Configure Multiple Certificate Authentication on FTD for RAVPN

Contents

Introduction

This document describes the procedure to use Multiple Certificate Authentication for Secure Client on Firepower Threat Defense (FTD) managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Remote Access VPN (RAVPN)
- Experience with Firepower Management Center (FMC)
- Basic knowledge of X509 certificates

Components Used

The information in this document is based on these software and hardware versions:

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 11 with Cisco Secure Client 5.1.4.74

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Prior to software version 7.0, FTD supports single certificate based authentication, which means either the

user or the machine can be authenticated but not both, for a single connection attempt.

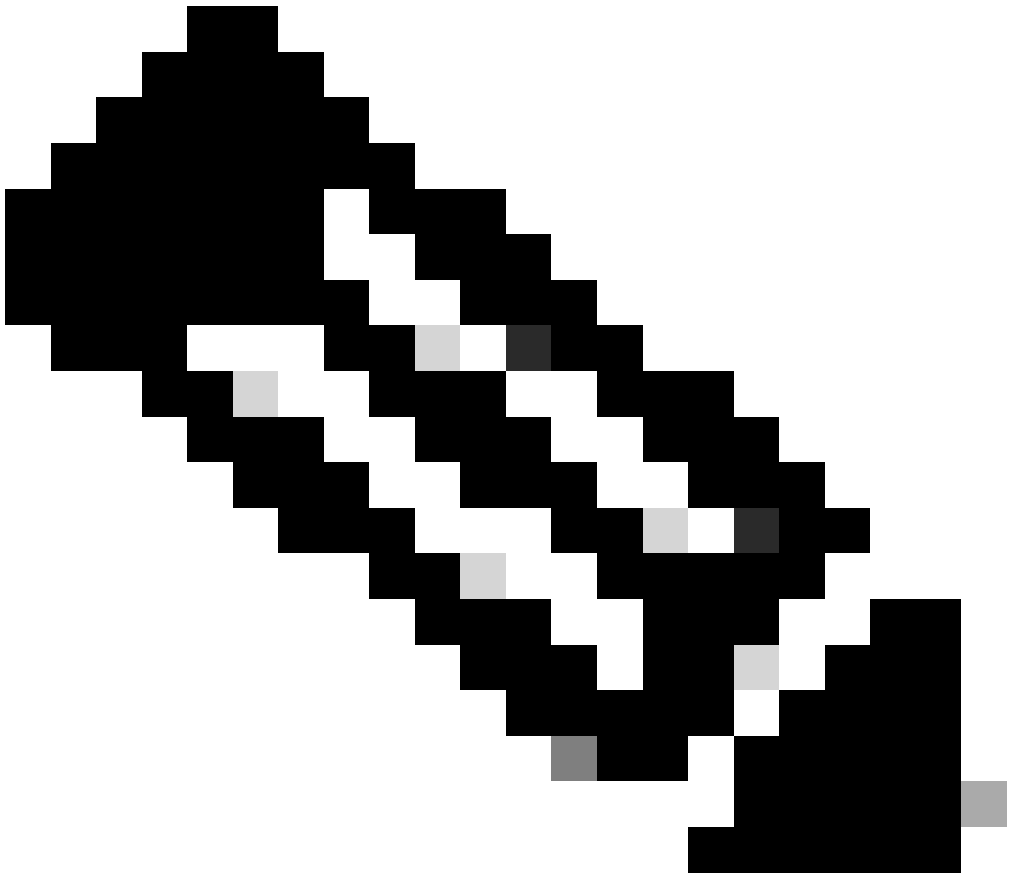
Multiple certificate based authentication gives the ability to have thethreat defensevalidate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the users identity certificate to allow VPN access using theSecure Clientduring SSL or IKEv2 EAP phase.

Multiple certificate authentication currently limits the number of certificates to two. Secure Clientmust indicate support for multiple certificate authentication. If that is not the case, then the gateway uses one of the legacy authentication methods or fails the connection.Secure Clientversion 4.4.04030 or later supports Multi-Certificate based authentication.

