Mehrere Zertifikatauthentifizierung auf FTD für RAVPN konfigurieren

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Konfigurationen

- Konfiguration auf FTD
- Zertifikate auf Benutzercomputer

Überprüfung

Fehlerbehebung

Einleitung

In diesem Dokument wird das Verfahren zur Verwendung der Authentifizierung mit mehreren Zertifikaten für den sicheren Client auf dem von FMC verwalteten FirePOWER Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes zum Remote Access VPN (RAVPN)
- Erfahrung mit FirePOWER Management Center (FMC)
- Grundkenntnisse der X509-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Vor der Softwareversion 7.0 unterstützt FTD eine einzelne zertifikatbasierte Authentifizierung, d. h. entweder der Benutzer oder das System kann authentifiziert werden, aber nicht beide, für einen einzigen Verbindungsversuch.

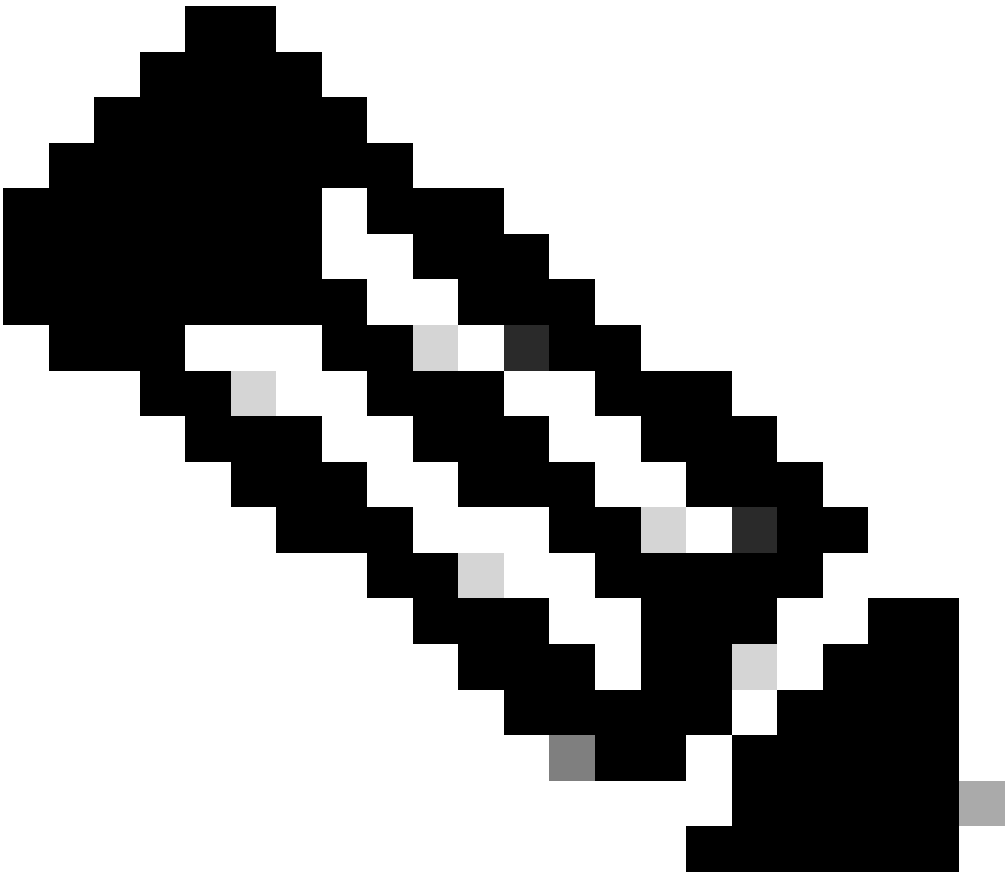
Die Authentifizierung auf Basis mehrerer Zertifikate ermöglicht es, dass die Bedrohungsabwehr das Computer- oder Gerätezertifikat validiert, um sicherzustellen, dass es sich bei dem Gerät um ein vom Unternehmen ausgestelltes Gerät handelt. Außerdem wird das Benutzeridentitätszertifikat authentifiziert, um den VPN-Zugriff über den Secure Client während der SSL- oder IKEv2-EAP-Phase zuzulassen.

Bei der Authentifizierung mit mehreren Zertifikaten ist die Anzahl der Zertifikate derzeit auf zwei beschränkt. Secure Client muss angeben, dass die Authentifizierung mit mehreren Zertifikaten unterstützt wird. Ist dies nicht der Fall, verwendet das Gateway eine der vorherigen Authentifizierungsmethoden oder schlägt die Verbindung fehl.Secure Clientversion 4.4.04030 oder höher unterstützt die Multi-Certificate-basierte Authentifizierung.

