Meervoudige certificaatverificatie op FTD voor RAVPN configureren

Inhoud

Inleiding

In dit document wordt de procedure beschreven om meervoudige certificaatverificatie te gebruiken voor een beveiligde client bij Firepower Threat Defence (FTD), beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Remote Access VPN (RAVPN)
- Ervaring met Firepower Management Center (FMC)
- Basiskennis van X509-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD - 7,6
- Cisco VCC - 7,6
- Windows 11 met Cisco Secure-client 5.1.4.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Voorafgaand aan softwareversie 7.0 ondersteunt FTD single certificate based authentication, wat betekent dat de gebruiker of de machine kan worden geverifieerd, maar niet beide, voor een enkele verbindingspoging.

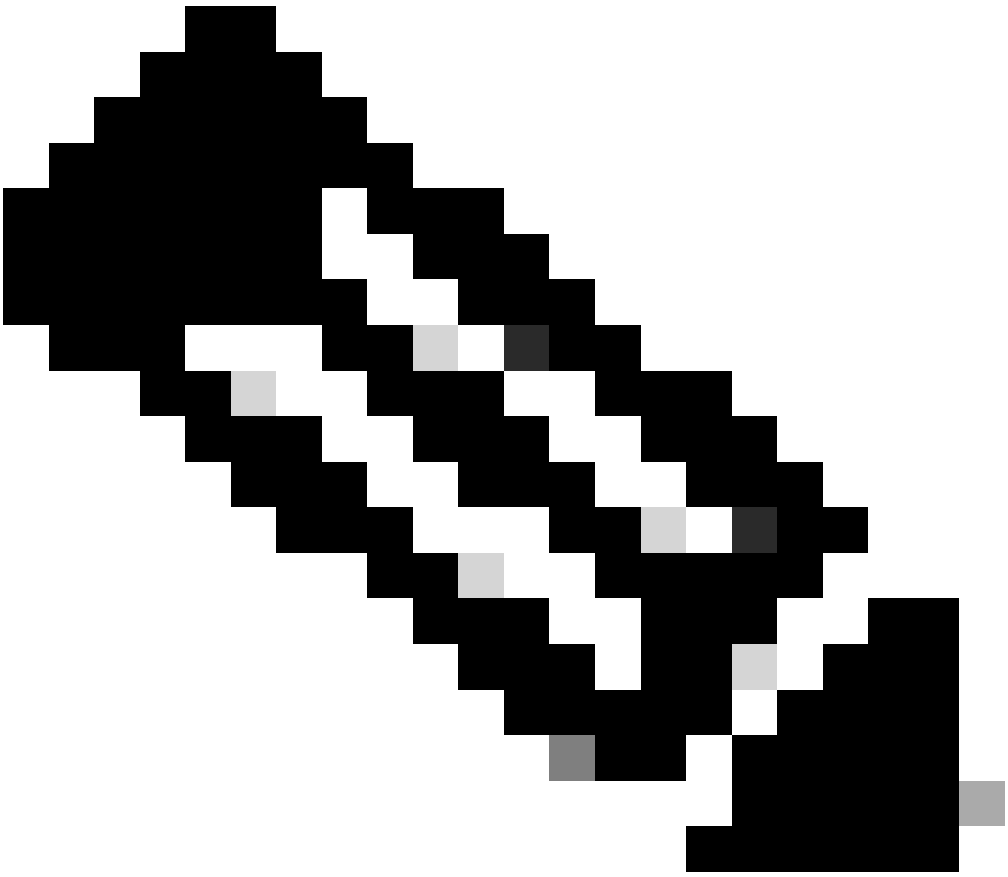
Meervoudige op certificaten gebaseerde verificatie geeft de mogelijkheid om de bedreiging defensevalidate van de machine of het apparaat certificaat, om ervoor te zorgen dat het apparaat een door het bedrijf afgegeven apparaat is, naast het authenticeren van de gebruikers identiteit certificaat om VPN toegang te verlenen met behulp van deSecure client tijdens SSL of IKEv2 EAP fase.

Meervoudige certificaatverificatie beperkt momenteel het aantal certificaten tot twee. Beveiligde client moet ondersteuning voor meervoudige certificaatverificatie aangeven. Als dat niet het geval is, dan gebruikt de gateway een van de legacy-verificatiemethoden of mislukt de verbinding.Secure Clientversie 4.4.04030 of later ondersteunt op Multi-Certificate gebaseerde verificatie.