Configurations

Configuration on FTD

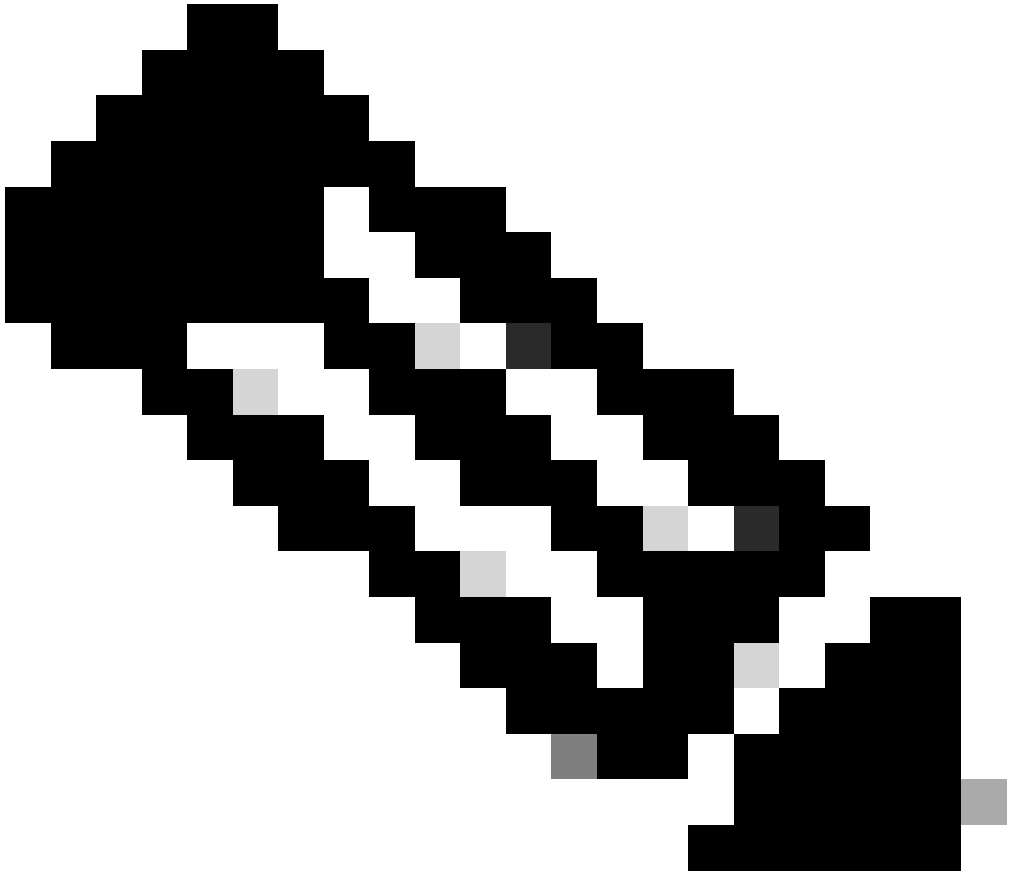
1. Navigate to **Devices > VPN > Remote Access**.
2. Select the **Remote Access VPN policy** and click **Edit**.



Note: If you have not configured a remote access VPN, click **Add** to create a new remote access VPN policy.

3. Select and edit a **Connection Profile** to configure multiple certificate authentication.

4. Click **AAA** settings and choose **Authentication Method** as **Client Certificate Only** or **Client Certificate & AAA**.



Note: Select the **Authentication Server** if you have selected the Client Certificate & AAA authentication method.