Konfigurationen

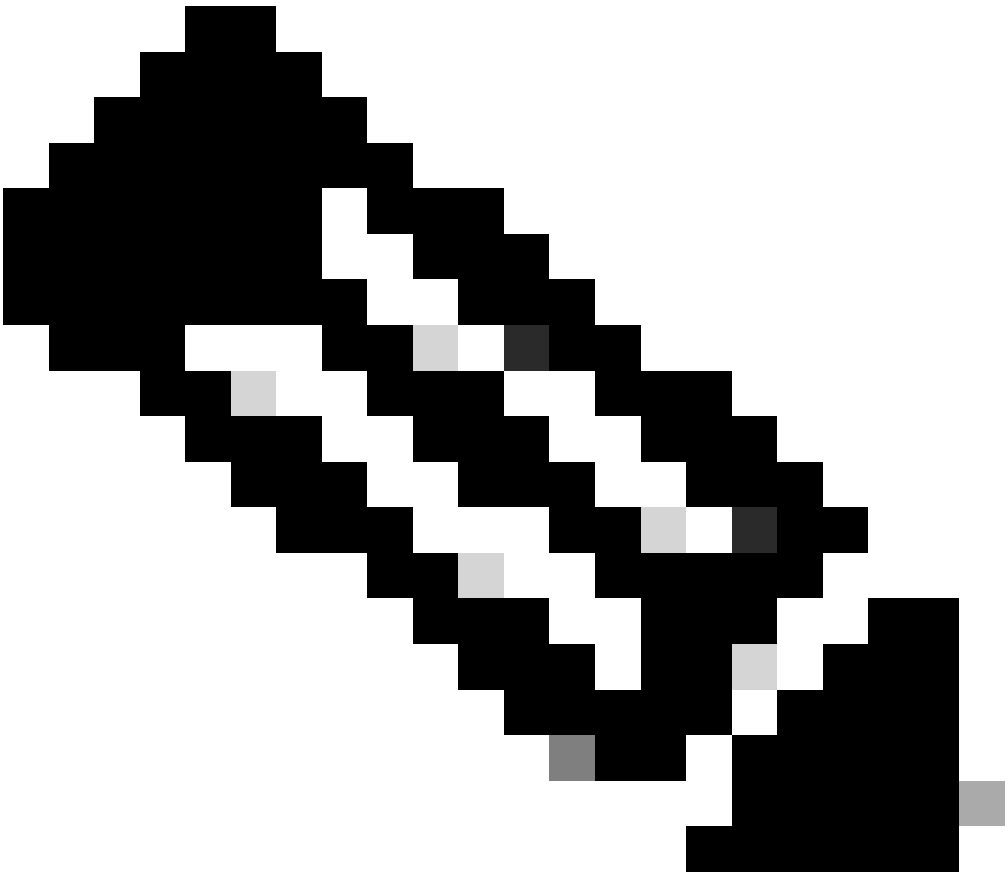
Konfiguration auf FTD

1. Navigieren Sie zuGeräte > VPN > RAS.
2. Wählen Sie die VPN-Richtlinie für den Remotezugriff aus, und klicken Sie auf Bearbeiten.



Anmerkung: Wenn Sie kein Remotezugriff-VPN konfiguriert haben, klicken Sie auf Hinzufügen, um eine neue Richtlinie für den Remotezugriff-VPN zu erstellen.

3. Wählen Sie ein Verbindungsprofil aus, und bearbeiten Sie es, um die Authentifizierung mehrerer Zertifikate zu konfigurieren.
4. Klicken Sie auf AAA-Einstellungen, und wählen Sie Authentication Method als Client Certificate Only (Nur Client-Zertifikat) oder Client Certificate & AAA aus.

