Configurer l'authentification de certificats multiples sur FTD pour RAVPN

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurations

- Configuration sur FTD
- Certificats sur l'ordinateur utilisateur

Vérifier

Dépannage

Introduction

Ce document décrit la procédure à suivre pour utiliser l'authentification par certificats multiples pour le client sécurisé sur Firepower Threat Defense (FTD) géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN d'accès à distance (RAVPN)
- Expérience avec Firepower Management Center (FMC)
- Connaissances de base des certificats X509

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD - 7,6
- Cisco FMC - 7,6
- Windows 11 avec 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Avant la version 7.0 du logiciel, FTD prend en charge l'authentification basée sur un certificat unique, ce qui signifie que l'utilisateur ou la machine peuvent être authentifiés, mais pas les deux, pour une seule tentative de connexion.

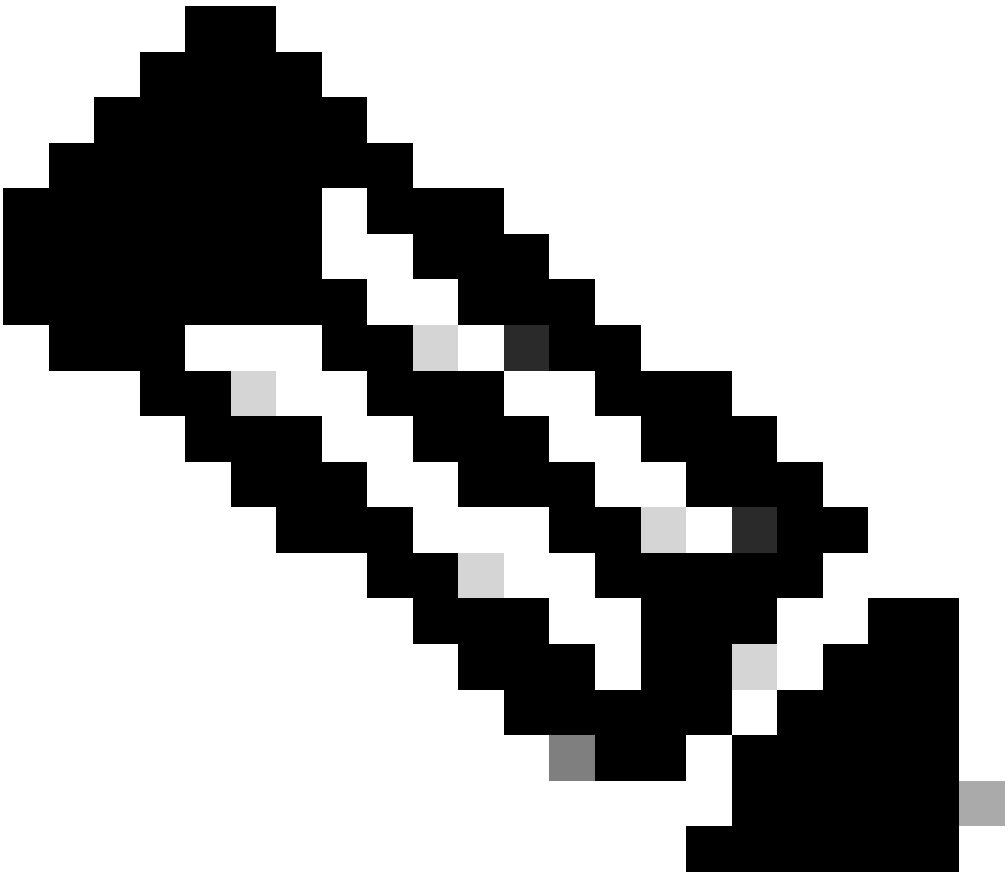
L'authentification basée sur plusieurs certificats permet de valider le certificat de la machine ou du périphérique par la défense contre les menaces, pour s'assurer que le périphérique est un périphérique d'entreprise, en plus d'authentifier le certificat d'identité des utilisateurs pour permettre l'accès VPN à l'aide du client sécurisé pendant la phase SSL ou IKEv2 EAP.

L'authentification de certificats multiples limite actuellement le nombre de certificats à deux. Secure Client doit indiquer la prise en charge de l'authentification de certificats multiples. Si ce n'est pas le cas, alors la passerelle utilise l'une des méthodes d'authentification héritées ou échoue la connexion.Secure Client version 4.4.04030 ou ultérieure prend en charge l'authentification basée sur Multi-Certificate.

