Configurazione dell'autenticazione di più certificati su FTD per RAVPN

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Configurazioni

- Configurazione su FTD
- Certificati sul computer utente

Verifica

Risoluzione dei problemi

Introduzione

In questo documento viene descritta la procedura per utilizzare l'autenticazione con più certificati per client sicuri su Firepower Threat Defense (FTD) gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di RAVPN (Remote Access VPN)
- Esperienza con Firepower Management Center (FMC)
- Conoscenze base dei certificati X509

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Prima della versione 7.0 del software, FTD supporta l'autenticazione basata su singolo certificato, il che significa che l'utente o il computer possono essere autenticati, ma non entrambi, per un singolo tentativo di connessione.

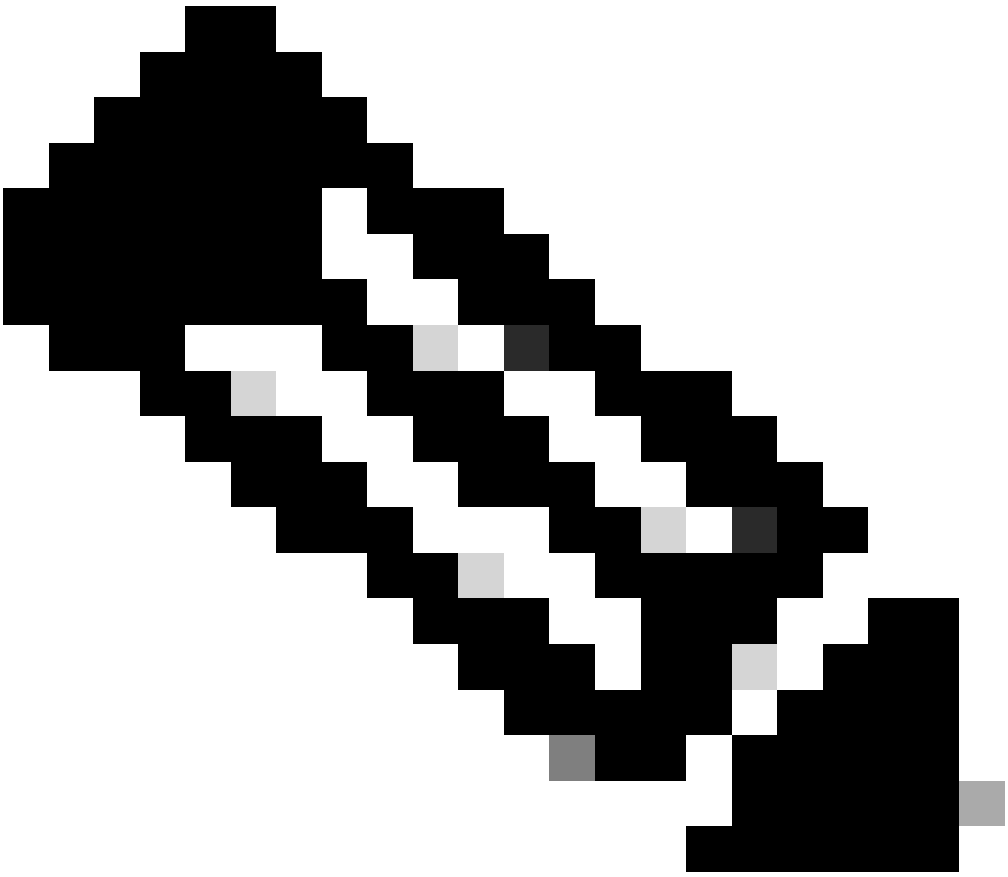
L'autenticazione basata su più certificati consente di convalidare la minaccia sul computer o sul certificato del dispositivo, di garantire che il dispositivo sia un dispositivo emesso dall'azienda, oltre ad autenticare il certificato di identità degli utenti per consentire l'accesso VPN tramite il client protetto durante la fase EAP SSL o IKEv2.

L'autenticazione con più certificati limita il numero di certificati a due. Il client sicuro deve indicare il supporto per l'autenticazione con più certificati. In caso contrario, il gateway utilizza uno dei metodi di autenticazione legacy o non riesce a stabilire la connessione. Secure Client versione 4.4.04030 o successive supporta l'autenticazione basata su più certificati.