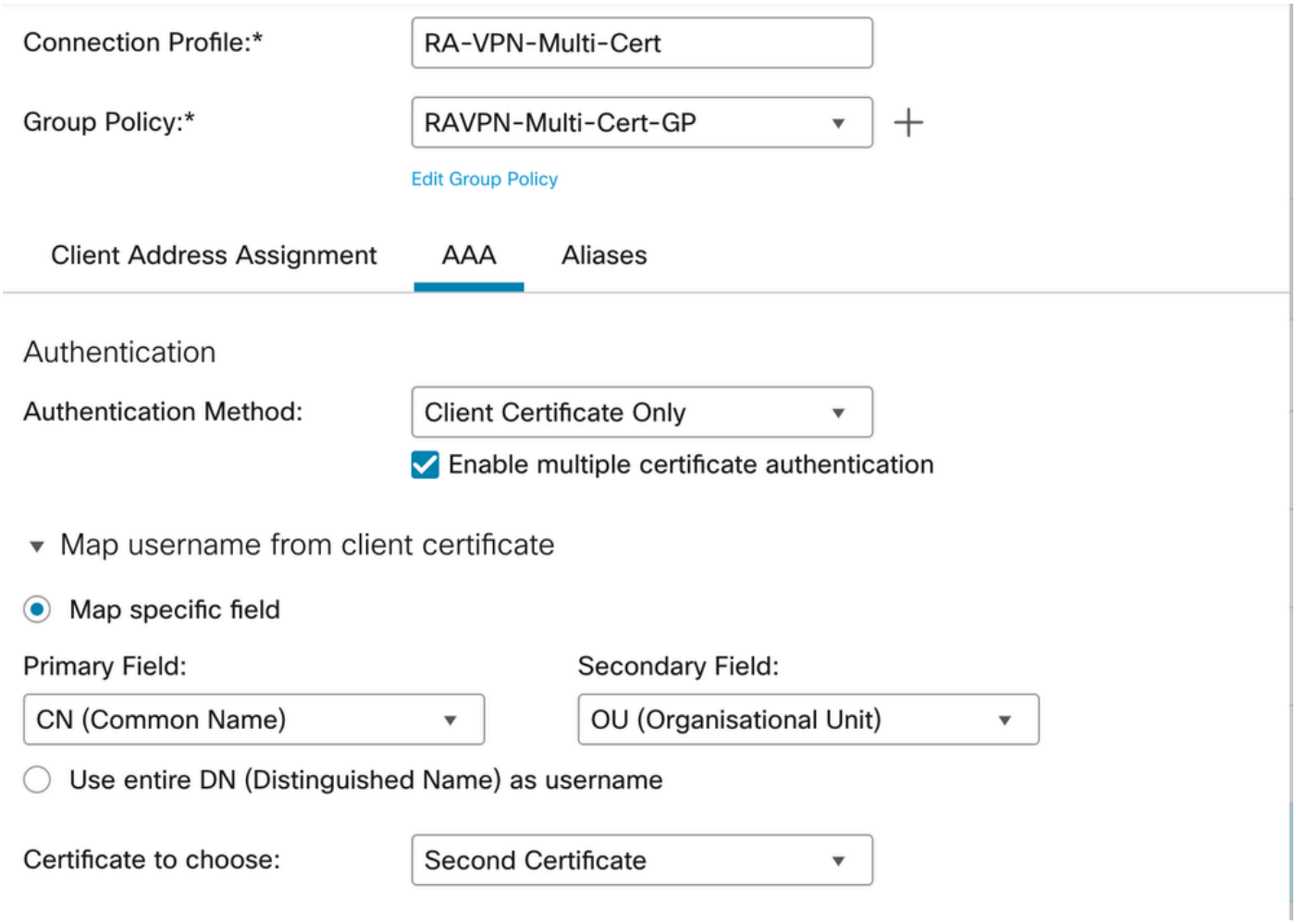


Anmerkung: Wählen Sie den Authentifizierungsserver aus, wenn Sie die Authentifizierungsmethode Clientzertifikat und AAA ausgewählt haben.

5. Aktivieren Sie das Kontrollkästchen Mehrfachzertifikatauthentifizierung aktivieren.
6. Wählen Sie eines der Zertifikate aus, die dem Clientzertifikat zugeordnet werden sollen:
    - Erstes Zertifikat - Wählen Sie diese Option aus, um den Benutzernamen des Computerzertifikats zuzuordnen, das vom VPN-Client gesendet wurde.
    - Zweites Zertifikat - Wählen Sie diese Option aus, um den Benutzernamen aus dem Benutzerzertifikat zuzuordnen, das vom Client gesendet wurde.