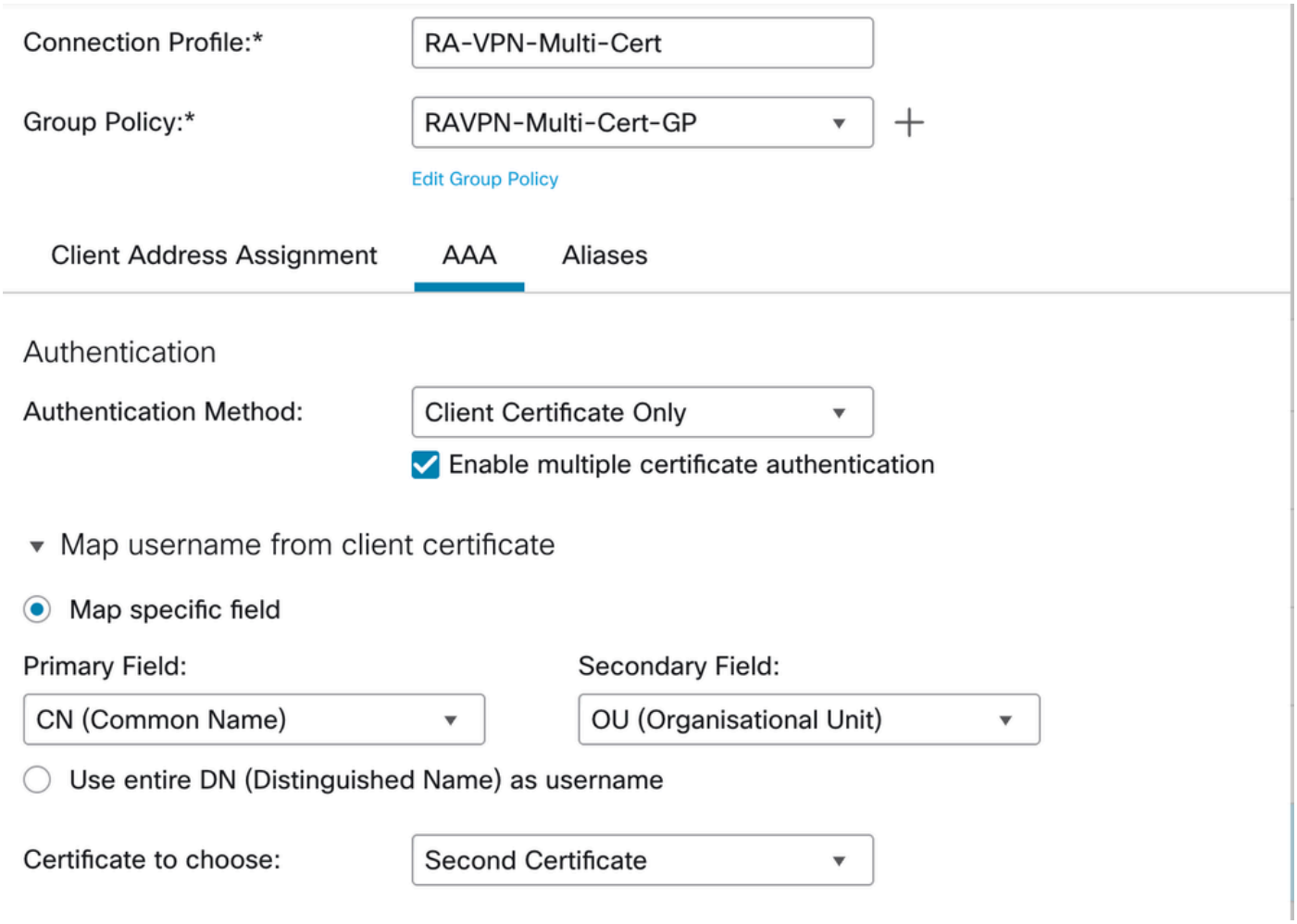
5. Select the **Enable multiple certificate authentication** checkbox.

6. Choose one of the certificates to **Map username from client certificate**:

   - **First Certificate**— Select this option to map the username from the machine certificate sent from the VPN client.
   - **Second Certificate**— Select this option to map the username from the user certificate sent from the client.