Configurations

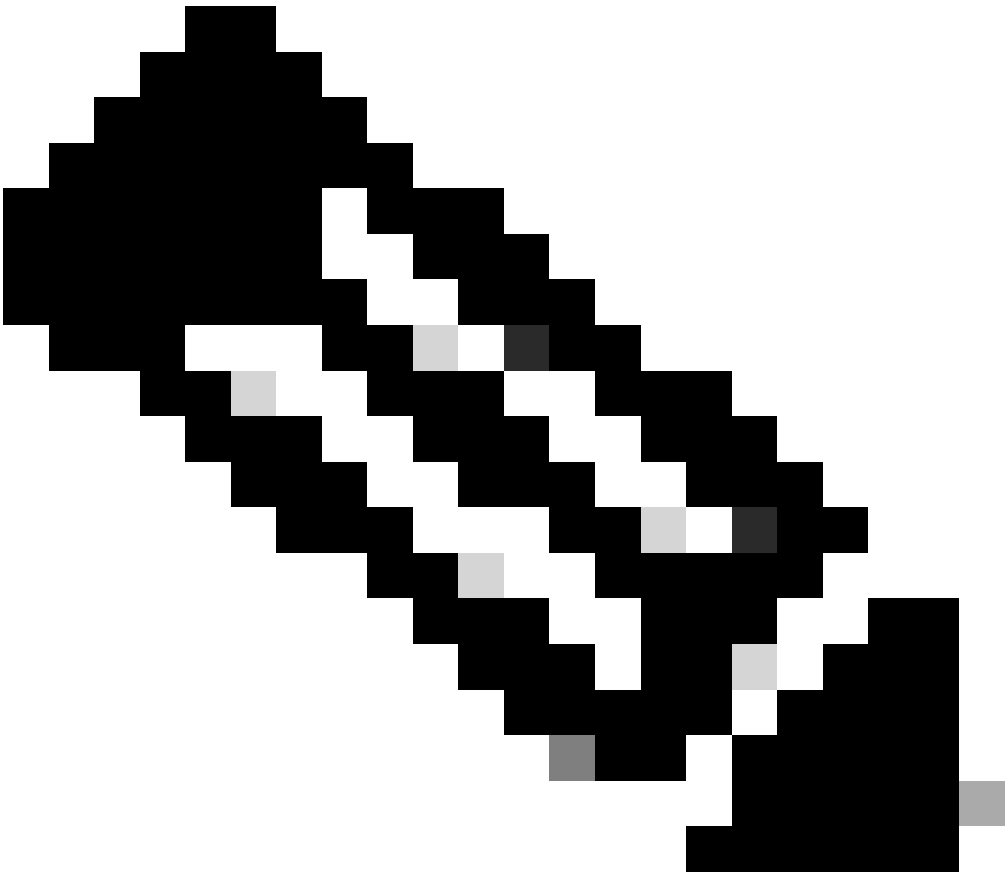
Configuration sur FTD

1. Accédez à Devices > VPN > Remote Access.
2. Sélectionnez la stratégie VPN d'accès à distance et cliquez sur Edit.



Remarque : Si vous n'avez pas configuré un VPN d'accès à distance, cliquez sur Add pour créer une nouvelle stratégie VPN d'accès à distance.

3. Sélectionnez et modifiez un profil de connexion pour configurer l'authentification de certificats multiples.
4. Cliquez sur les paramètres AAA et choisissez Authentication Method comme Client Certificate Only ou Client Certificate & AAA.



Remarque : Sélectionnez le serveur d'authentification si vous avez sélectionné la méthode d'authentification AAA et certificat client.