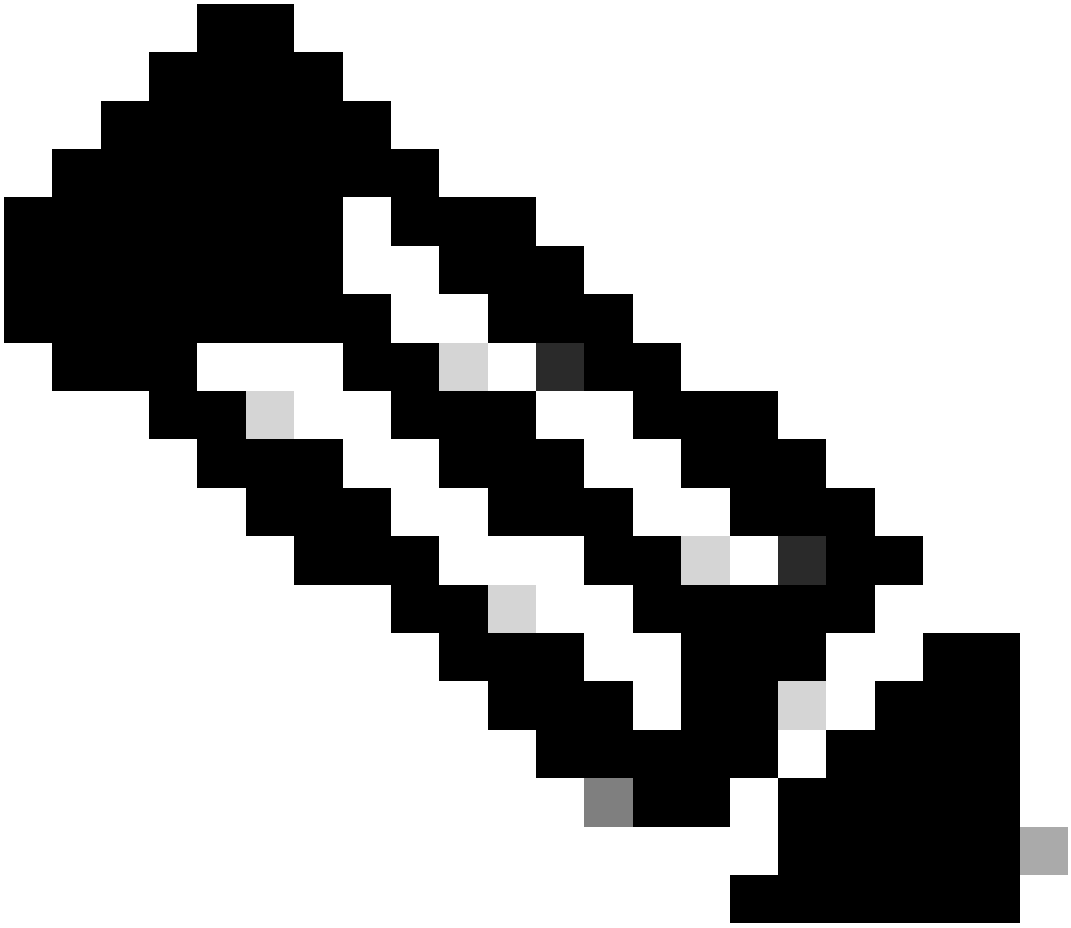
    Der vom Client gesendete Benutzername wird als VPN-Sitzungsbenutzername verwendet, wenn die Authentifizierung nur für Zertifikate aktiviert ist. Wenn AAA und die Zertifikatsauthentifizierung aktiviert sind, basiert der VPN-Sitzungsbenutzername auf der Option "Prefill" (Vorfüllen).
7. Wenn Sie die Option Spezifisches Feld zuordnen auswählen, die den Benutzernamen aus dem Clientzertifikat enthält, werden in den Feldern Primär und Sekundär Standardwerte

angezeigt: Allgemeiner Name (CN) und Organisationseinheit (OU).



AAA-Einstellungen des Verbindungsprofils

8. Wenn Sie die Option Gesamten Distinguished Name (DN) als Benutzernamen verwenden auswählen, ruft das System automatisch die Benutzeridentität ab. Ein Distinguished Name ist eine eindeutige Identifikation, die aus einzelnen Feldern besteht, die beim Zuordnen von Benutzern zu einem Verbindungsprofil als Identifikation verwendet werden können. DN-Regeln werden für die erweiterte Zertifikatsauthentifizierung verwendet.



Anmerkung: Wenn Sie das Client-Zertifikat und die AAA-Authentifizierung ausgewählt haben, wählen Sie die Option Benutzername vom Zertifikat bei Benutzeranmeldung vorfüllen aus, um den sekundären Benutzernamen vom Client-Zertifikat vorauszufüllen, wenn der Benutzer über das Secure Client VPN-Modul von Cisco Secure Client eine Verbindung herstellt.

