# Configuración de la Autenticación de Varios Certificados en FTD para RAVPN

## Contenido



## Introducción

Este documento describe el procedimiento para utilizar la Autenticación de certificados múltiples para Secure Client en Firepower Threat Defense (FTD) administrado por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de VPN de acceso remoto (RAVPN)
- Experiencia con Firepower Management Center (FMC)
- Conocimientos básicos de los certificados X509

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD de Cisco - 7,6
- Cisco FMC - 7,6
- Windows 11 con Cisco Secure Client 5.1.4.74

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

Antes de la versión 7.0 del software, FTD admite la autenticación basada en un solo certificado, lo que significa que el usuario o la máquina se pueden autenticar, pero no ambos, para un único intento de conexión.

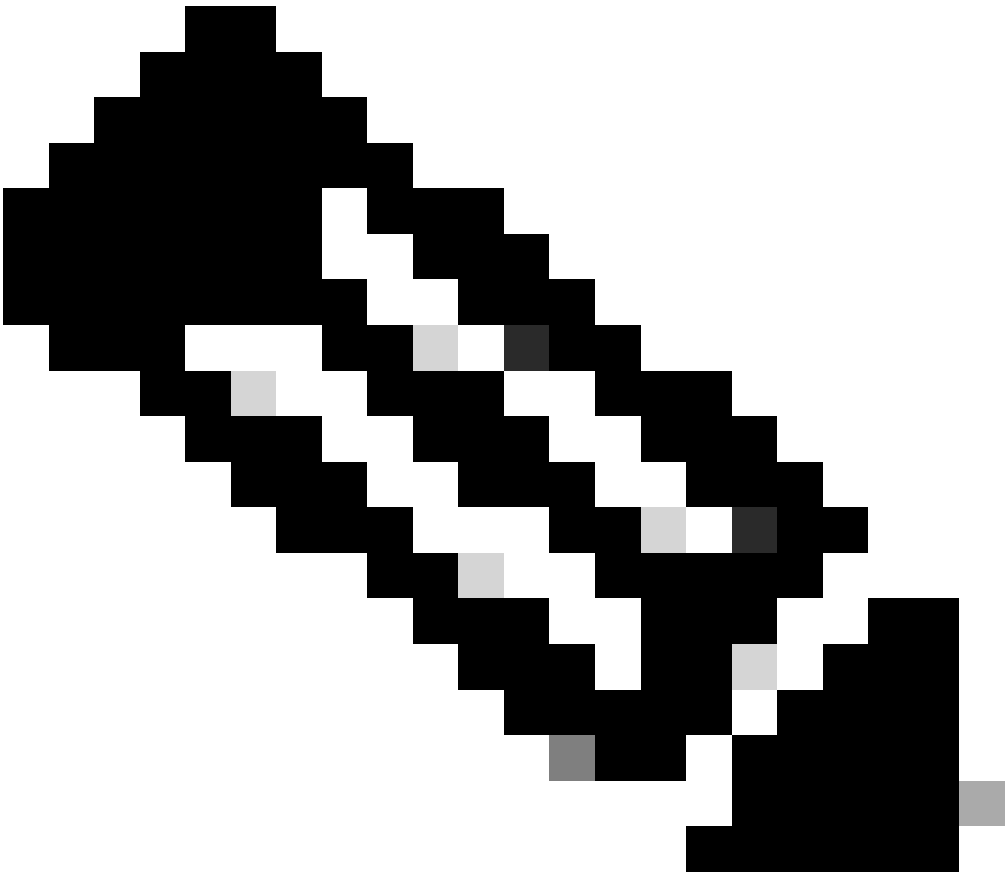
La autenticación basada en varios certificados ofrece la posibilidad de que la defensa contra amenazas valide el certificado de la máquina o del dispositivo para garantizar que el dispositivo es un dispositivo corporativo, además de autenticar el certificado de identidad de los usuarios para permitir el acceso VPN mediante el cliente seguro durante la fase EAP de SSL o IKEv2.