Configuraties

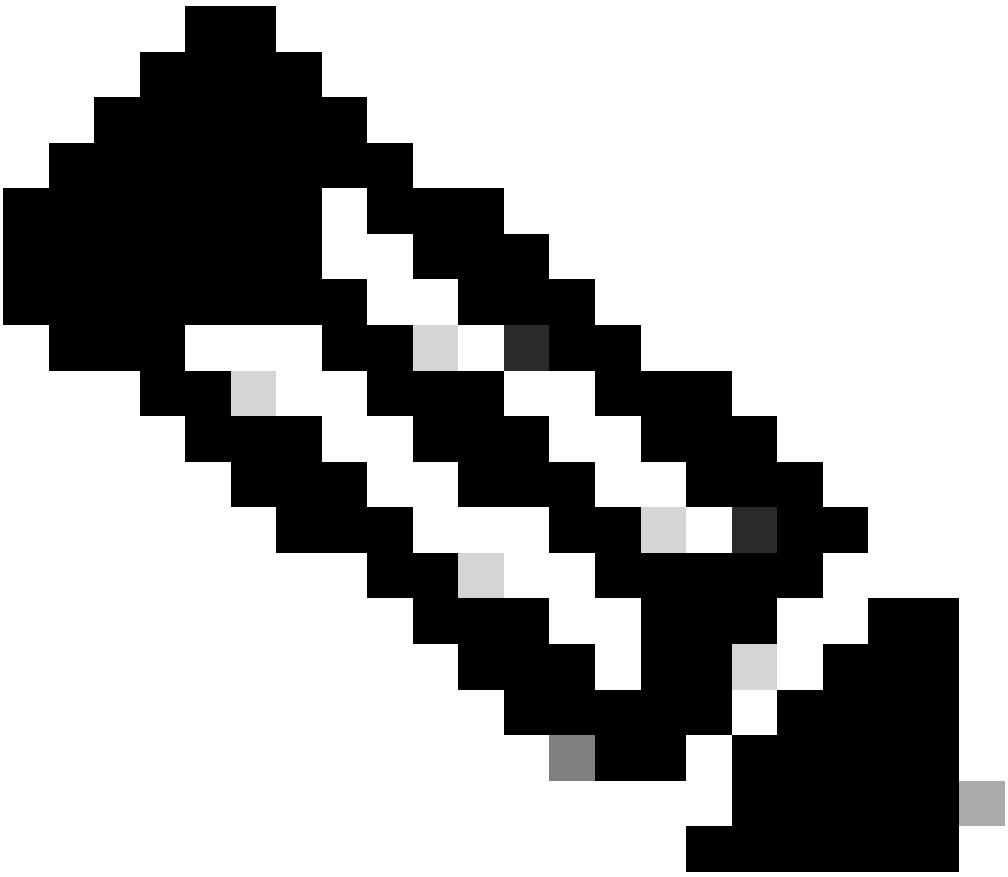
Configuratie op FTD

1. Navigeer naar apparaten > VPN > Externe toegang.
2. Selecteer het VPN-beleid voor externe toegang en klik op Bewerken.



Opmerking: Als u geen externe VPN-toegang hebt geconfigureerd, klikt u op Toevoegen om een nieuw VPN-beleid voor externe toegang te maken.

3. Selecteer en bewerk een verbindingsprofiel om meervoudige certificaatverificatie te configureren.
4. Klik op AAA-instellingen en kies Verificatiemethode als alleen clientcertificaat of alleen clientcertificaat en AAA.