Configurazioni

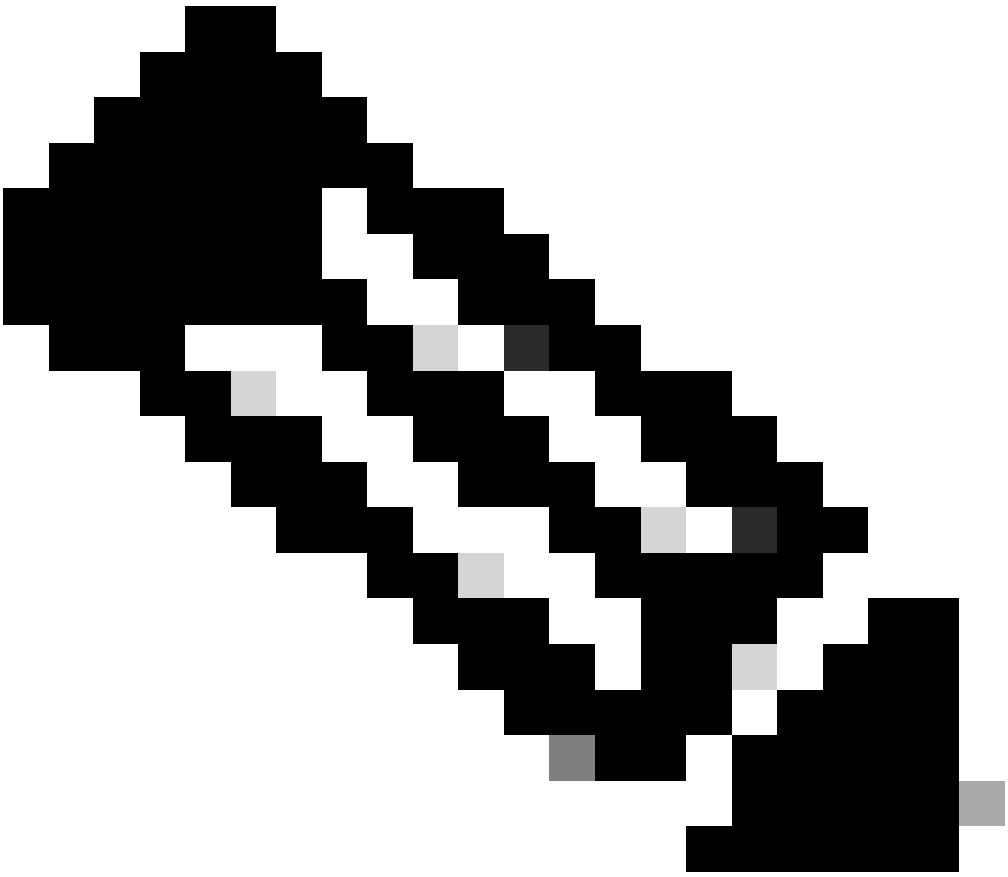
Configurazione su FTD

1. Selezionare Dispositivi > VPN > Accesso remoto.
2. Selezionare il criterio VPN di accesso remoto e fare clic su Modifica.



Nota: Se non è stata configurata una VPN di accesso remoto, fare clic su Aggiungi per creare un nuovo criterio VPN di accesso remoto.

