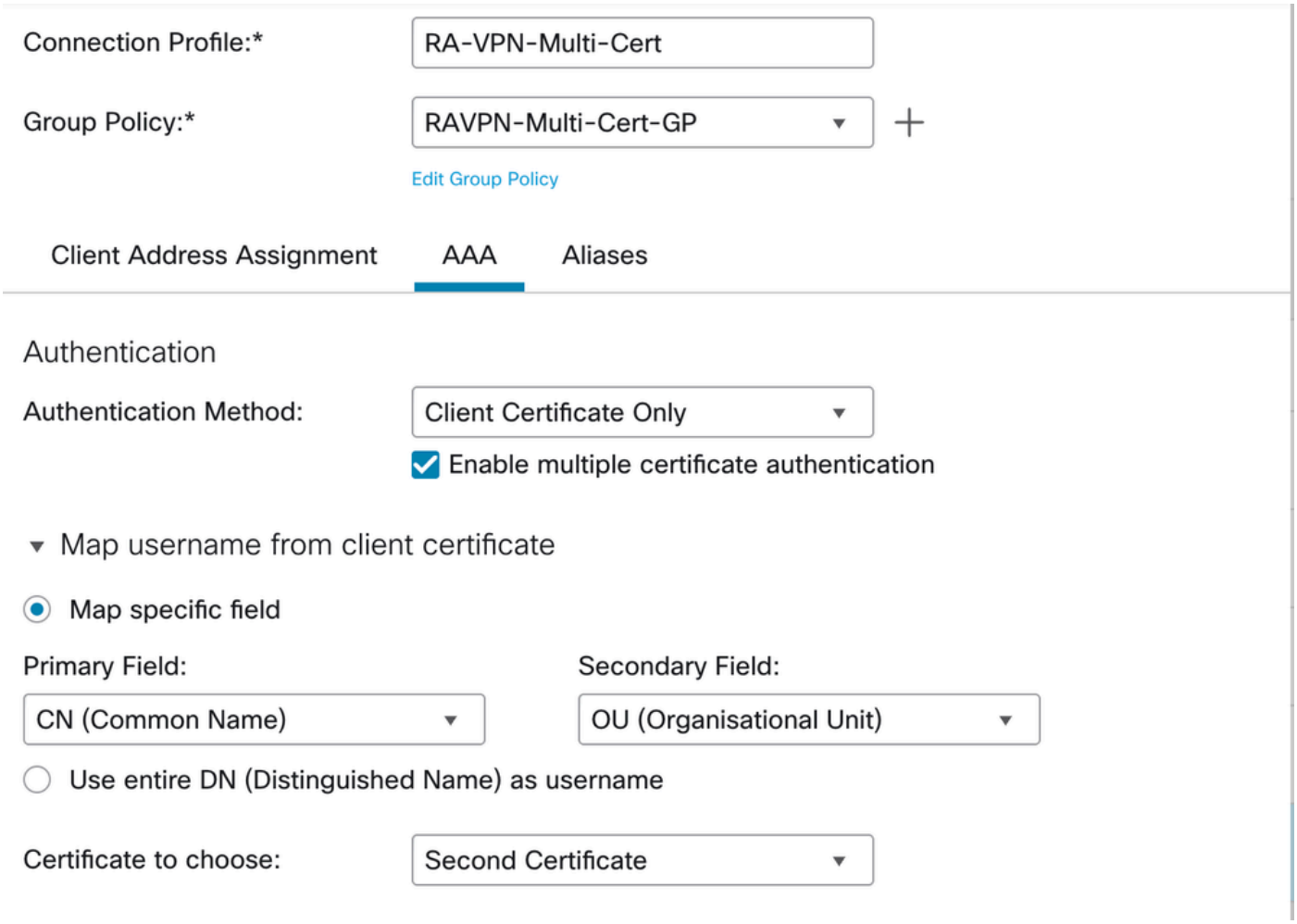
5. 選中Enable multiple certificate authentication覈取方塊。

6. 從客戶端證書中選擇要對映使用者名稱的證書之一:

   - First Certificate — 選擇此選項以對映從VPN客戶端傳送的電腦證書的使用者名稱。
   - 第二個證書(Second Certificate) — 選擇此選項以對映從客戶端傳送的使用者證書中的使用者名稱。

