在FTD上为RAVPN配置多证书身份验证

目录

简介

本文档介绍对FMC管理的Firepower威胁防御(FTD)上的安全客户端使用多证书身份验证的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解远程访问VPN(RAVPN)
- 具有Firepower管理中心(FMC)的经验
- X509证书的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD - 7.6
- 思科FMC - 7.6
- Windows 11，带Cisco安全客户端5.1.4.74

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在软件版本7.0之前，FTD支持基于单个证书的身份验证，这意味着对于单个连接尝试，用户或机器

可以进行身份验证，但不能同时进行身份验证。

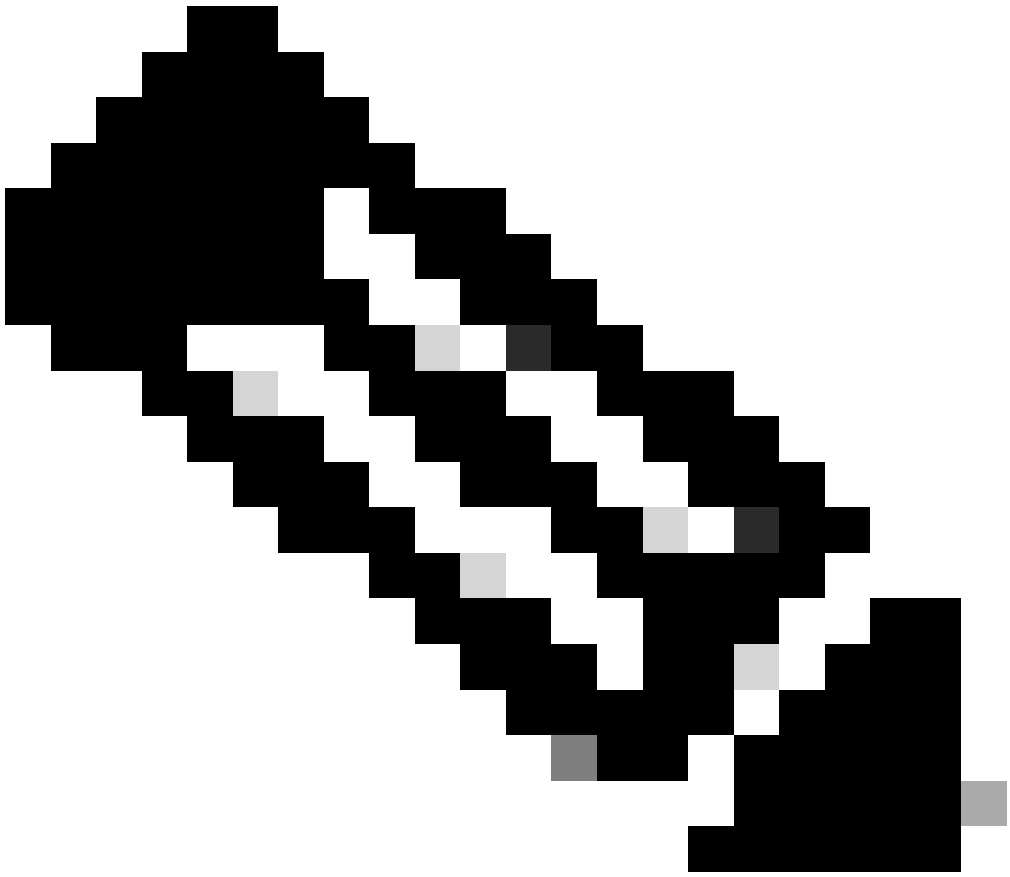
除了验证用户身份证书以在SSL或IKEv2 EAP阶段使用SecureClient进行VPN访问外，多证书身份验证还能够使用threat防御验证计算机或设备证书，以确保设备是公司颁发的设备。

多个证书身份验证当前将证书数量限制为两个。安全客户端必须表示支持多个证书身份验证。如果情况并非如此，则网关使用传统身份验证方法之一或连接失败。Secure Clientversion 4.4.04030或更高版本支持基于多证书的身份验证。