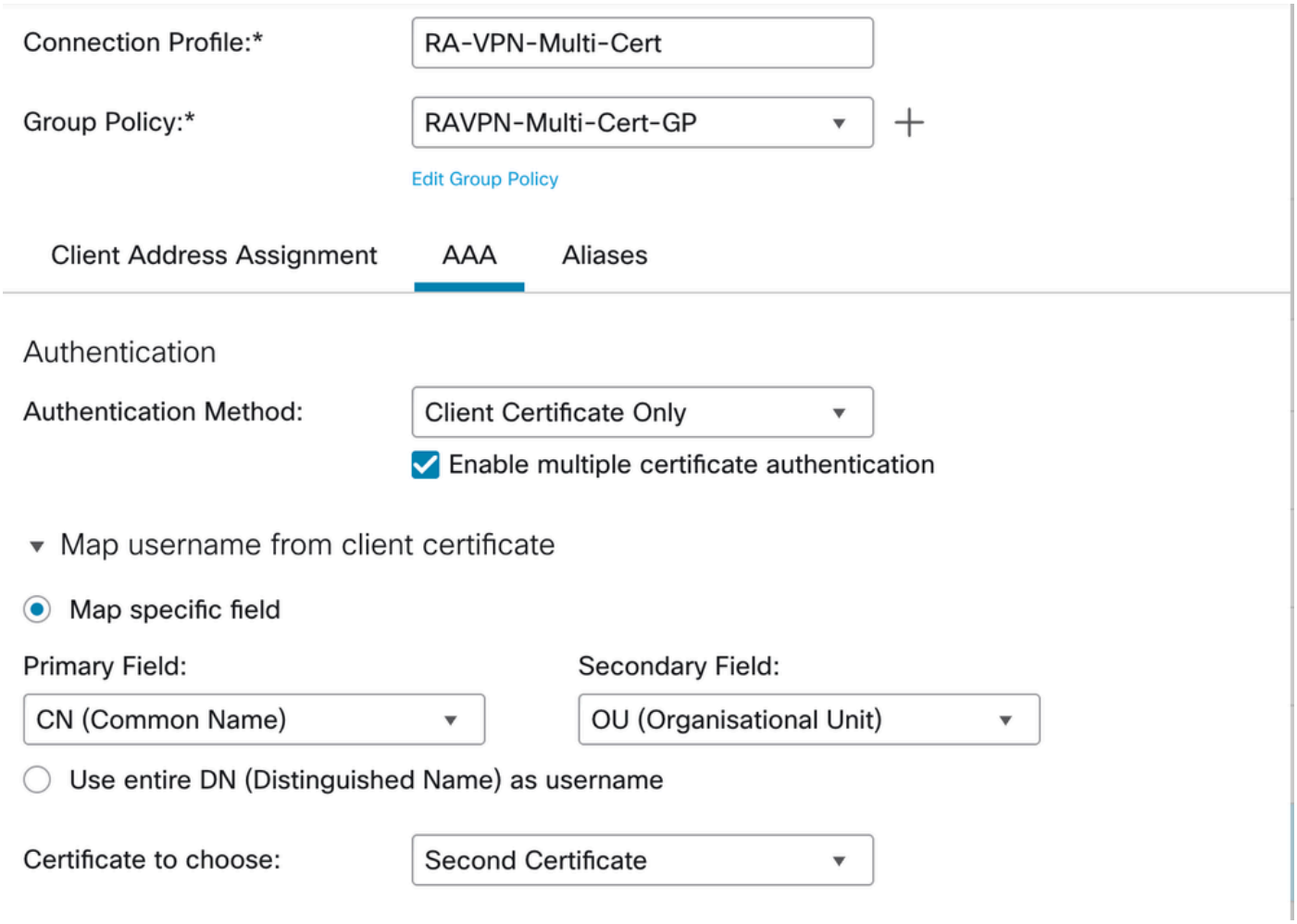
3. Selezionare e modificare un profilo di connessione per configurare l'autenticazione con più certificati.
4. Fare clic su Impostazioni AAA e scegliere Metodo di autenticazione come Solo certificato client o Certificato client e AAA.



Nota: Selezionare il server di autenticazione se è stato selezionato il metodo di autenticazione Certificato client e AAA.