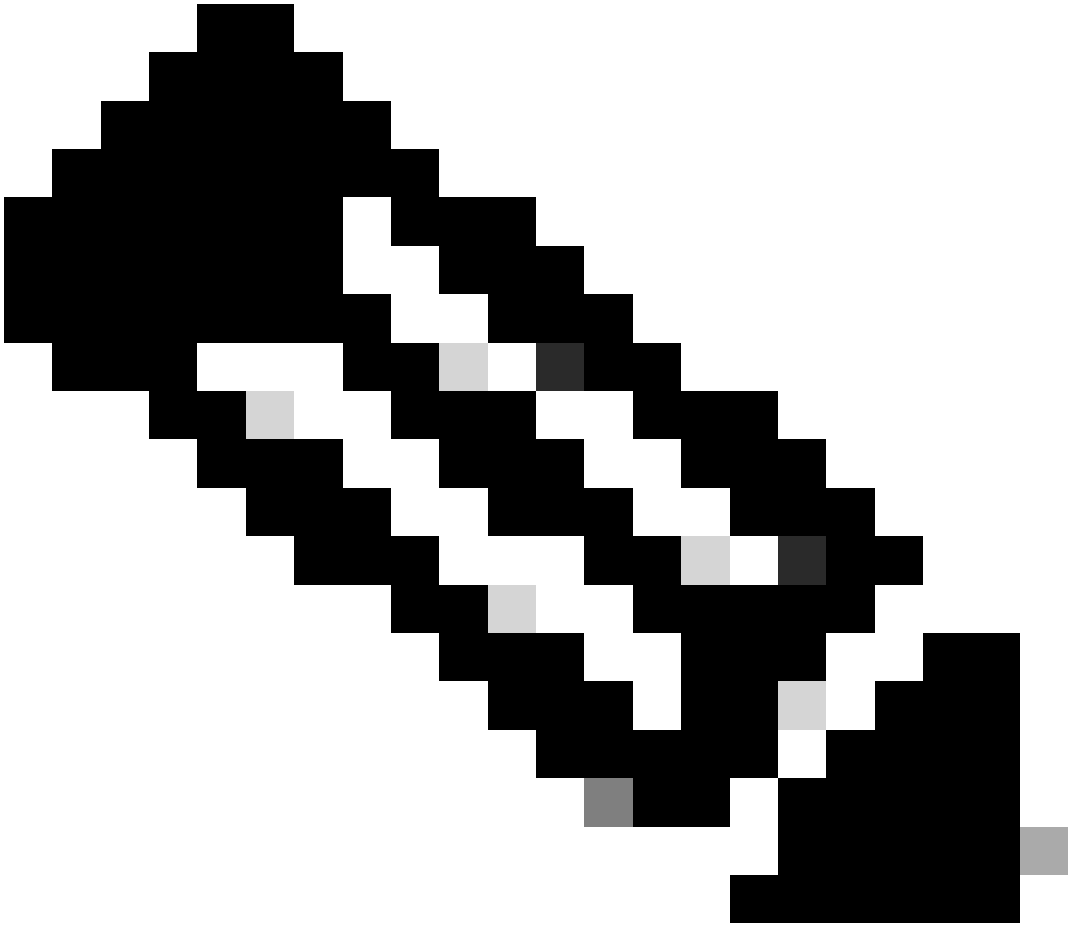
   The username sent from the client is used as the VPN session username when certificate only authentication is enabled. When AAA and certificate authentication is enabled, VPN session username is based on Prefill option.

7. If you select the **Map specific field** option, which includes the username from the client certificate, the Primary and Secondary fields display default values: Common Name (CN) and Organizational Unit (OU) respectively.



AAA Settings of Connection Profile

8. If you select the **Use entire Distinguished Name (DN) as username** option, the system automatically retrieves the user identity. A distinguished name is a unique identification, made up of individual fields that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.



Note: If you have selected the Client Certificate & AAA authentication, then select the **Prefill username from certificate on user login window** option to prefill the secondary username from the client certificate when the user connects via Secure Client VPN module of Cisco Secure Client.

Hide username in login window: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.