配置

FTD上的配置

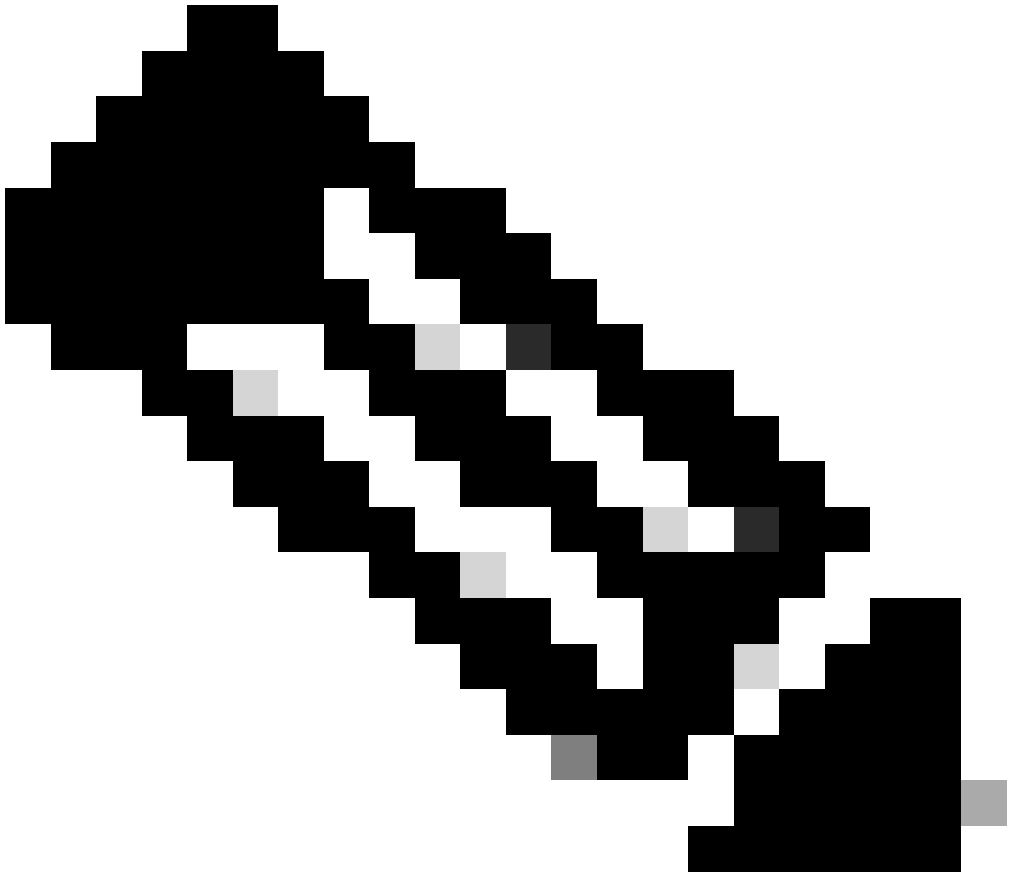
1. 导航到设备 > VPN > 远程访问。
2. 选择Remote Access VPN policy并单击Edit。



注意：如果尚未配置远程访问VPN，请单击Add创建新的远程访问VPN策略。

3. 选择并编辑连接配置文件以配置多个证书身份验证。

4. 单击AAA设置，然后选择Authentication Method作为Client Certificate Only或Client Certificate & AAA。