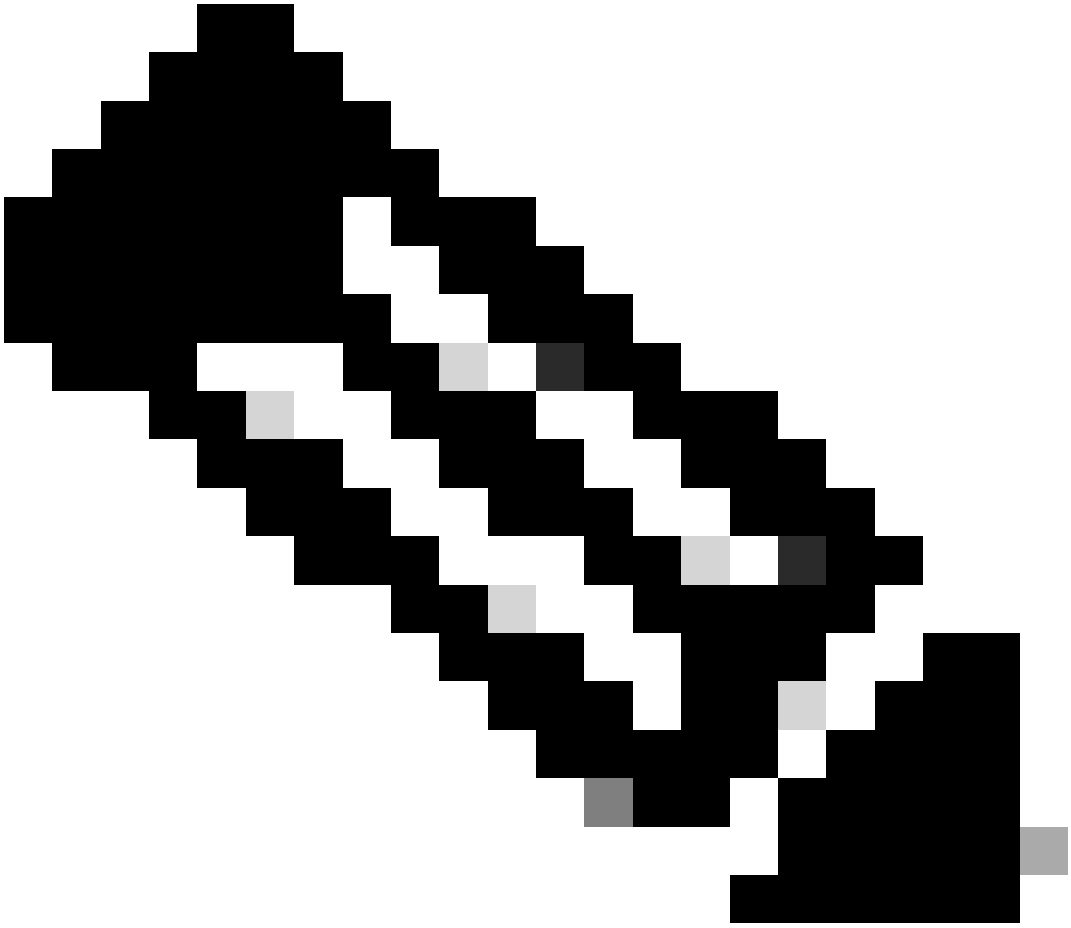
5. Selezionare la casella di controllo Abilita autenticazione con più certificati.
6. Scegliere uno dei certificati da mappare al nome utente dal certificato client:
   - Primo certificato: selezionare questa opzione per mappare il nome utente dal certificato del computer inviato dal client VPN.
   - Secondo certificato: selezionare questa opzione per mappare il nome utente dal certificato utente inviato dal client.

   Il nome utente inviato dal client viene utilizzato come nome utente della sessione VPN quando è abilitata l'autenticazione solo certificato. Quando l'autenticazione AAA e il certificato sono abilitati, il nome utente della sessione VPN è basato sull'opzione Prefill.
7. Se si seleziona l'opzione Corrispondenza campo specifico, che include il nome utente del certificato client, nei campi Principale e Secondario vengono visualizzati rispettivamente i valori predefiniti Nome comune (CN) e Unità organizzativa (OU) .



Impostazioni AAA del profilo di connessione

8. Se si seleziona l'opzione Usa intero nome distinto (DN) come nome utente, il sistema recupera automaticamente l'identità dell'utente. Un nome distinto è un'identificazione univoca, costituita da singoli campi che possono essere utilizzati come identificatore quando gli utenti corrispondono a un profilo di connessione. Le regole DN vengono utilizzate per l'autenticazione avanzata dei certificati.



Nota: Se è stata selezionata l'autenticazione Certificato client e AAA, selezionare l'opzione Precompila nome utente da certificato nella finestra di accesso utente per precompilare il nome utente secondario dal certificato client quando l'utente si connette tramite il modulo VPN client sicuro di Cisco Secure Client.

Nascondi nome utente nella finestra di accesso: Il nome utente secondario è precompilato dal certificato client, ma nascosto all'utente in modo che non modifichi il nome utente precompilato.