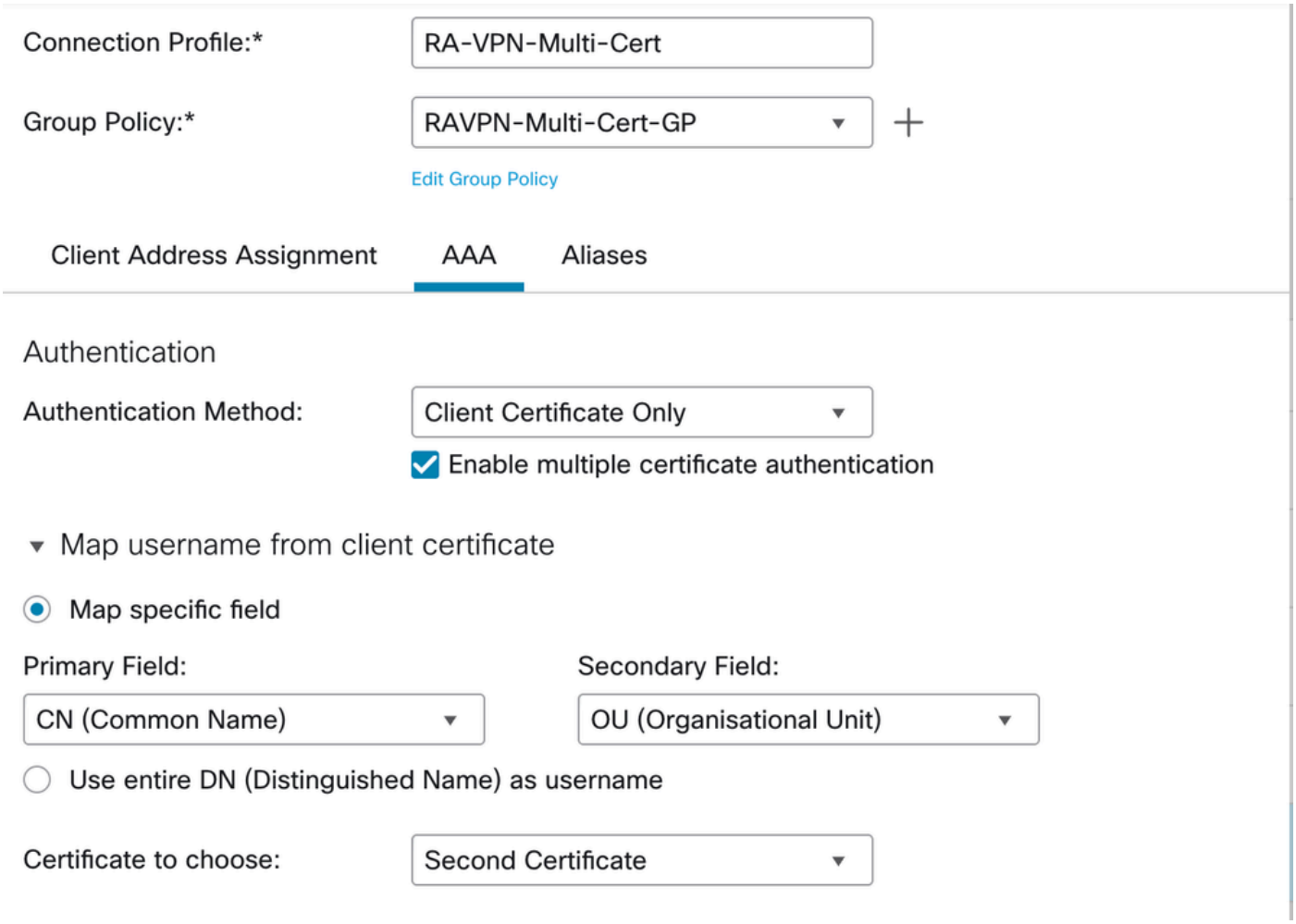


Opmerking: Selecteer de verificatieserver als u de methode Clientcertificaat en AAA-verificatie hebt geselecteerd.

5. Selecteer het selectievakje Meerdere certificaatverificatie inschakelen.
6. Kies een van de certificaten toMap gebruikersnaam van client certificaat:
   - Eerste certificaat - Selecteer deze optie om de gebruikersnaam toe te wijzen van het machinecertificaat dat van de VPN-client is verzonden.
   - Tweede certificaat— Selecteer deze optie om de gebruikersnaam toe te wijzen van het gebruikerscertificaat dat van de client is verzonden.