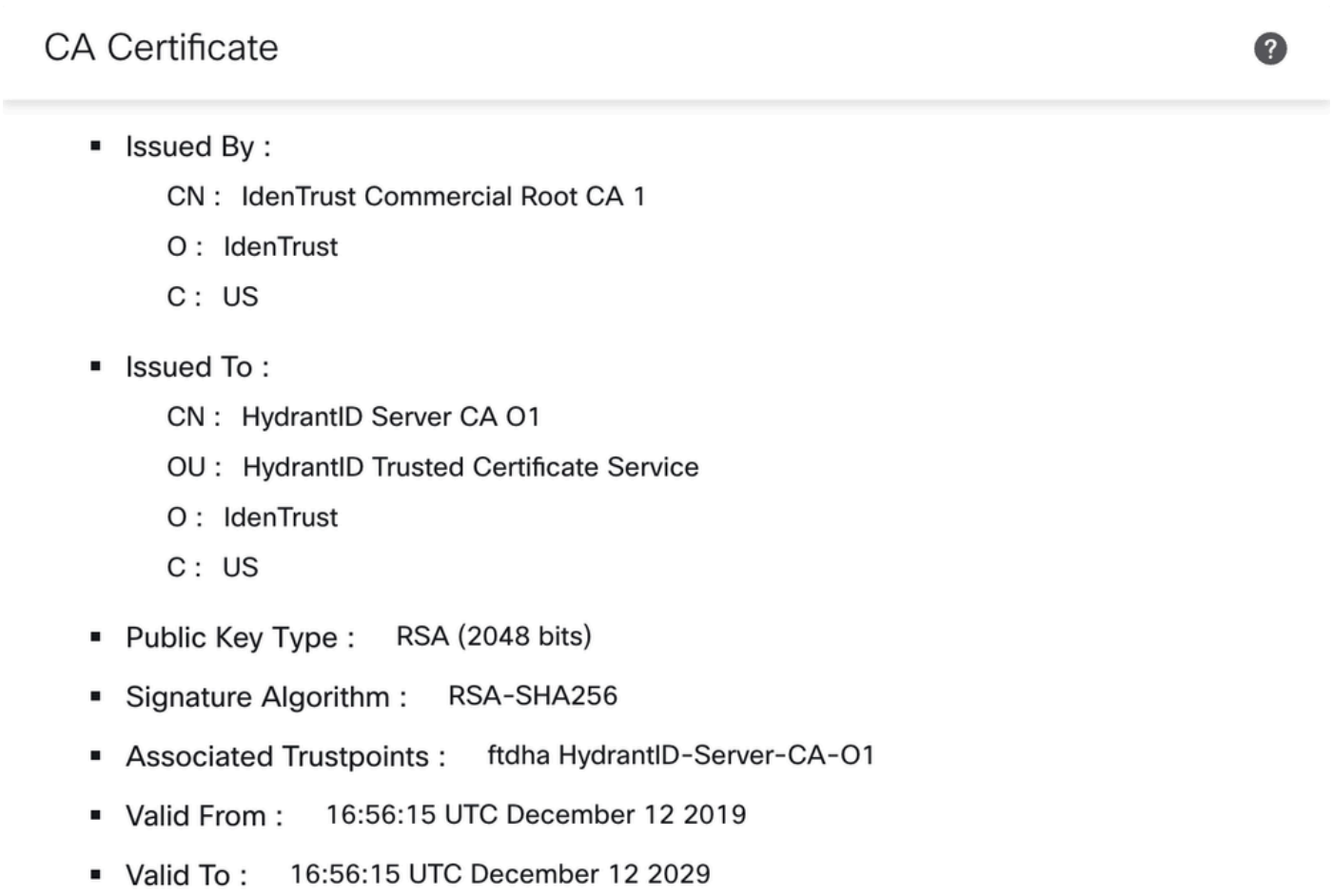
Benutzernamen im Anmeldefenster ausblenden: Der sekundäre Benutzername wird aus dem Clientzertifikat ausgefüllt, für den Benutzer jedoch ausgeblendet, sodass der Benutzer den ausgefüllten Benutzernamen nicht ändert.