---

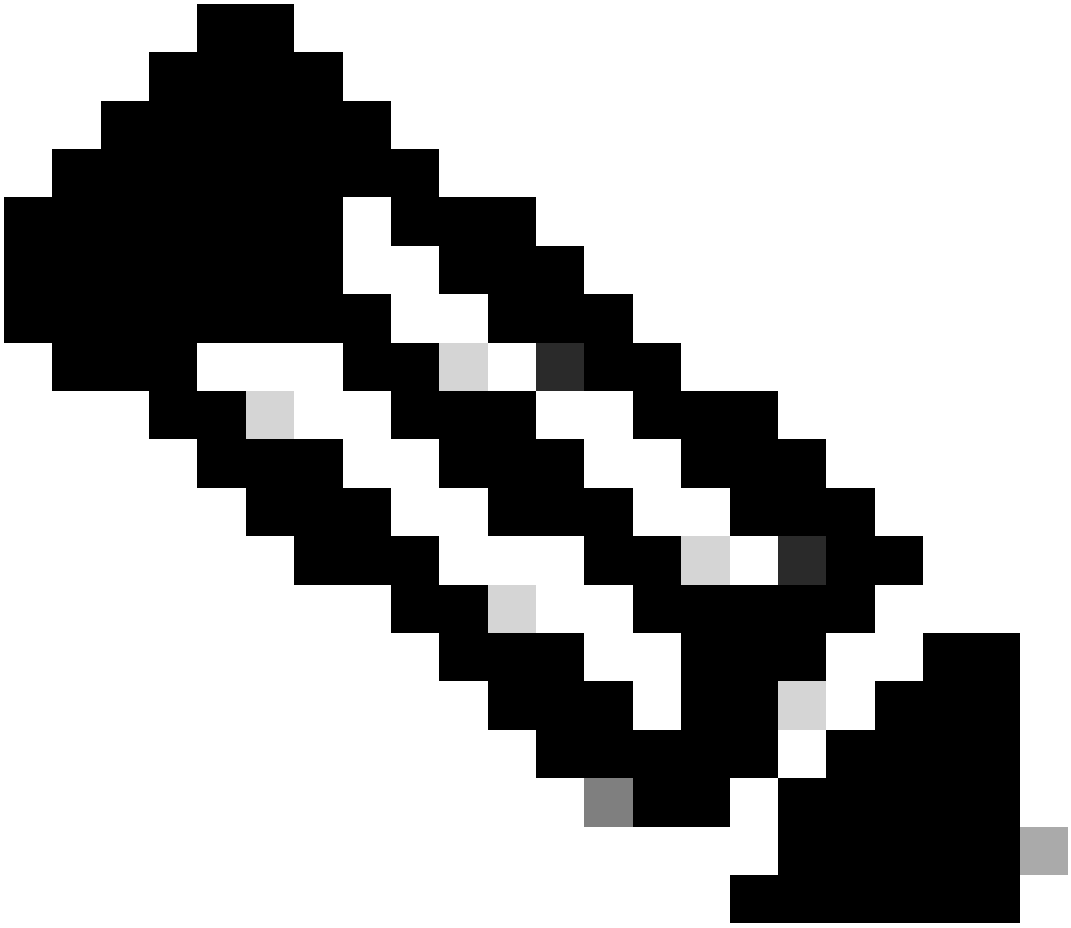
9. Per ulteriori informazioni sulla configurazione, consultare il documento sulla configurazione della VPN ad accesso remoto con client sicuro (AnyConnect) su FTD.

10. Caricare i certificati CA del certificato dell'archivio utenti e del certificato dell'archivio computer nell'FTD per convalidare correttamente. Poiché in questo scenario, il certificato dell'archivio utenti e il certificato dell'archivio computer sono firmati dalla stessa CA, l'installazione di tale CA è sufficiente. Se il certificato dell'archivio utenti e il certificato dell'archivio computer sono firmati da un'autorità di certificazione diversa, entrambi i certificati devono essere caricati nell'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