注意：如果选择了客户端证书和AAA身份验证方法，请选择Authentication Server。

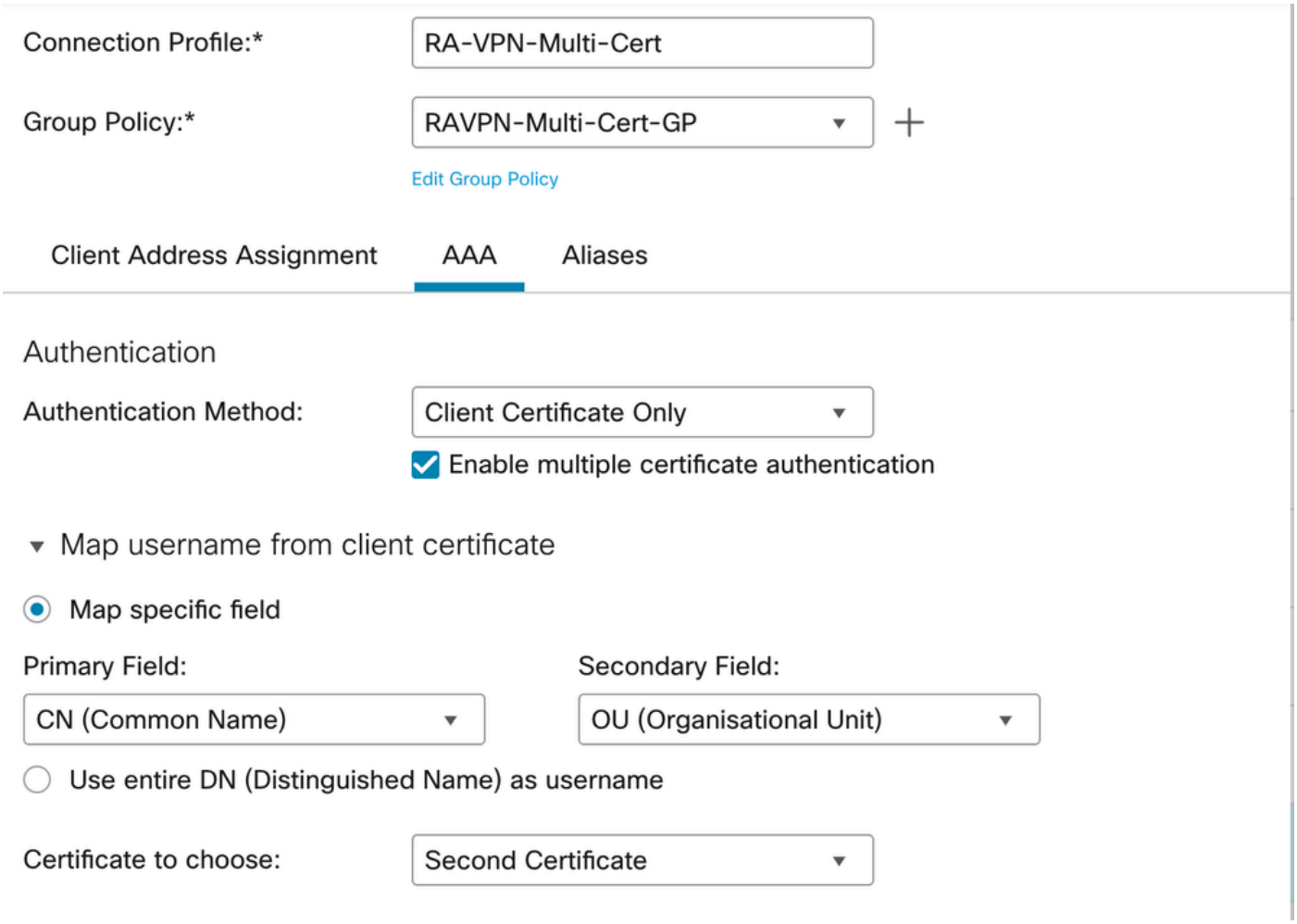
5. 选中Enable multiple certificate authentication 复选框。

6. 从客户端证书中选择一个要映射用户名的证书:

   - First Certificate — 选择此选项以映射来自VPN客户端发送的计算机证书的用户名。
   - 第二个证书(Second Certificate) — 选择此选项以映射从客户端发送的用户证书中的用户名。