---

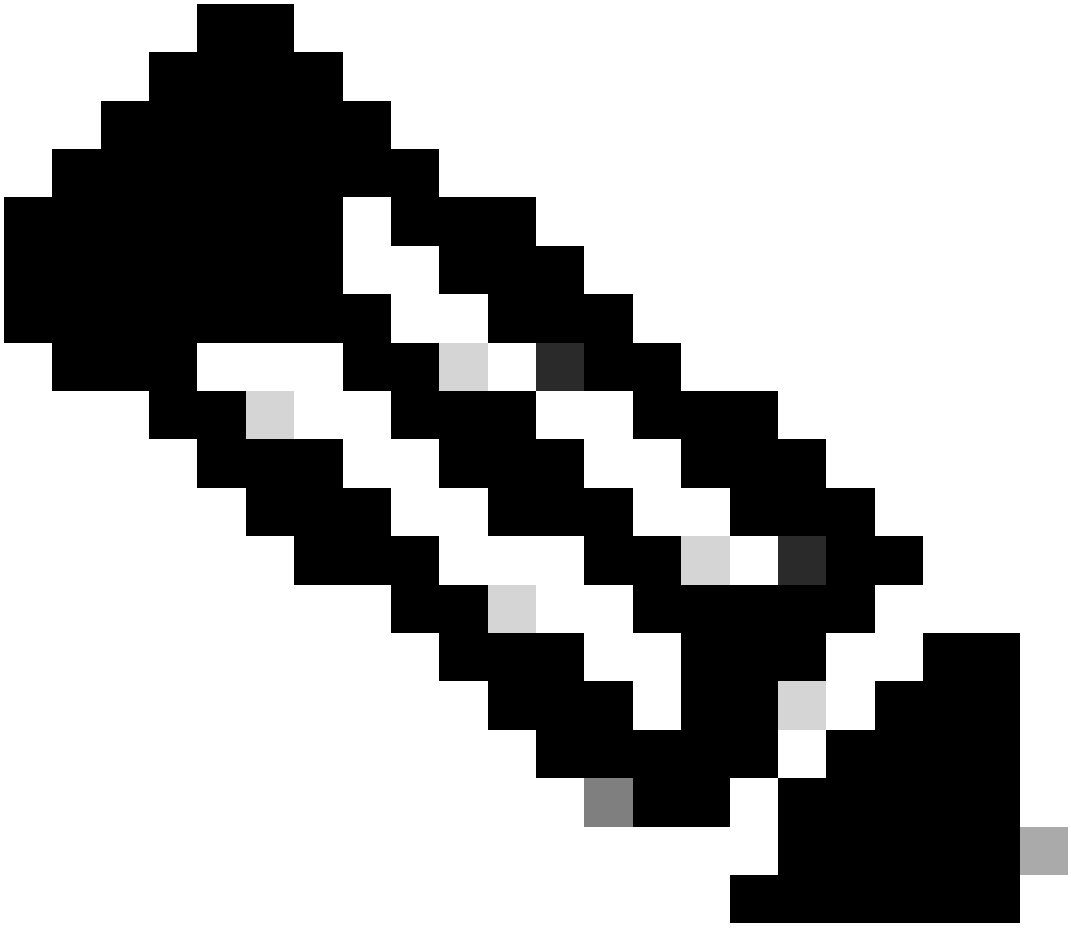
9. For other detailed configuration, refer to Configure Secure Client (AnyConnect) Remote Access VPN on FTD.

10. Upload the CA certificates of the User store certificate and the Machine store certificate to the FTD for successful Validation. Since in this scenario, User store certificate and Machine store certificate are signed by same CA, installing that one CA is enough. If User store certificate and Machine store certificate are signed by different CA, then both those CA certificates must be uploaded to the 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