Certificato CA installato nel FTD da FMC

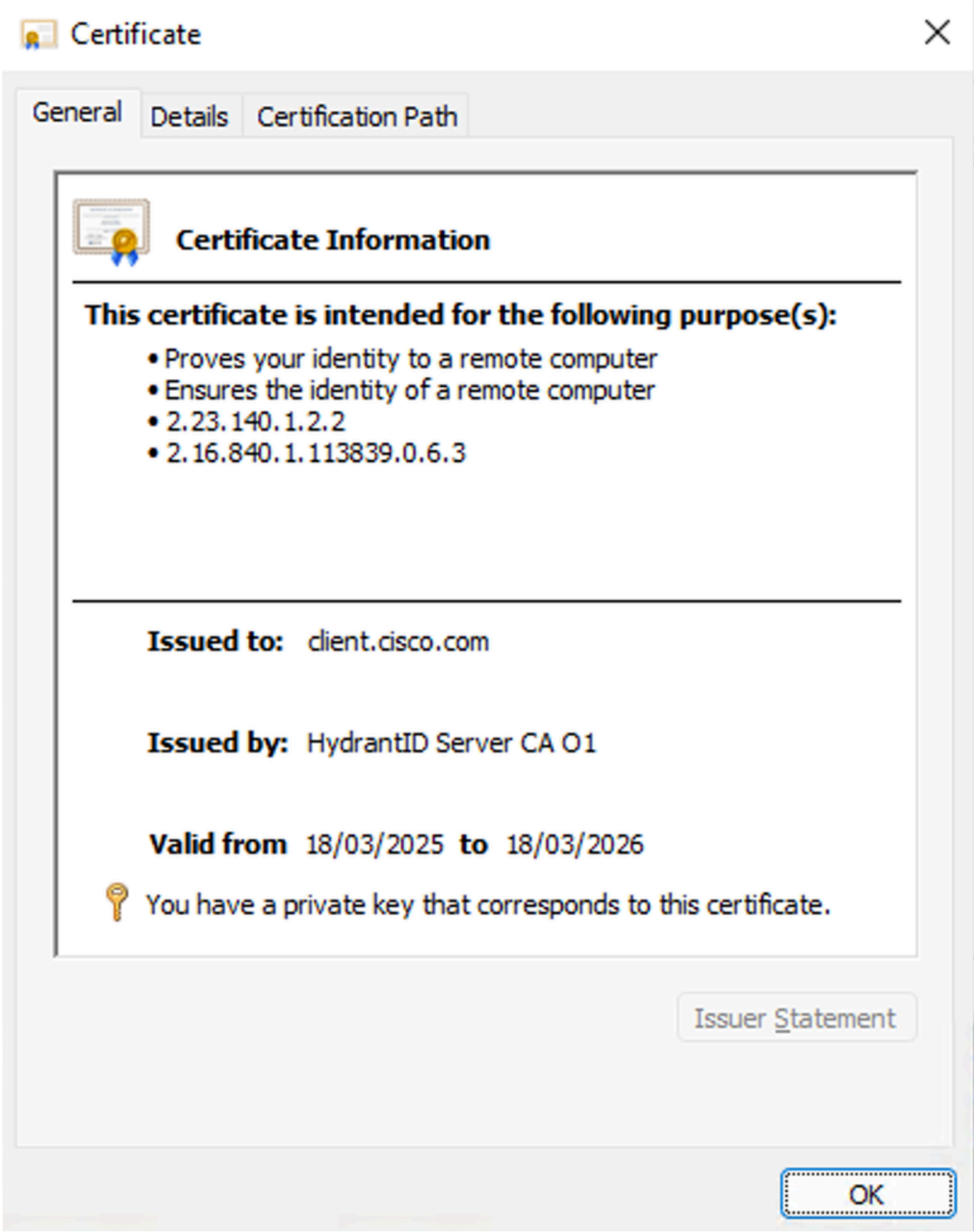


Nota: CertificateStore deve essere impostato su All per AnyConnect Client Profile e CertificateStoreOverride deve essere impostato su true se l'utente non dispone dei diritti di amministratore.