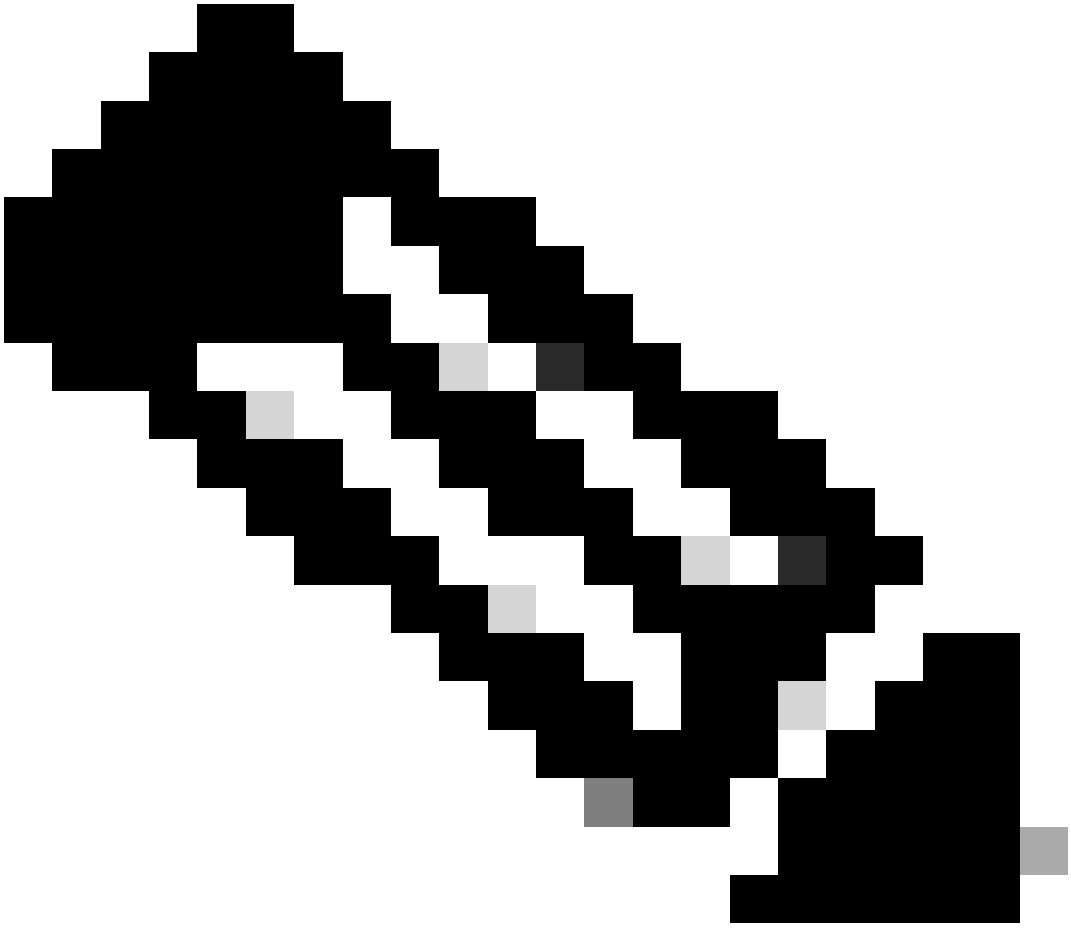
   启用仅证书身份验证时，将从客户端发送的用户名用作VPN会话用户名。启用AAA和证书身份验证时，VPN会话用户名基于Prefill选项。

7. 如果选择Map specific field选项（包括来自客户端证书的用户名），则Primary和Secondary字段将显示默认值：Common Name(CN)和Organizational Unit(OU)。



连接配置文件的AAA设置

8.如果选择使用整个可分辨名称(DN)作为username选项，系统会自动检索用户身份。可分辨名称是一个唯一标识，由单个字段组成，在将用户与连接配置文件进行匹配时可用作标识符。DN规则用于增强证书身份验证。



注意：如果已选择Client Certificate & AAA authentication，则选择Prefill username from certificate on user login选项以当用户通过Cisco Secure Client的Secure Client VPN模块进行连接时从客户端证书预填充辅助用户名。