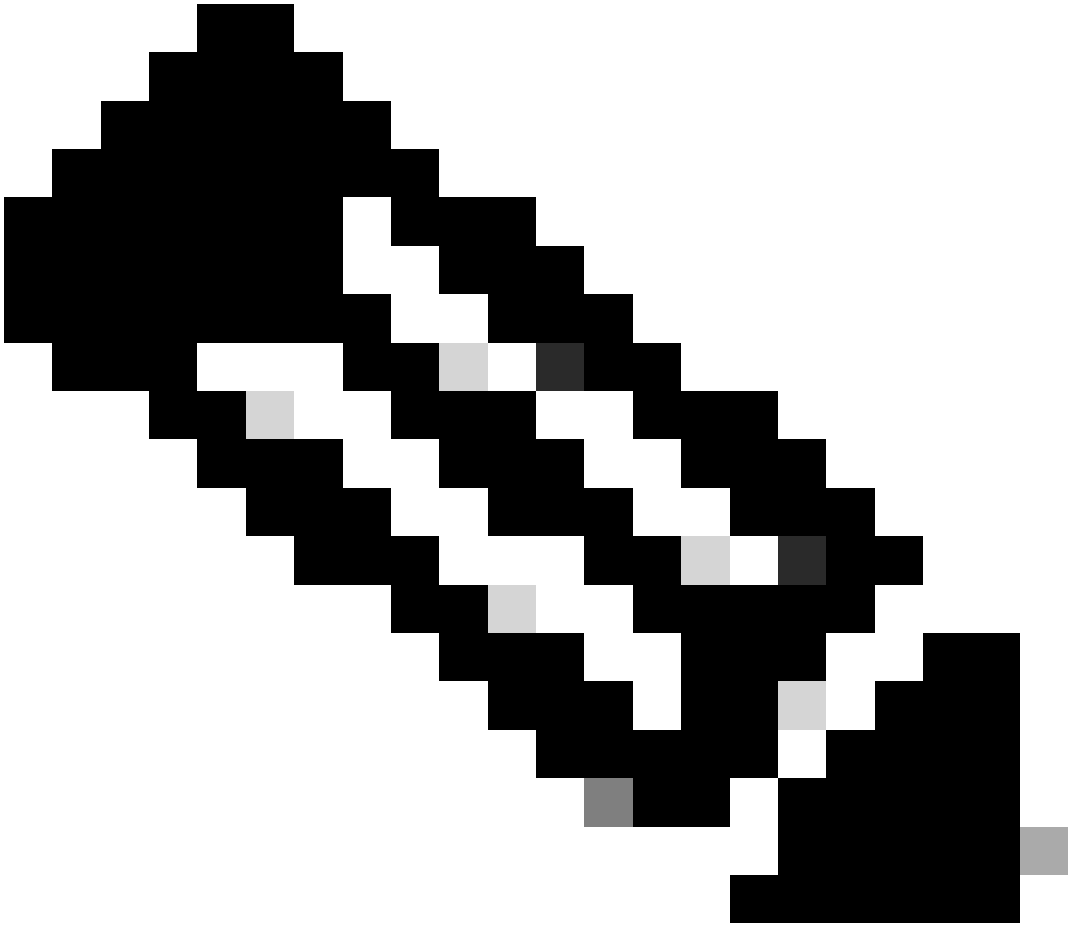
   De gebruikersnaam die vanaf de client wordt verzonden, wordt gebruikt als de VPN-sessiegebruikersnaam wanneer alleen certificaatverificatie is ingeschakeld. Wanneer AAA- en certificaatverificatie is ingeschakeld, is de VPN-sessiegebruikersnaam gebaseerd op de optie Prefill.
7. Als u de specifieke optie Map selecteert, die de gebruikersnaam van het clientcertificaat bevat, worden in de primaire en de secundaire velden de standaardwaarden weergegeven:

algemene naam (CN)respectievelijk Organisatorische eenheid (OU).



AAA-instellingen van het verbindingsprofiel

8. Als u de optie De volledige Distinguished Name (DN) gebruiken als gebruikersnaam selecteert, wordt de gebruikersidentiteit automatisch door het systeem opgehaald. Een voorname naam is een unieke identificatie, die bestaat uit afzonderlijke velden die kunnen worden gebruikt als identificatie bij het koppelen van gebruikers aan een verbindingsprofiel. DN-regels worden gebruikt voor verbeterde certificaatverificatie.



Opmerking: Als u het clientcertificaat en de AAA-verificatie hebt geselecteerd, selecteert u de optie Prefill-gebruikersnaam uit certificaat in het gebruikerslogvenster om de secundaire gebruikersnaam uit het clientcertificaat voor te vullen wanneer de gebruiker verbinding maakt via de beveiligde client-VPN-module van Cisco Secure Client.