Certificati sul computer utente

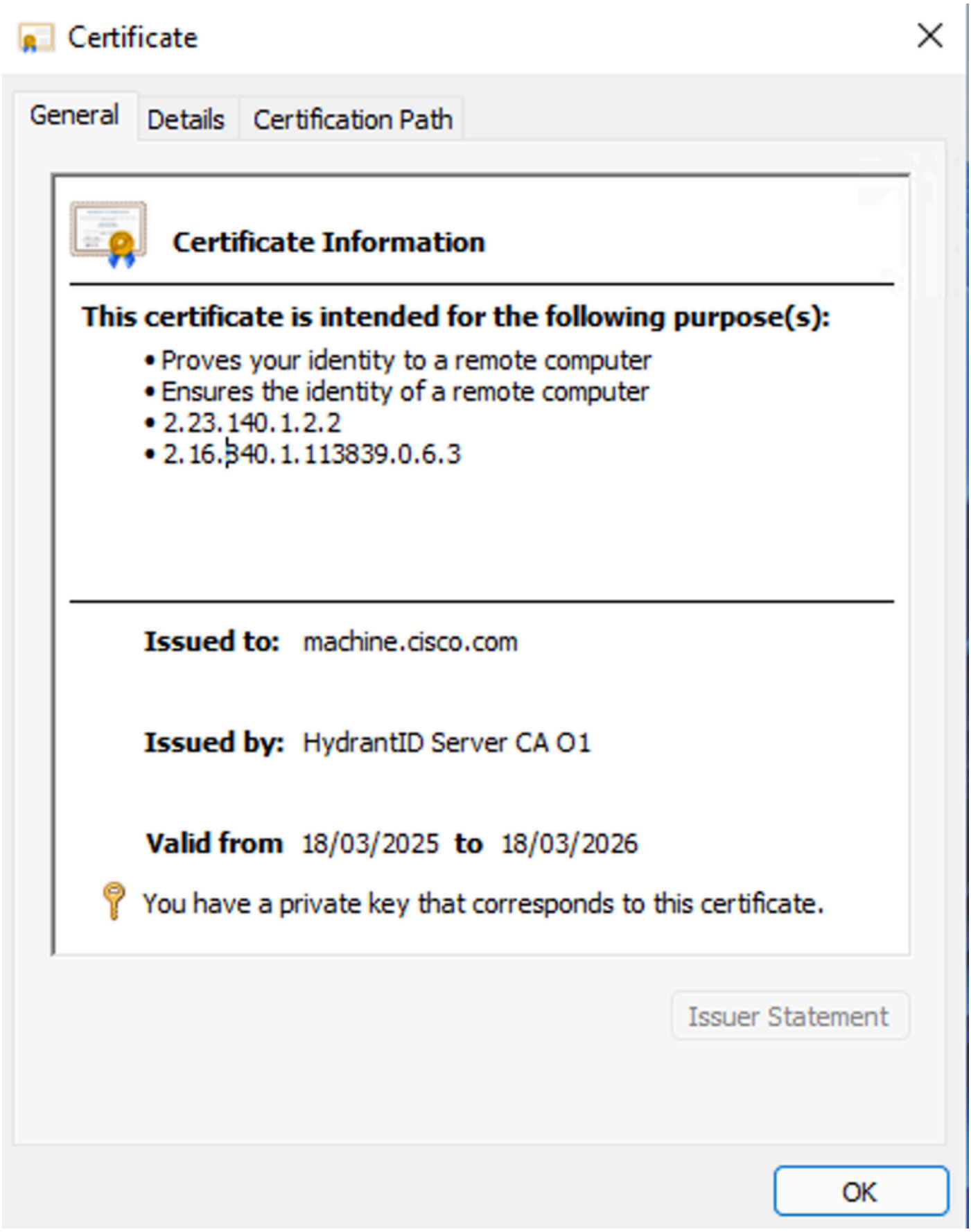
Nel computer utente che deve connettersi a questo profilo di connessione devono essere installati certificati validi nell'archivio utenti e nell'archivio computer.

Certificato dall'archivio utenti:



Certificato archivio utenti

Certificato dall'archivio computer:



Certificato archivio computer

Verifica

1. Verificare la configurazione del profilo di connessione dalla CLI FTD:

<#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. Eseguire questo comando per verificare la connessione:

<#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
```

Il nome utente client.cisco.com viene recuperato dal CN del certificato dell'archivio utenti. Il nome utente per la mappatura del secondo certificato è selezionato nella sezione AAA. Se si seleziona Primo certificato, il nome utente viene recuperato dal certificato dell'archivio computer che è machine.cisco.com.

Risoluzione dei problemi

1. Verificare che i certificati validi siano presenti nell'archivio certificati utente e nell'archivio certificati del computer.

2. Raccogliere i debug su FTD per controllare i log relativi alla convalida del certificato utilizzando debug crypto ca 14.
3. Rivedere DART dal computer dell'utente.

Registri DART da scenario di lavoro:

<#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

****

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).