在登录窗口中隐藏用户名：辅助用户名是从客户端证书预填充的，但对用户隐藏，以便用户不修改预填充的用户名。

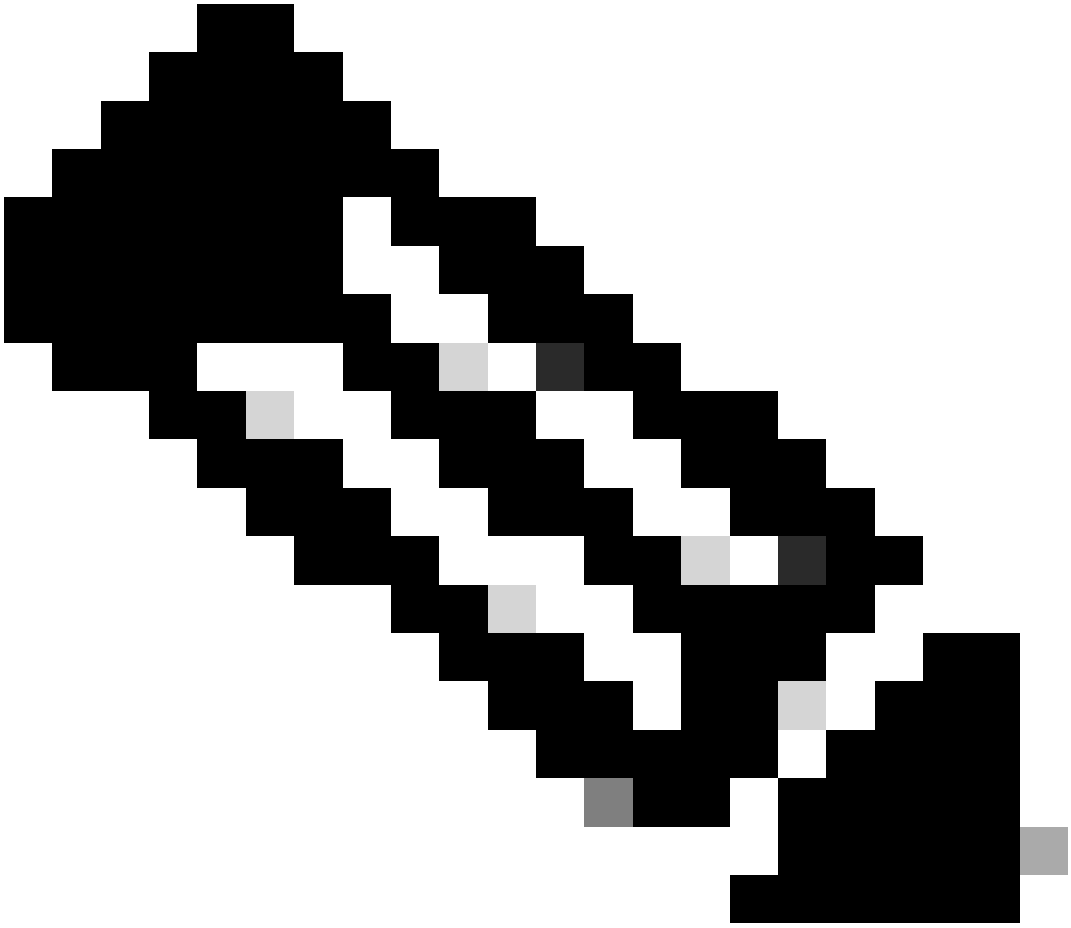
9.有关其他详细配置，请参阅在FTD上配置安全客户端(AnyConnect)远程访问VPN。

10.将用户存储证书和计算机存储证书的CA证书上传到FTD以成功验证。因为在此场景中，用户存储证书和计算机存储证书由同一CA签名，所以安装该CA就足够了。如果用户存储证书和计算机存储证书由不同的CA签名，则必须将这两个CA证书上传到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