5. Cochez la case Enable multiple certificate authentication.

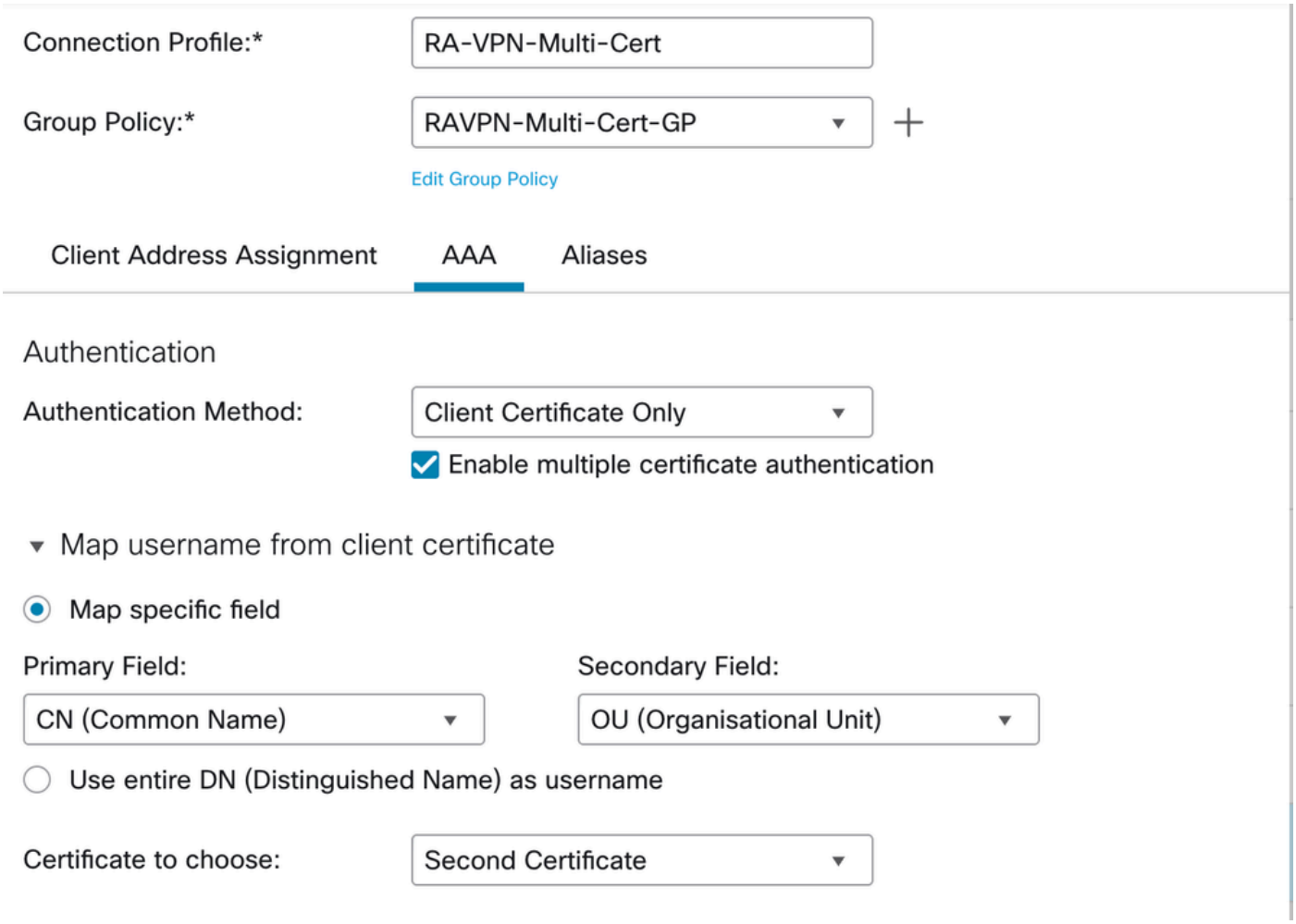
6. Choisissez l'un des certificats pour mapper le nom d'utilisateur à partir du certificat client :

   - First Certificate : sélectionnez cette option pour mapper le nom d'utilisateur à partir du certificat de machine envoyé à partir du client VPN.
   - Second Certificate : sélectionnez cette option pour mapper le nom d'utilisateur à partir du certificat d'utilisateur envoyé par le client.

   Le nom d'utilisateur envoyé par le client est utilisé comme nom d'utilisateur de session VPN lorsque l'authentification par certificat uniquement est activée. Lorsque AAA et l'authentification de certificat sont activés, le nom d'utilisateur de la session VPN est basé sur l'option Prefill.