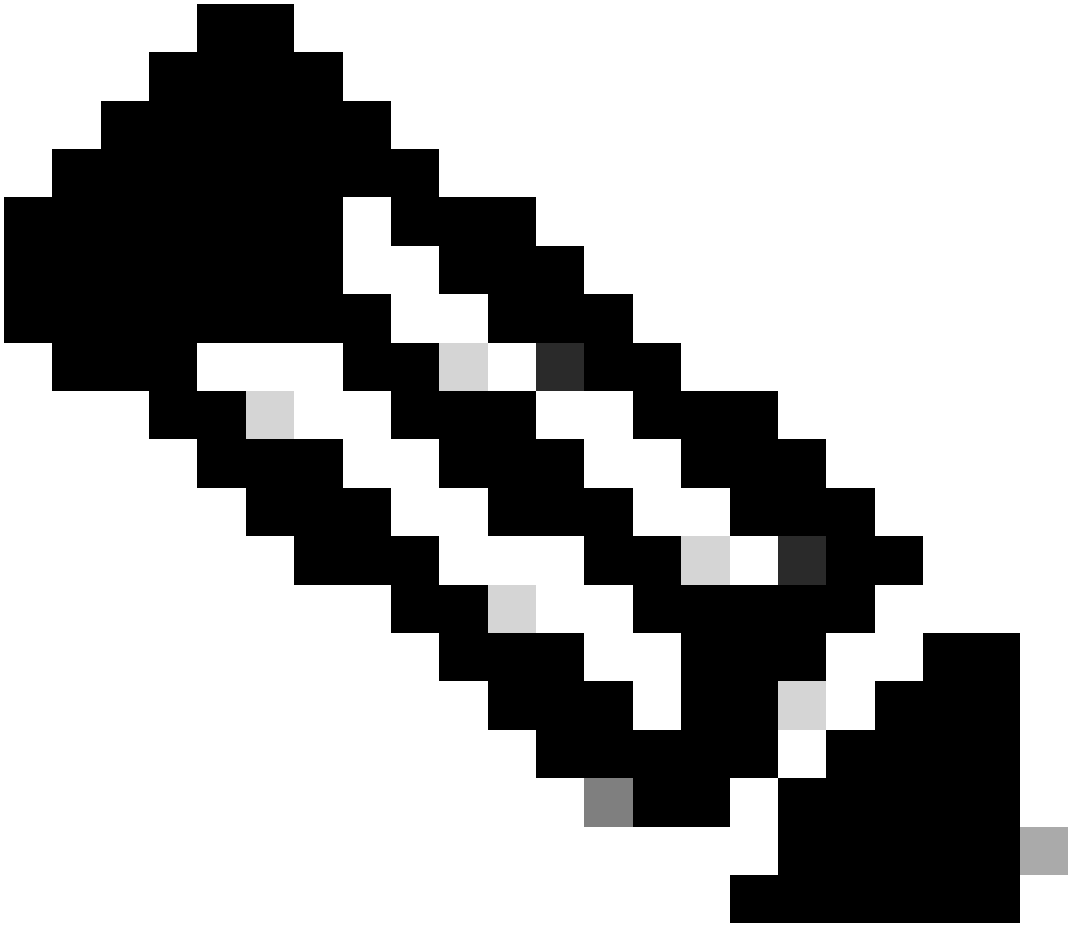
   啟用僅證書身份驗證時，將從客戶端傳送的使用者名稱用作VPN會話使用者名稱。啟用AAA和證書身份驗證時，VPN會話使用者名稱基於Prefill選項。

7. 如果選擇Map specific field選項（包括來自客戶端證書的使用者名稱），則Primary和Secondary欄位將顯示預設值：Common Name(CN)和Organizational Unit(OU)。



連線配置檔案的AAA設定

8.如果選擇使用整個可分辨名稱(DN)作為username選項，系統會自動檢索使用者身份。可分辨名稱是一個唯一標識，由單個欄位組成，在將使用者與連線配置檔案進行匹配時，這些欄位可用作識別符號。DN規則用於增強型證書身份驗證。



附註：如果您已選擇Client Certificate & AAA authentication，則選擇Prefill username from certificate on user login選項，以在使用者通過Cisco Secure Client的Secure Client VPN模組進行連線時從客戶端證書中預填輔助使用者名稱。