CA Certificate Installed to FTD from FMC

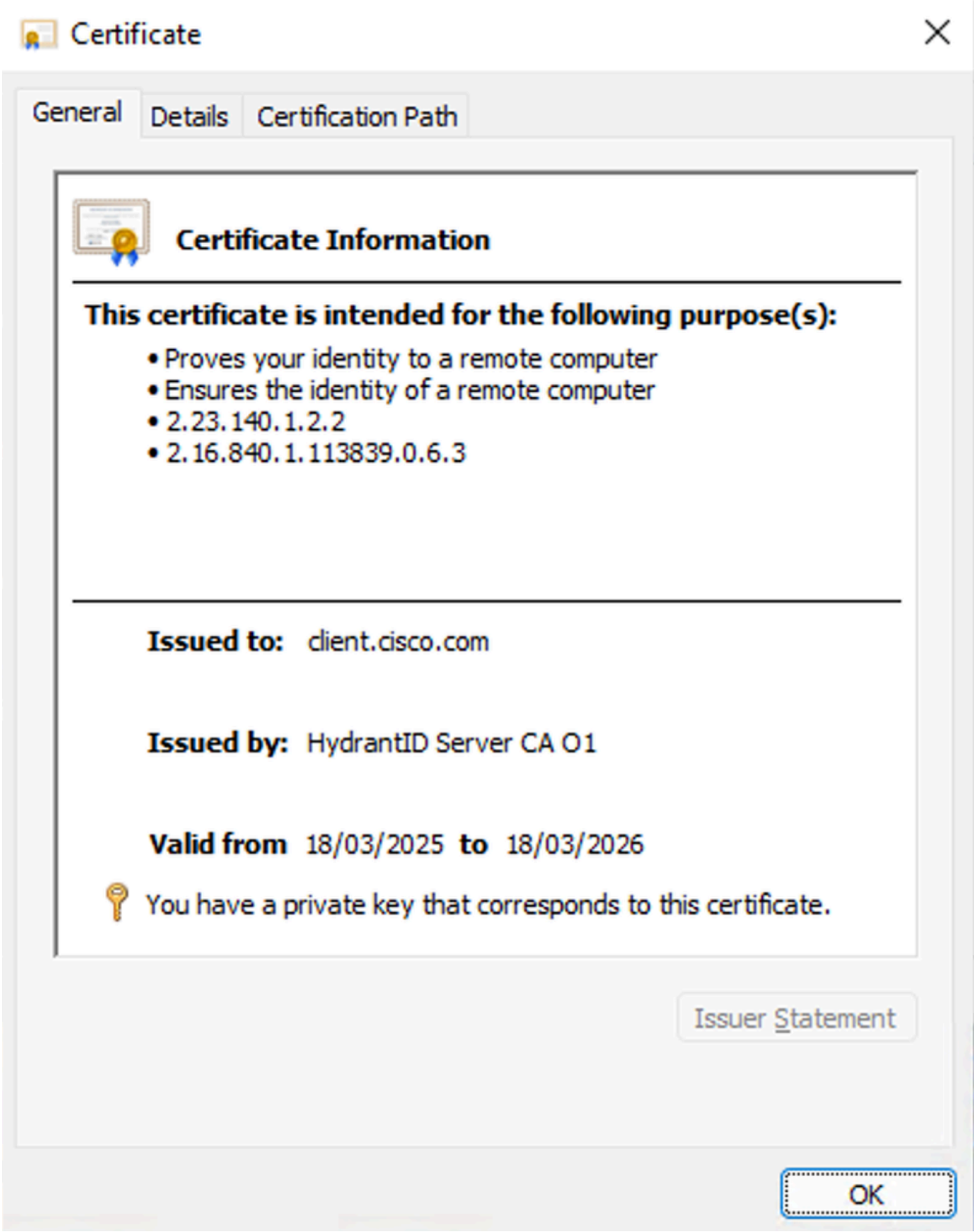


Note: AnyConnect Client Profile must have **CertificateStore** set to **All** and **CertificateStoreOverride** set to **true** if the user does not have admin rights.