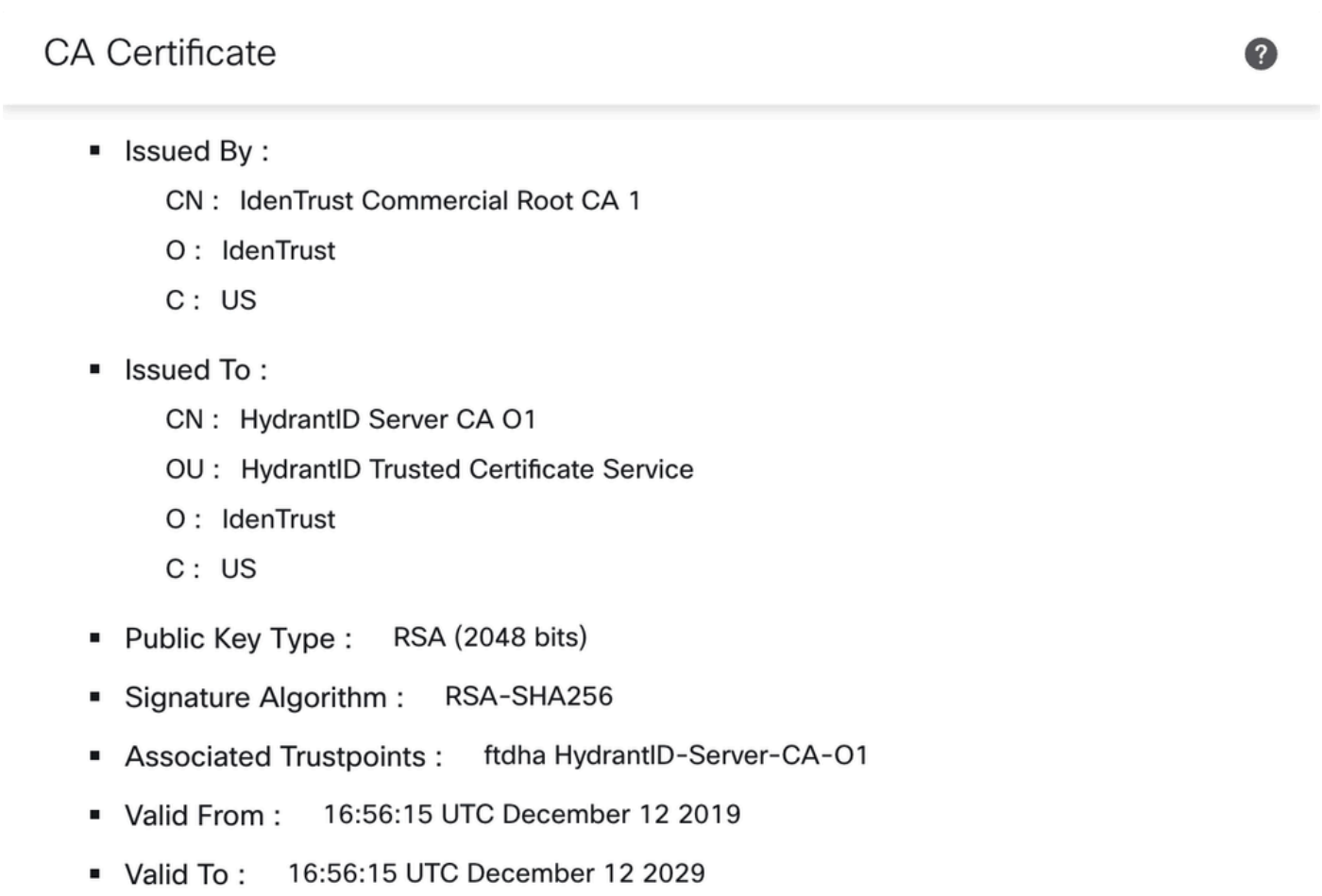
Gebruikersnaam verbergen in inlogvenster: De secundaire gebruikersnaam is vooraf ingevuld van het clientcertificaat, maar verborgen voor de gebruiker, zodat de gebruiker de voorgevulde gebruikersnaam niet wijzigt.