---

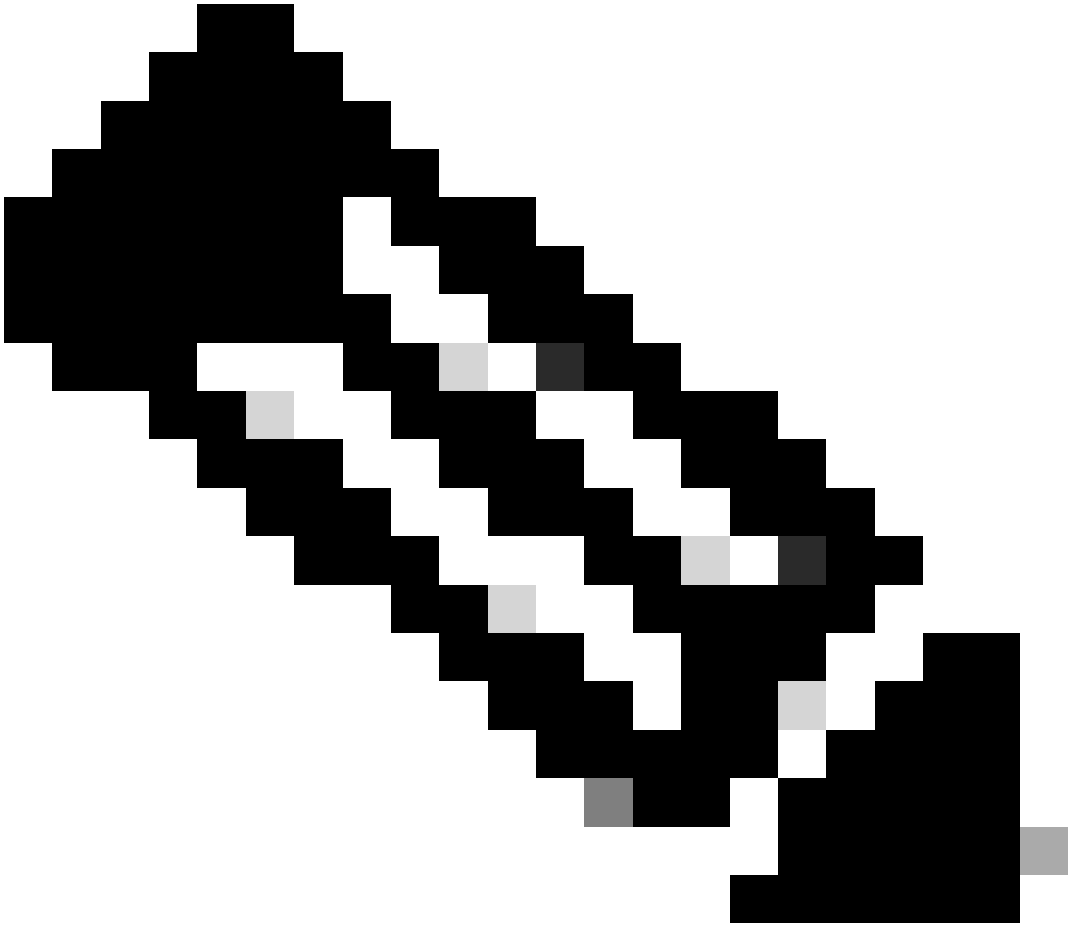
9. Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren von Secure Client (AnyConnect) Remote Access VPN auf FTD.

10. Laden Sie die Zertifizierungsstellenzertifikate des Benutzerspeicherzertifikats und des Computerspeicherzertifikats zur erfolgreichen Validierung in das FTD hoch. Da in diesem Szenario Benutzerspeicherzertifikat und Computerspeicherzertifikat von derselben Zertifizierungsstelle signiert werden, reicht es aus, diese eine Zertifizierungsstelle zu installieren.

Wenn das Benutzerspeicherzertifikat und das Computerspeicherzertifikat von einer anderen Zertifizierungsstelle signiert werden, müssen beide Zertifizierungsstellenzertifikate in die FTD hochgeladen werden.