在登入視窗中隱藏使用者名稱：次要使用者名稱從客戶端證書中預先填充，但對使用者隱藏，以便使用者不修改預先填充的使用者名稱。

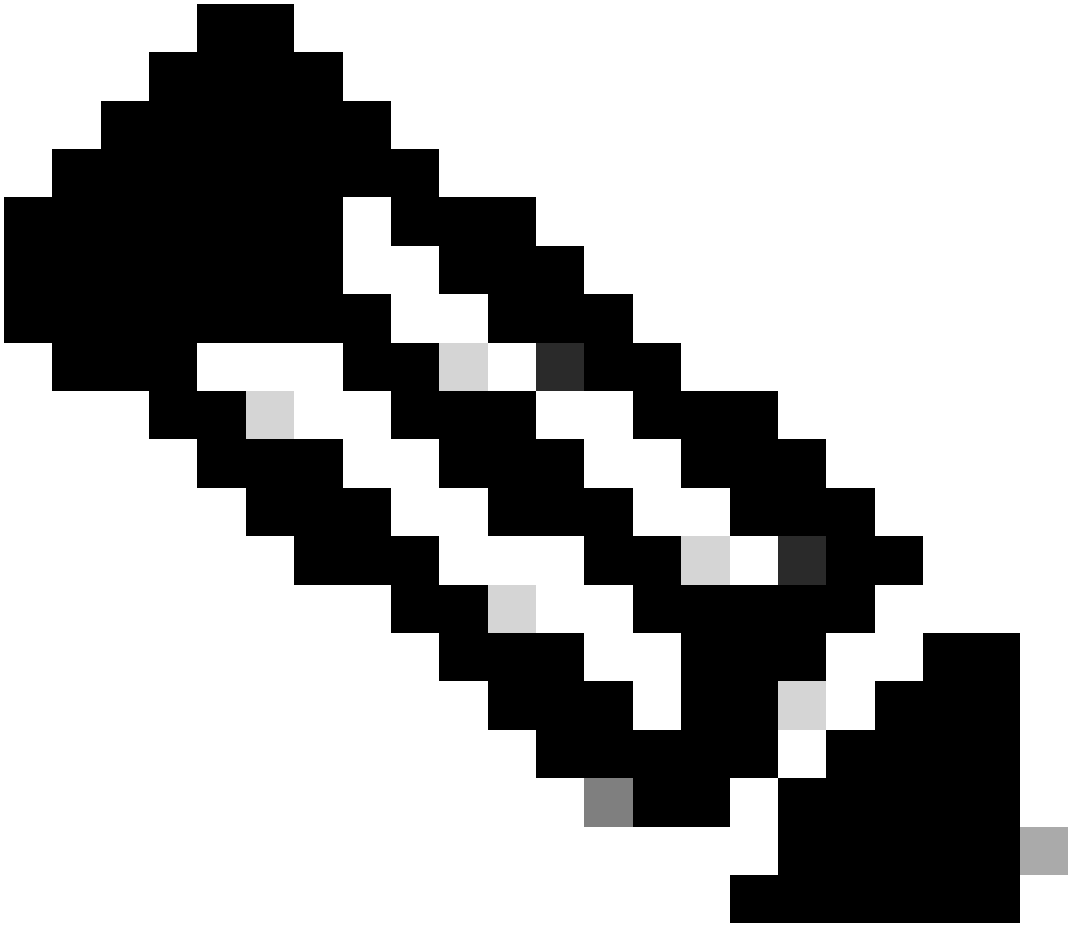
9.有關其他詳細設定，請參閱在FTD上設定安全使用者端(AnyConnect)遠端存取VPN。

10.將使用者儲存區憑證和機器儲存區憑證的CA憑證上傳到FTD以成功驗證。由於在此方案中，使用者儲存證書和電腦儲存證書是由同一CA簽名的，因此安裝該CA就足夠了。如果使用者儲存憑證和機器儲存憑證是由不同的CA簽署，則這兩個CA憑證必須上傳到FTD。