---

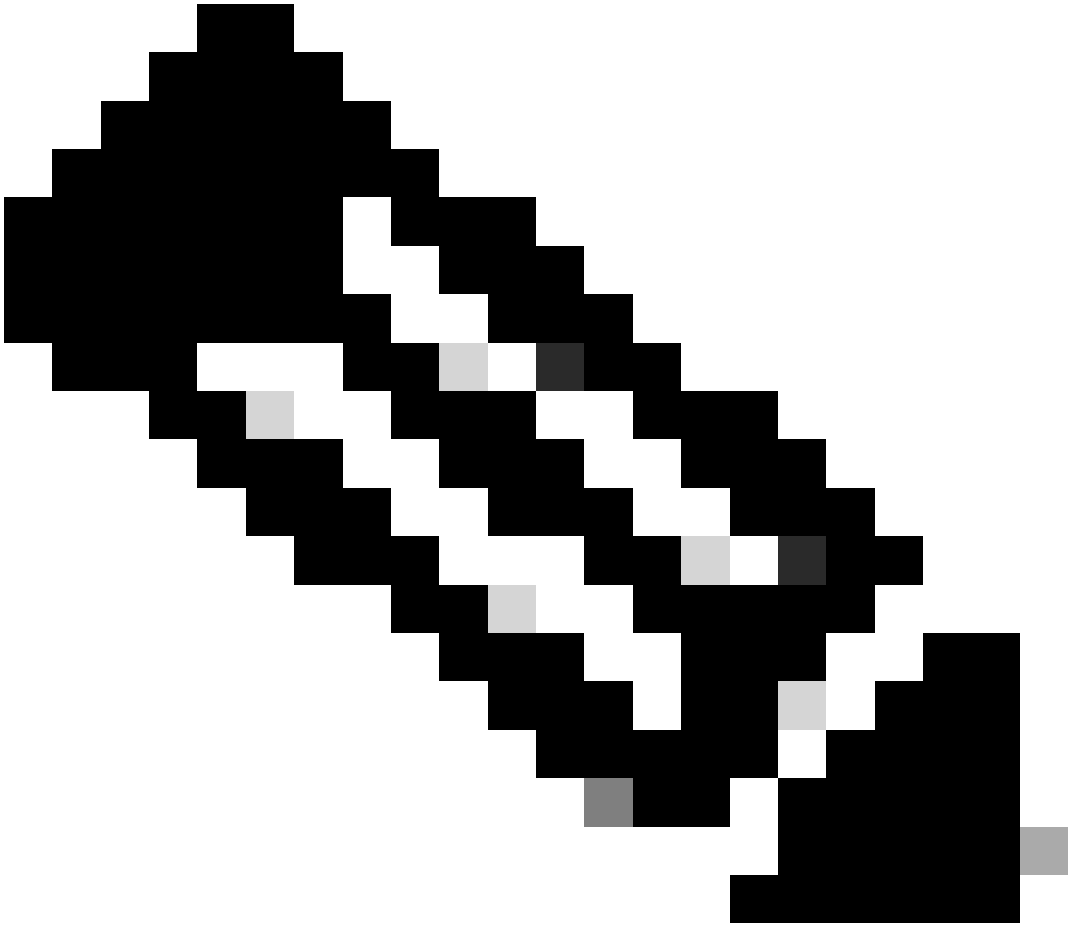
9. Raadpleeg voor andere gedetailleerde configuratie Secure Client (AnyConnect) Remote Access VPN op FTD configureren.

10. Upload de CA-certificaten van het User Store-certificaat en het Machine Store-certificaat naar het FTD voor succesvolle validatie. Aangezien in dit scenario het certificaat van de gebruikersopslag en het certificaat van de machinereservering door zelfde CA worden ondertekend, die installeren dat één CA genoeg is. Als Gebruikersopslagcertificaat en Machineopslagcertificaat zijn ondertekend door verschillende CA, moeten beide CA-certificaten

worden geüpload naar de FTD.