从FMC安装到FTD的CA证书

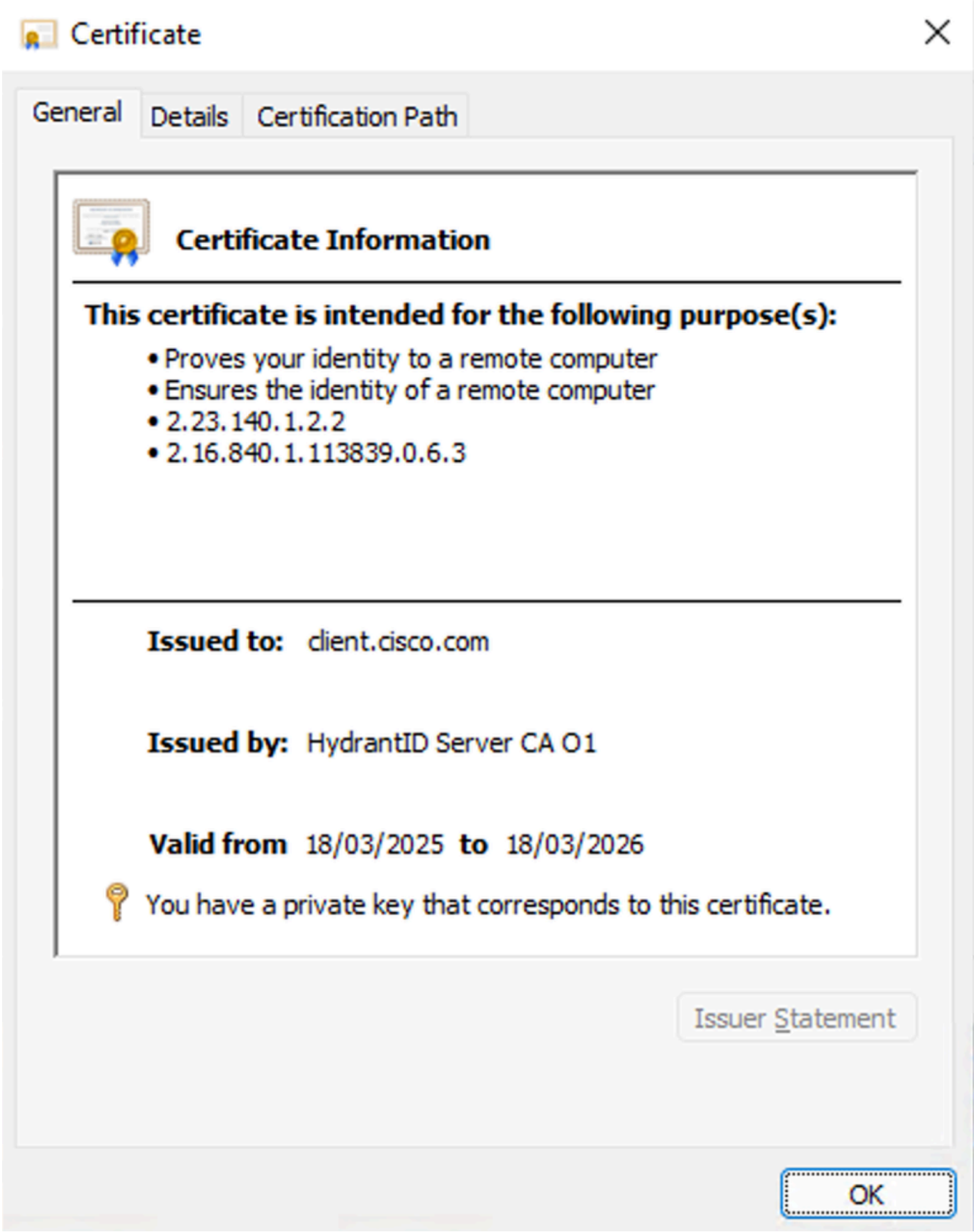


注意：如果用户没有管理员权限，则AnyConnect客户端配置文件必须将CertificateStore设置为All，并将CertificateStoreOverride设置为true。