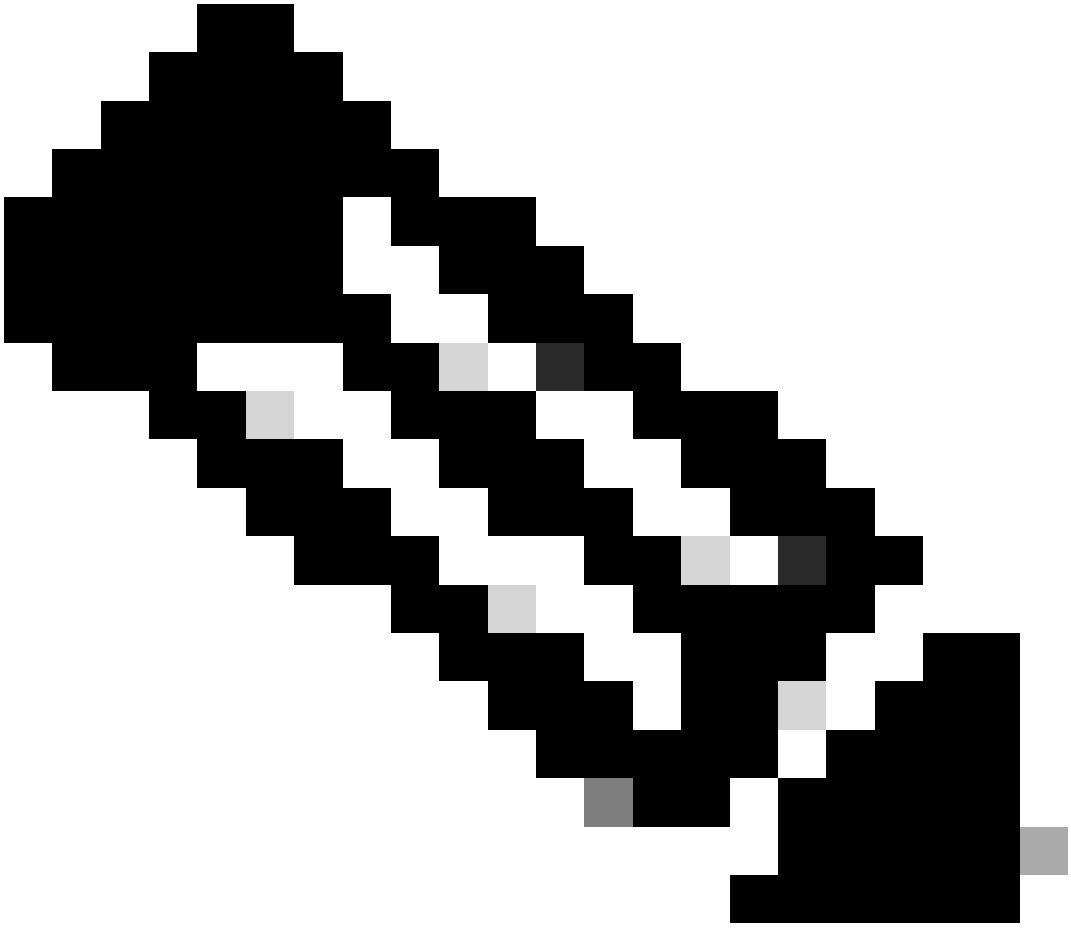
7. Si vous sélectionnez l'option de champ Mapper spécifique, qui inclut le nom d'utilisateur du certificat client, les champs Principal et Secondaire affichent les valeurs par défaut : Nom

commun (CN) et Unité d'organisation (OU) respectivement.



Paramètres AAA du profil de connexion

8. Si vous sélectionnez l'option Utiliser le nom distinctif (DN) complet comme nom d'utilisateur, le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif est une identification unique, composée de champs individuels qui peuvent être utilisés comme identificateur lors de la mise en correspondance d'utilisateurs avec un profil de connexion. Les règles DN sont utilisées pour l'authentification améliorée des certificats.



Remarque : Si vous avez sélectionné le certificat client et l'authentification AAA, sélectionnez l'option Prefill username from certificate on user login window pour préremplir le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte via le module VPN client sécurisé de Cisco Secure Client.

Masquer le nom d'utilisateur dans la fenêtre de connexion : Le nom d'utilisateur secondaire est pré-rempli à partir du certificat client, mais il est masqué pour l'utilisateur afin qu'il ne modifie pas le nom d'utilisateur pré-rempli.

---

9. Pour une autre configuration détaillée, référez-vous à Configurer le VPN d'accès à distance Secure Client (AnyConnect) sur FTD.