CA-certificaat geïnstalleerd op FTD vanuit het VCC

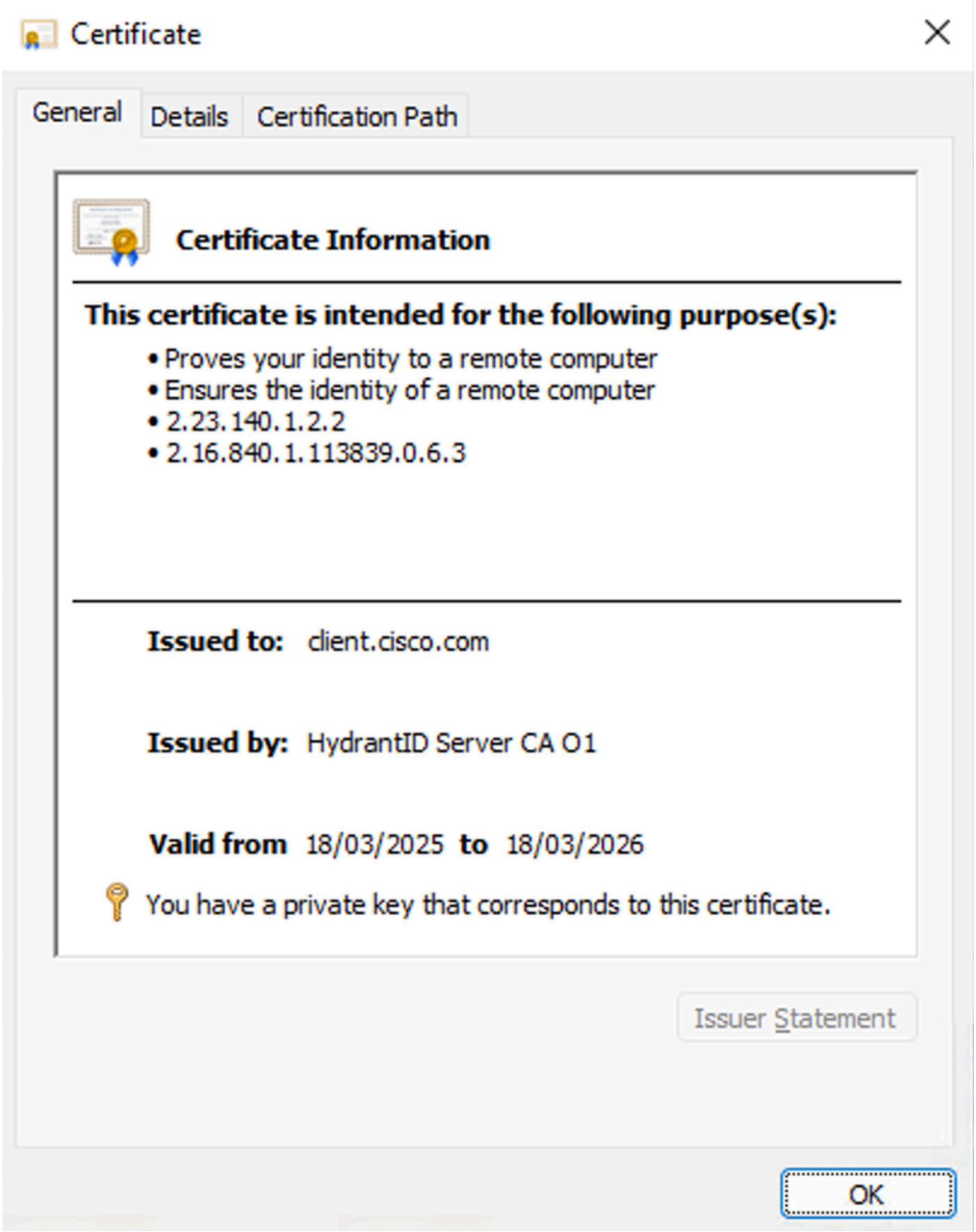


Opmerking: AnyConnect-clientprofiel moet CertificateStore hebben ingesteld op All en CertificateStoreOverride op true als de gebruiker geen beheerrechten heeft.