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

從FMC安裝到FTD的CA憑證

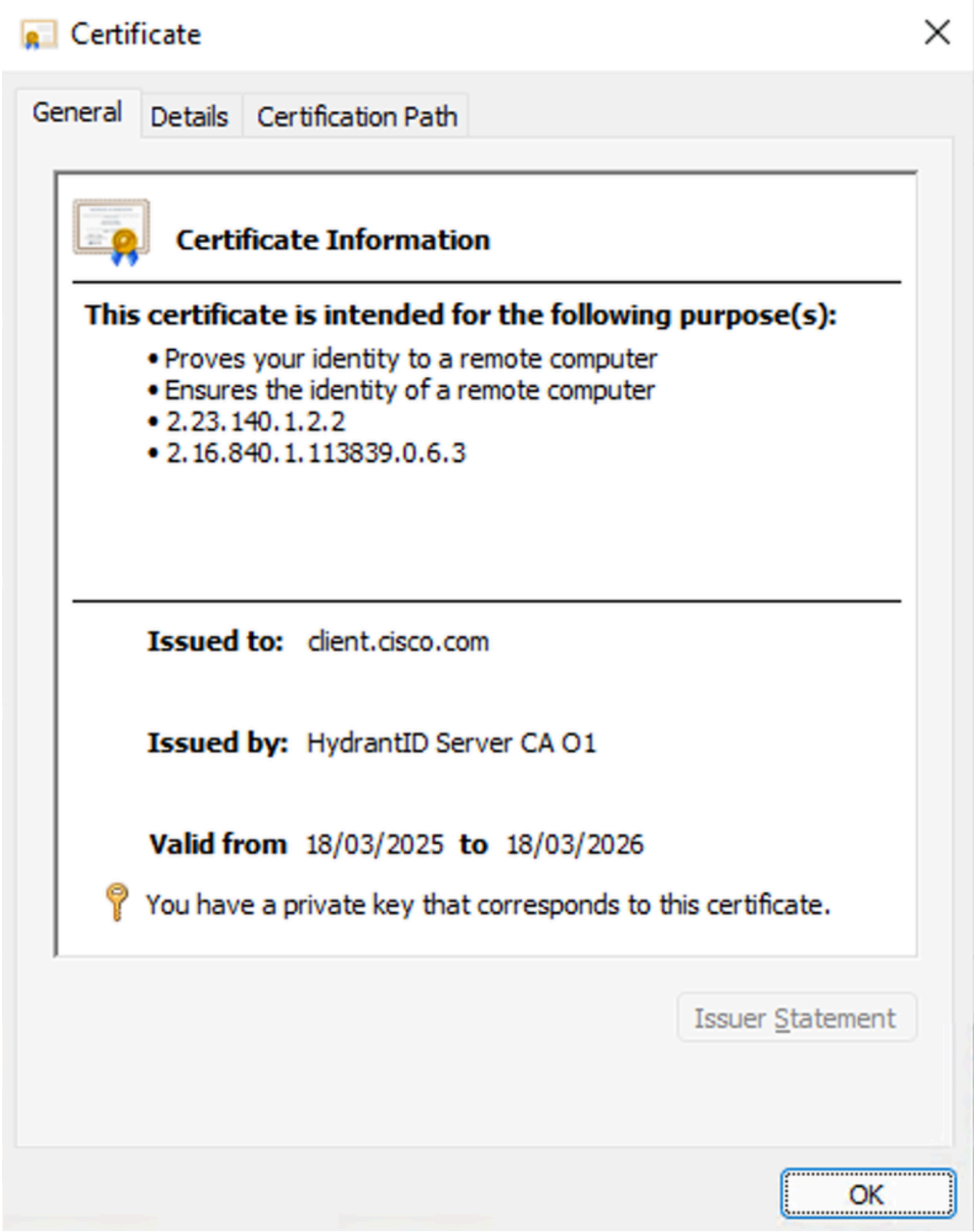


附註：如果使用者沒有管理員許可權，AnyConnect客戶端配置檔案必須將CertificateStore設定為All，並將CertificateStoreOverride設定為true。