CA-Zertifikat von FMC auf FTD installiert

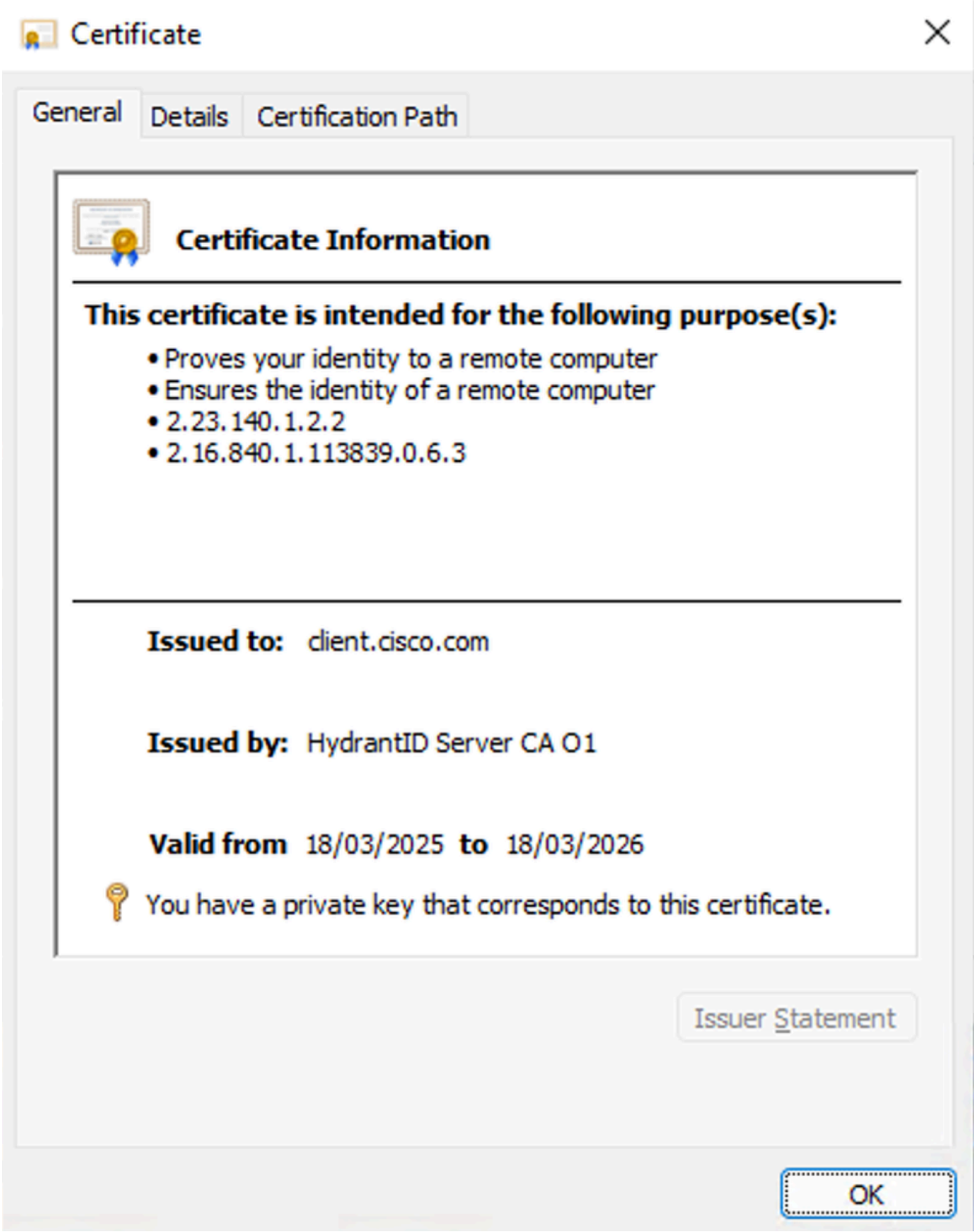


Anmerkung: Für das AnyConnect-Clientprofil muss CertificateStore auf All (Alle) und CertificateStoreOverride auf true festgelegt sein, wenn der Benutzer keine Administratorrechte hat.