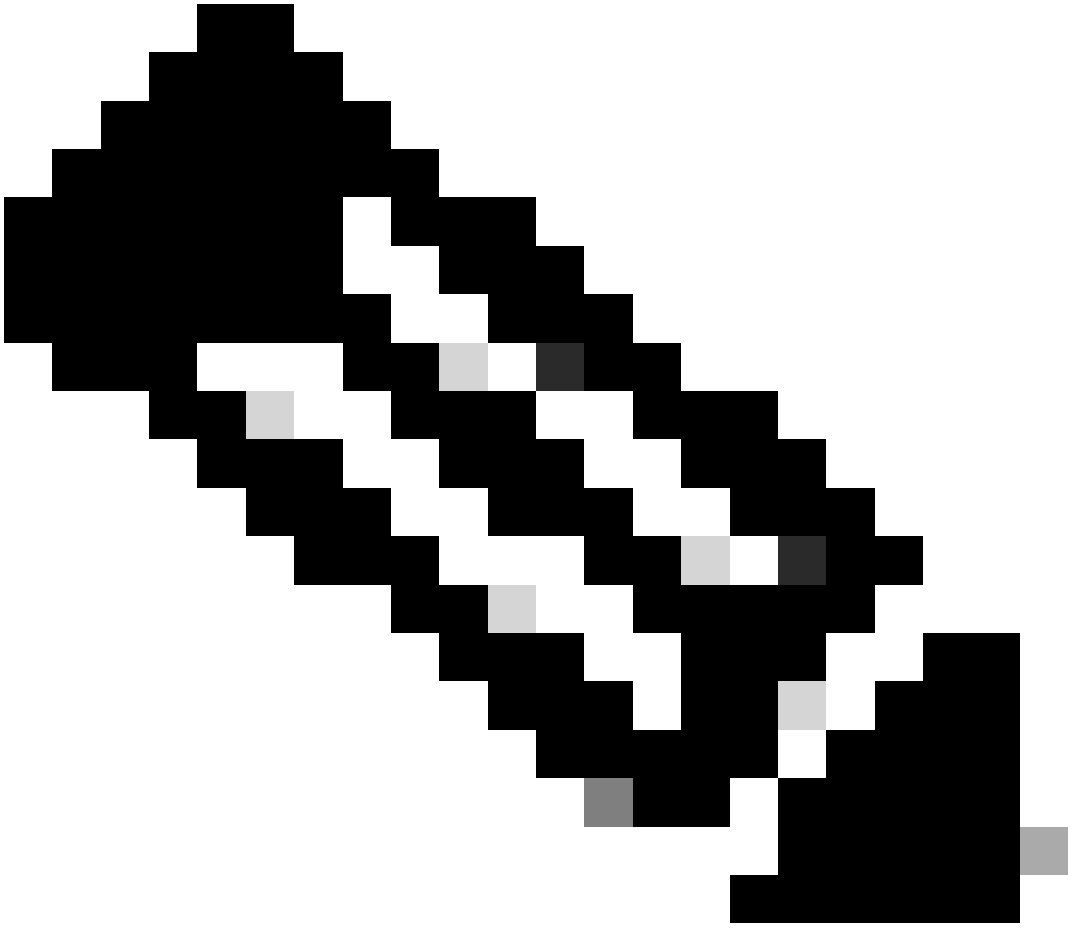
10. Téléchargez les certificats CA du certificat du magasin d'utilisateurs et du certificat du magasin d'ordinateurs vers le FTD pour une validation réussie. Étant donné que dans ce scénario, le certificat du magasin d'utilisateurs et le certificat du magasin d'ordinateurs sont signés par la même autorité de certification, l'installation de cette autorité de certification suffit. Si le certificat du magasin d'utilisateurs et le certificat du magasin d'ordinateurs sont signés par une autorité de

certification différente, ces deux certificats d'autorité de certification doivent être téléchargés dans le 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