用户计算机上的证书

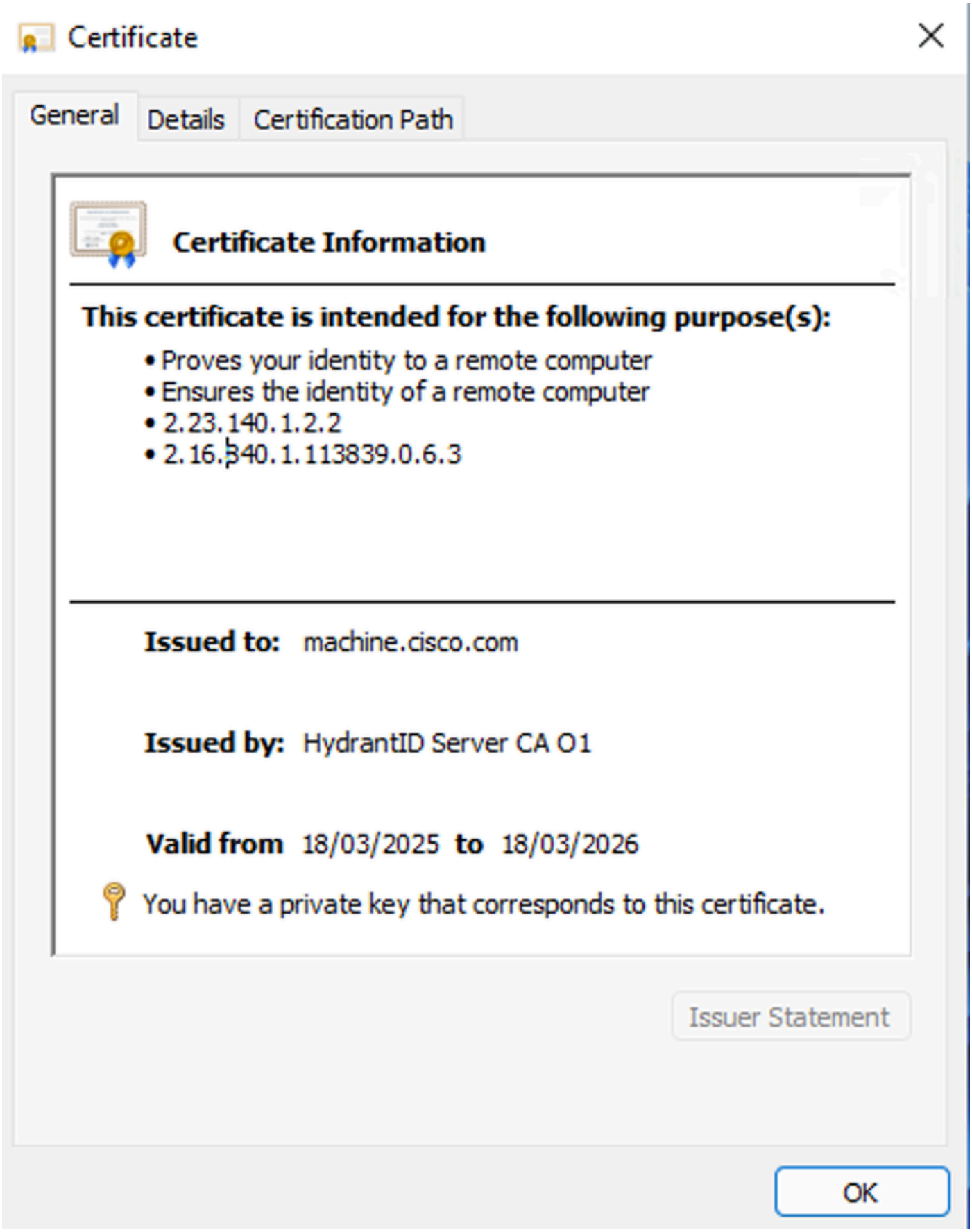
应该连接到此连接配置文件的用户计算机必须在用户存储和计算机存储中安装有效证书。

来自用户存储的证书：



用户存储证书

来自计算机存储的证书：


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

计算机存储证书

验证

1.从FTD CLI验证连接配置文件配置：

<#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.执行以下命令以验证连接：

<#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
```

用户名client.cisco.comis从用户存储证书CN检索，因为在AAA部分中选择了来自第二个证书的映射用户名。如果选择First Certificate，则会从计算机存储证书(machine.cisco.com)中检索用户名。

故障排除

1. 确保用户证书存储和计算机证书存储中存在有效证书。
2. 收集FTD上的调试，以使用debug crypto ca 14检查与证书验证相关的日志。
3. 从用户计算机查看DART。

工作场景中的DART日志：

<#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

****

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。