Zertifikate auf Benutzercomputer

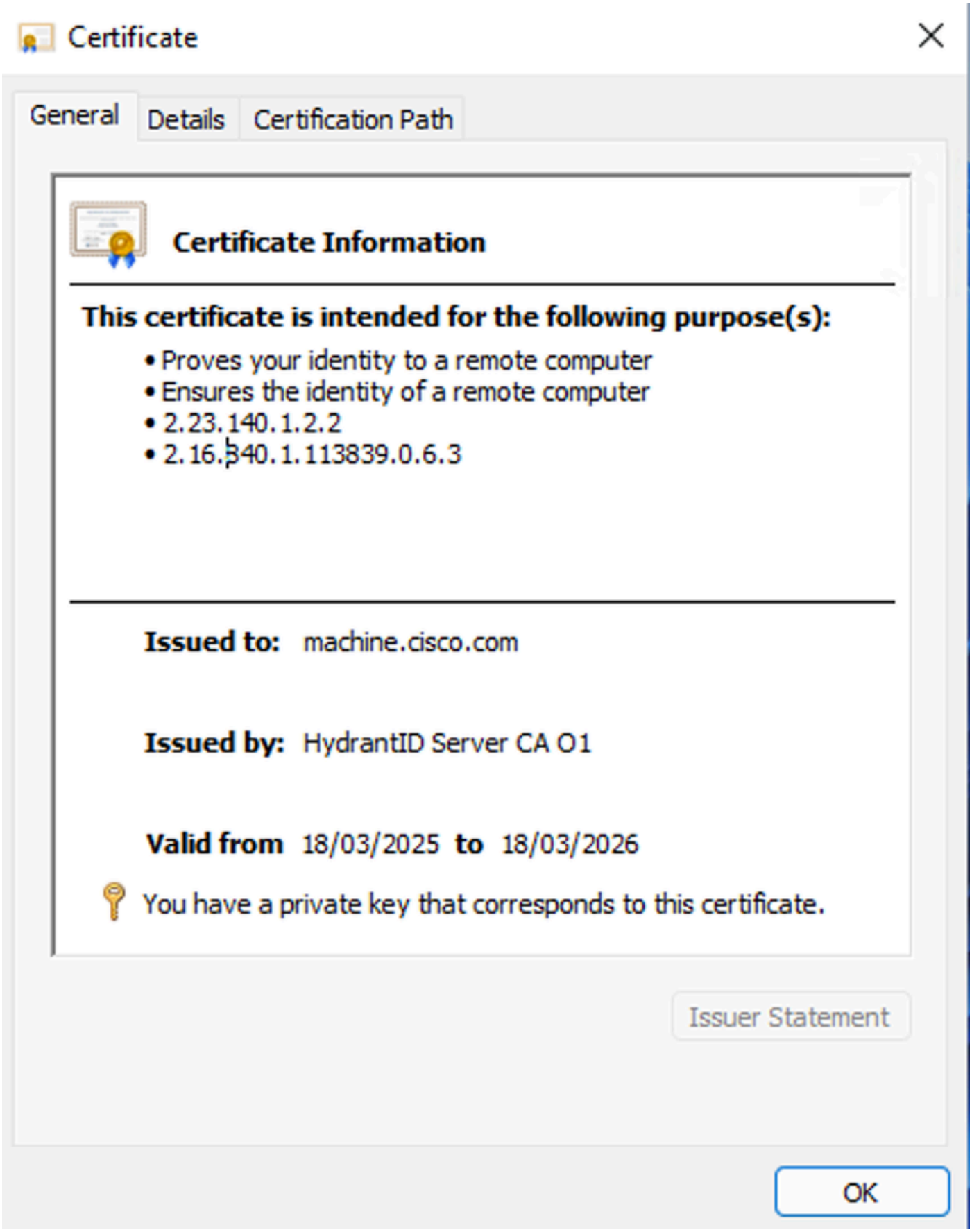
Auf dem Benutzercomputer, der eine Verbindung mit diesem Verbindungsprofil herstellen soll, müssen gültige Zertifikate im Benutzerspeicher und Computerspeicher installiert sein.

Zertifikat aus dem Benutzerspeicher:



Zertifikat des Benutzerspeichers

Zertifikat aus dem Computerspeicher:



Zertifikat für den Computerspeicher

Überprüfung

1. Überprüfen Sie die Konfiguration des Verbindungsprofils über die 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. Führen Sie diesen Befehl aus, um die Verbindung zu überprüfen:

<#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
```

Der Benutzername client.cisco.com, der von der CN des Benutzerspeicherzertifikats abgerufen wird, wird im AAA-Abschnitt als Zuordnung des Benutzernamens aus dem zweiten Zertifikat ausgewählt. Wenn das erste Zertifikat ausgewählt ist, wird der Benutzername aus dem Zertifikat des Computerspeichers abgerufen, das machine.cisco.com lautet.

Fehlerbehebung

1. Stellen Sie sicher, dass im Benutzerzertifikatspeicher und im Computerzertifikatspeicher gültige Zertifikate vorhanden sind.

2. Sammeln Sie Debug-Meldungen auf FTD, um Protokolle zur Zertifikatsvalidierung mithilfe von debug crypto ca. 14 zu überprüfen.
3. Überprüfen Sie DART vom Benutzergerät.

DART-Protokolle aus dem Arbeitsszenario:

<#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

****

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.