Certificat CA installé sur FTD à partir de FMC

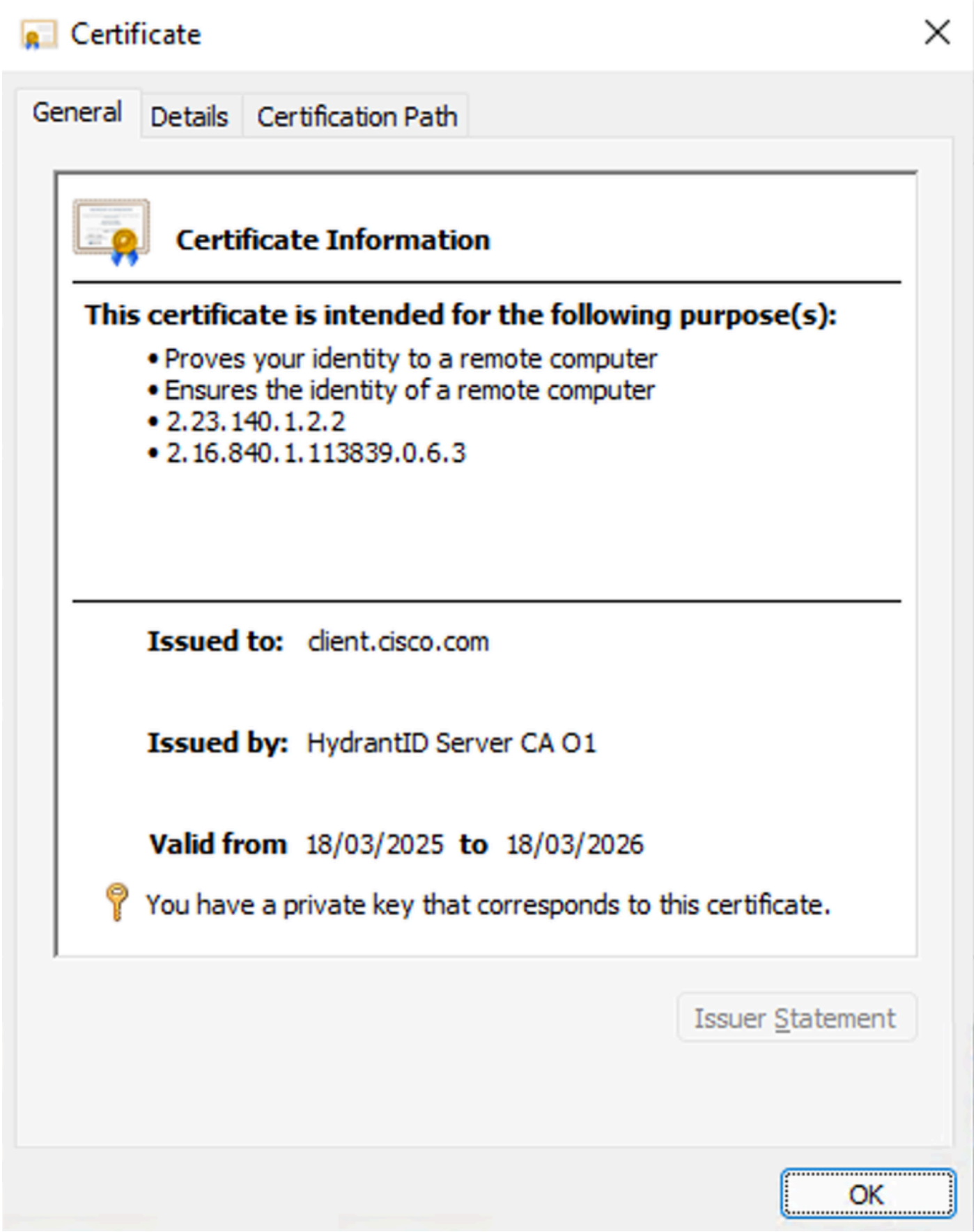


Remarque : Le CertificateStore du profil client AnyConnect doit être défini sur All et le CertificateStoreOverride doit être défini sur True si l'utilisateur ne dispose pas de droits d'administration.