使用者電腦上的證書

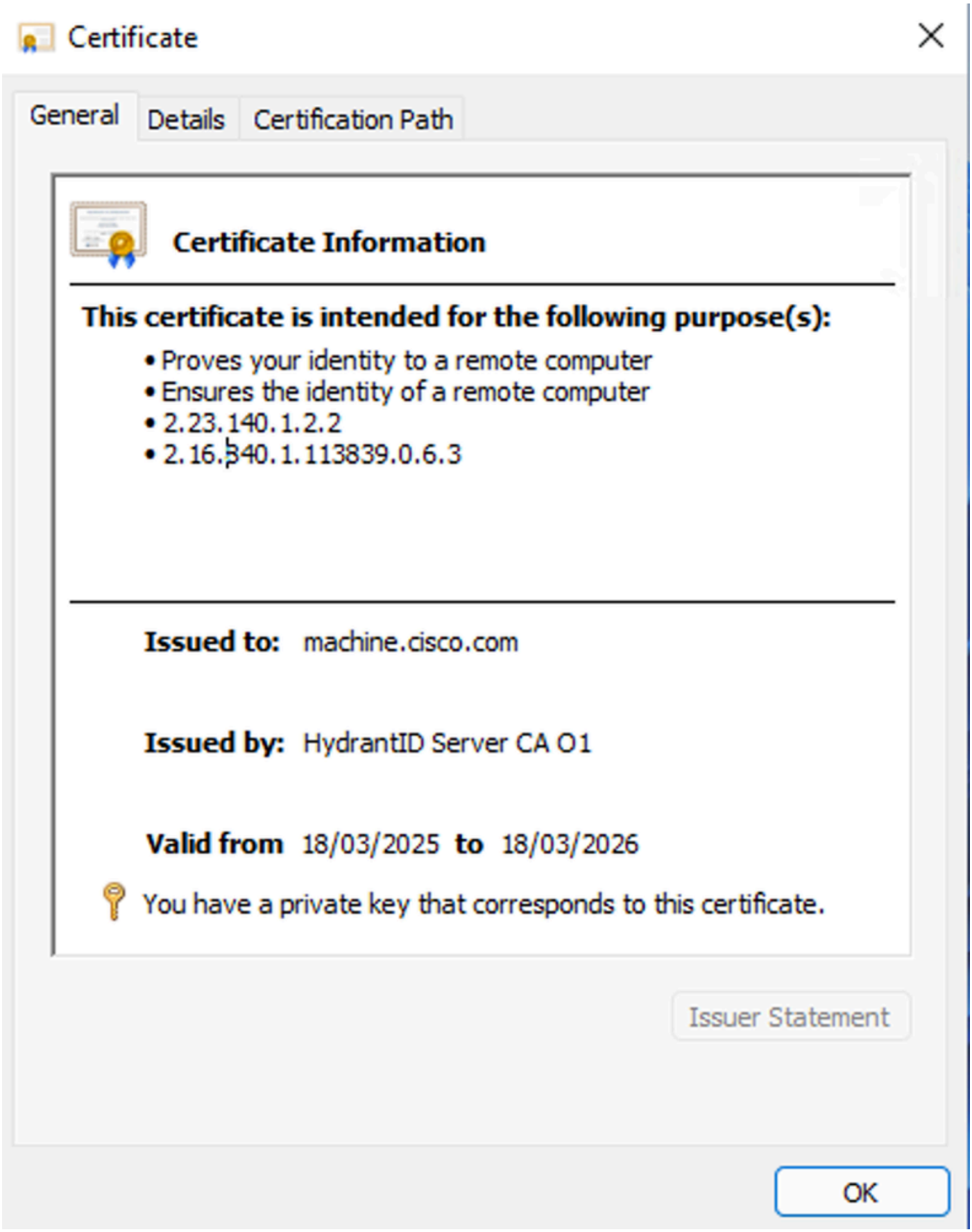
應該連線到此連線配置檔案的使用者電腦必須在使用者儲存和電腦儲存中安裝有效證書。

來自使用者儲存的證書：



使用者儲存證書

來自電腦儲存的證書：


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2.23.140.1.2.2
• 2.16.840.1.113839.0.6.3
Issued to: machine.cisco.com
Issued by: HydrantID Server CA O1
Valid from 18/03/2025 to 18/03/2026
You have a private key that corresponds to this certificate.
Issuer Statement
OK

電腦儲存證書

驗證

1.從FTD CLI驗證連線設定檔組態：

<#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.執行以下命令驗證連線：

<#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
```

從User store certificate CN中檢索的使用者名稱client.cisco.comis，因為AAA部分選擇了Map username from Second Certificate。如果選擇了First Certificate，則從電腦儲存證書(machine.cisco.com)中檢索使用者名稱。

疑難排解

1. 確保使用者證書儲存和電腦證書儲存中存在有效的證書。
2. 收集FTD上的偵錯，以使用debug crypto ca 14檢查與憑證驗證相關的日誌。
3. 從使用者電腦檢視DART。

工作場景中的DART日誌：

<#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

****

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。