Certificates on User Machine

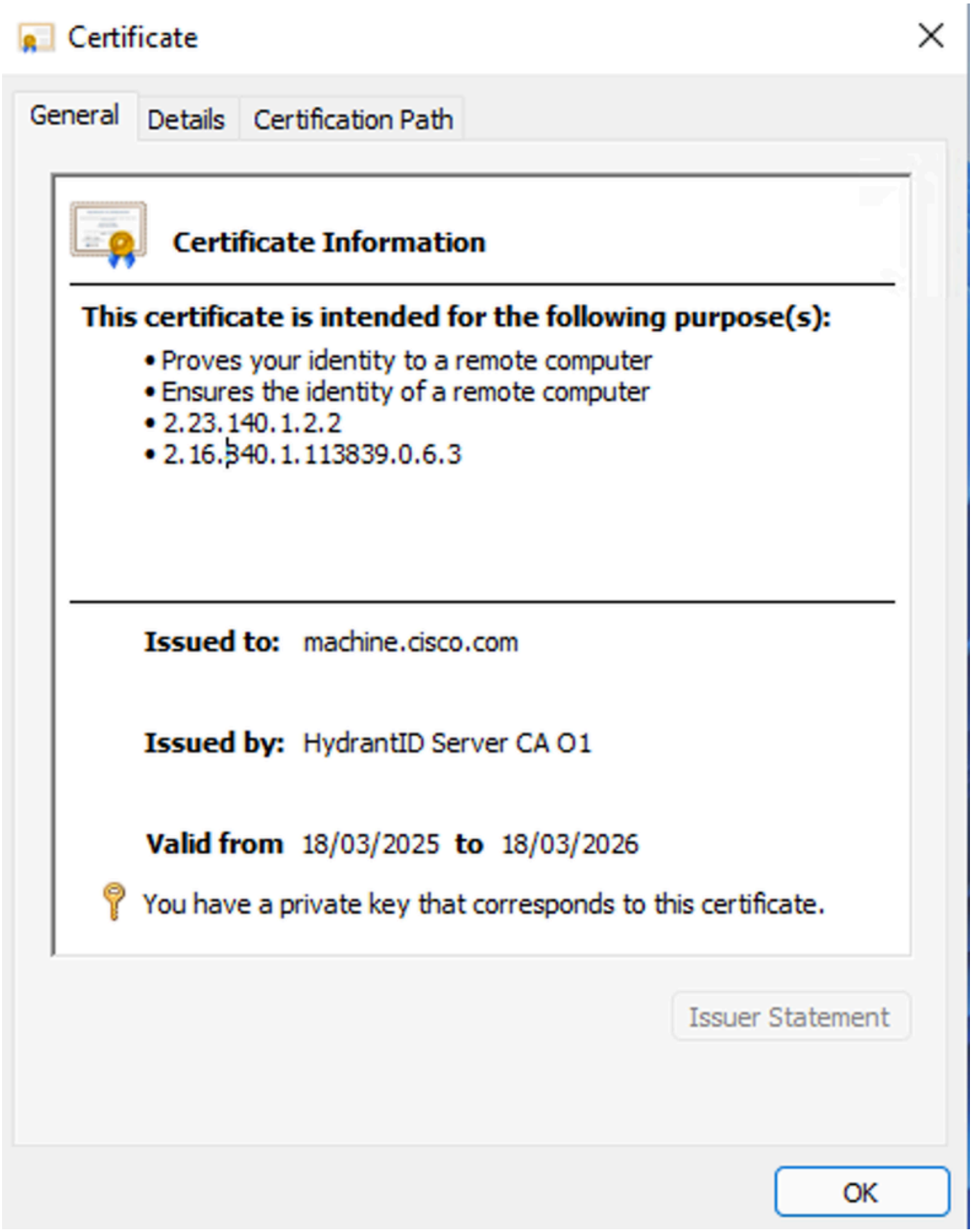
User machine that is supposed to connect to this connection profile must have valid certificates installed in User store and Machine store.

Certificate from User Store:



User Store Certificate

Certificate from Machine Store:



Machine Store Certificate

Verify

1. Verify the connection profile configuration from the FTD CLI:

<#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. Execute this command to verify the connection:

<#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
```

Username client.cisco.comis retrieved from User store certificate CN as map username from Second Certificate is selected in the AAA section. If First Certificate is selected, then username is retrieved from Machine store certificate which is machine.cisco.com.

Troubleshoot

1. Ensure that valid certificates are present in User Certificate store and Machine Certificate store.
2. Collect debugs on FTD to check logs related to certificate validation using **debug crypto ca 14**.
3. Review DART from user machine.

DART logs from Working Scenario:

<#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

****