Certificats sur l'ordinateur utilisateur

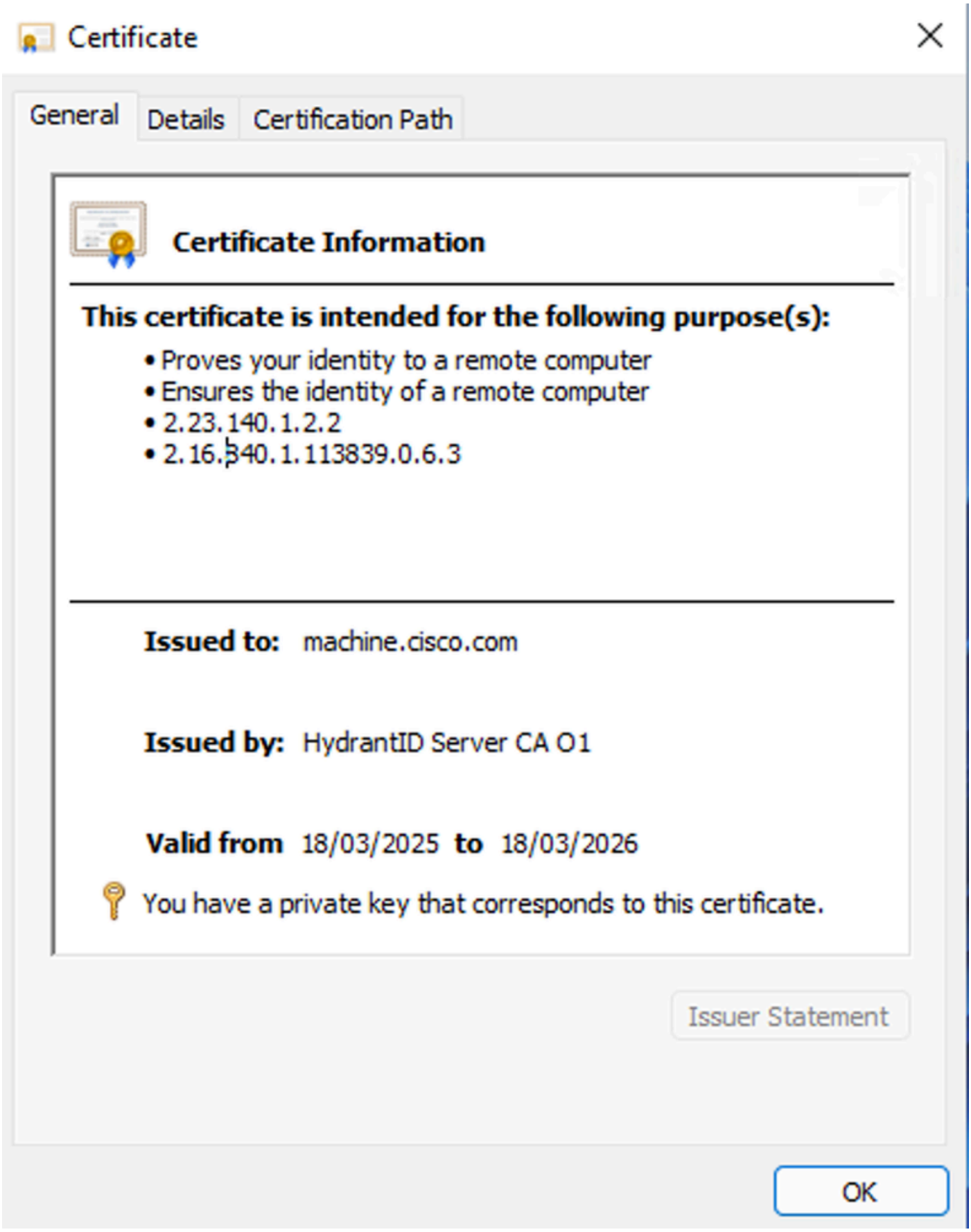
L'ordinateur utilisateur qui est censé se connecter à ce profil de connexion doit avoir des certificats valides installés dans le magasin d'utilisateurs et le magasin d'ordinateurs.

Certificat du magasin d'utilisateurs :



Certificat du magasin utilisateur

Certificat du magasin d'ordinateurs :



Certificat du magasin de machines

Vérifier

1. Vérifiez la configuration du profil de connexion à partir de l'interface de ligne de commande 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. Exécutez cette commande pour vérifier la connexion :

<#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
```

Nom d'utilisateur client.cisco.comis récupéré à partir du certificat du magasin d'utilisateurs CN comme nom d'utilisateur de mappage à partir du deuxième certificat est sélectionné dans la section AAA. Si Premier certificat est sélectionné, alors le nom d'utilisateur est récupéré à partir du certificat du magasin de la machine qui est machine.cisco.com.

Dépannage

1. Assurez-vous que des certificats valides sont présents dans le magasin de certificats d'utilisateur et le magasin de certificats d'ordinateur.

2. Collectez les débogages sur FTD pour vérifier les journaux liés à la validation de certificat en utilisant debug crypto ca 14.
3. Examinez le DART depuis l'ordinateur utilisateur.

Journaux DART du scénario de travail :

<#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

****

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.