Certificaten op gebruikersmachine

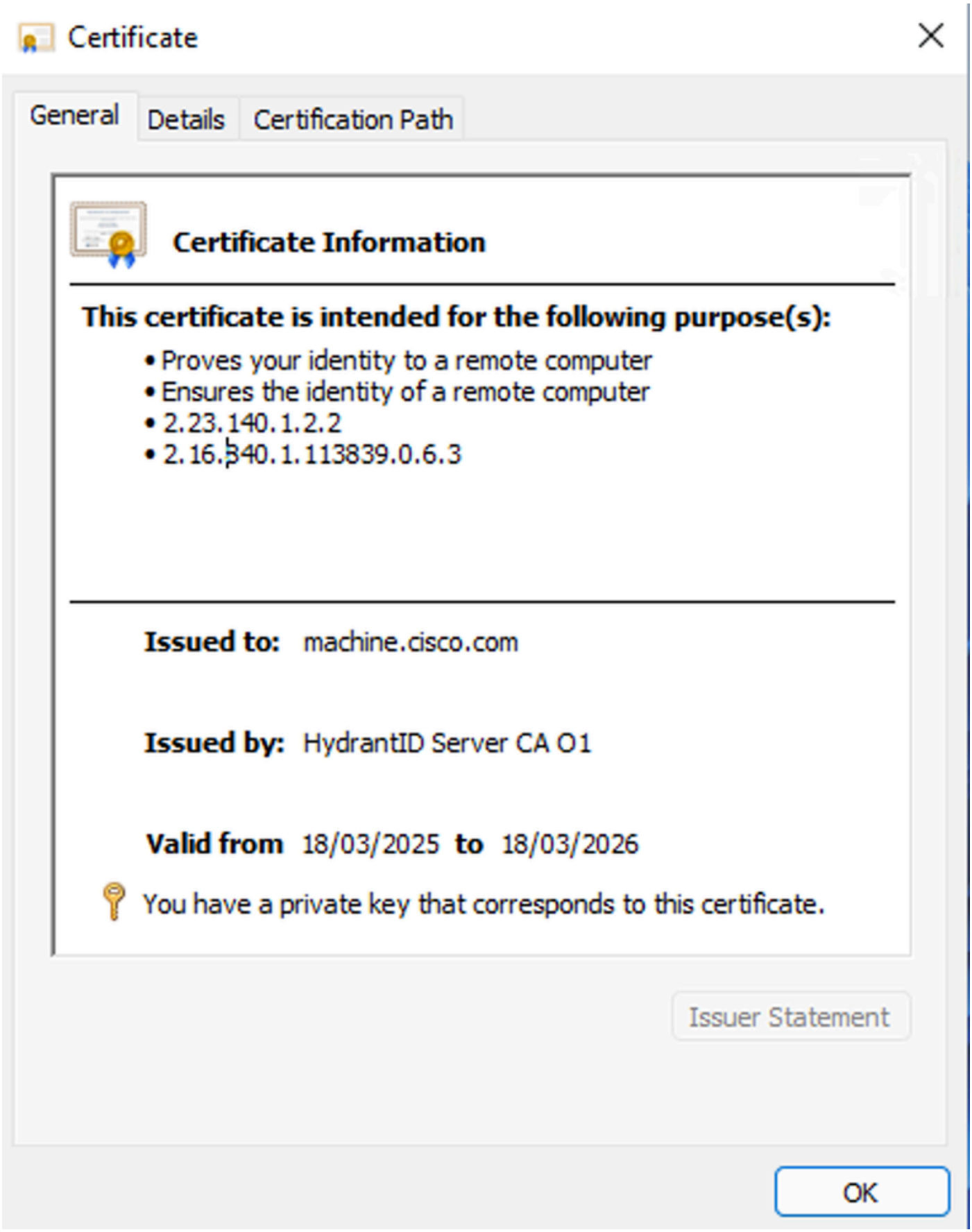
Voor een gebruikersmachine die verbinding moet maken met dit verbindingsprofiel, moeten geldige certificaten zijn geïnstalleerd in de winkel van de gebruiker en in de winkel van de machine.

Certificaat uit de Gebruikerswinkel:



Gebruikerswinkelcertificaat

Certificaat van Machine Store:



Certificaat van machineleesbare opslag

Verifiëren

1. Controleer de configuratie van het verbindingsprofiel vanuit de 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. Voer deze opdracht uit om de verbinding te verifiëren:

<#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
```

Gebruikersnaam client.cisco.com wordt opgehaald uit User Store certificaat CN als kaartgebruikersnaam van Tweede certificaat wordt geselecteerd in de AAA-sectie. Als Eerste certificaat is geselecteerd, wordt de gebruikersnaam opgehaald uit het machinerespot-certificaat dat machine.cisco.com is.

Problemen oplossen

1. Zorg ervoor dat er geldige certificaten aanwezig zijn in het opslaan van gebruikerscertificaten en machinecertificaten.

2. Verzamel debugs op FTD om logboeken met betrekking tot certificaatbevestiging te controleren met behulp van debug crypto ca 14.
3. DART bekijken van gebruikersmachine.

DART-logbestanden van het werkscenario:

<#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

****

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.