La autenticación de certificados múltiples actualmente limita el número de certificados a dos. Secure Client debe indicar la compatibilidad con la autenticación de certificados múltiples. Si no es así, la puerta de enlace utiliza uno de los métodos de autenticación heredados o no puede establecer la conexión.Secure Client versión 4.4.04030 o posterior admite la autenticación basada en certificados múltiples.

# Configuraciones

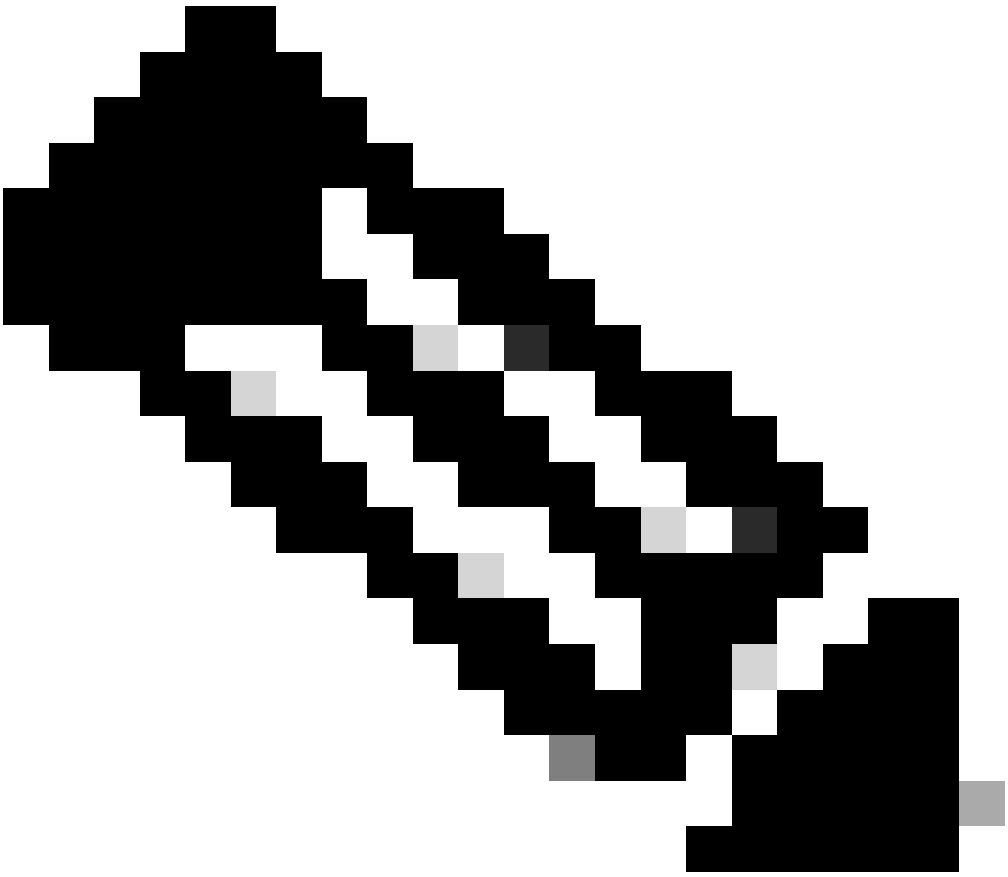
## Configuración en FTD

1. Vaya a Dispositivos > VPN > Acceso remoto.
2. Seleccione la directiva VPN de acceso remoto y haga clic en Editar.



Nota: Si no ha configurado una VPN de acceso remoto, haga clic en Agregar para crear una nueva directiva de VPN de acceso remoto.

3. Seleccione y edite un perfil de conexión para configurar la autenticación de certificados múltiples.
4. Haga clic en AAA settings y elija Authentication Method como Client Certificate Only o Client Certificate & AAA.



Nota: Seleccione el Servidor de autenticación si ha seleccionado el método de autenticación Certificado de cliente y AAA.

5. Seleccione la casilla de verificación Enable multiple certificate authentication.

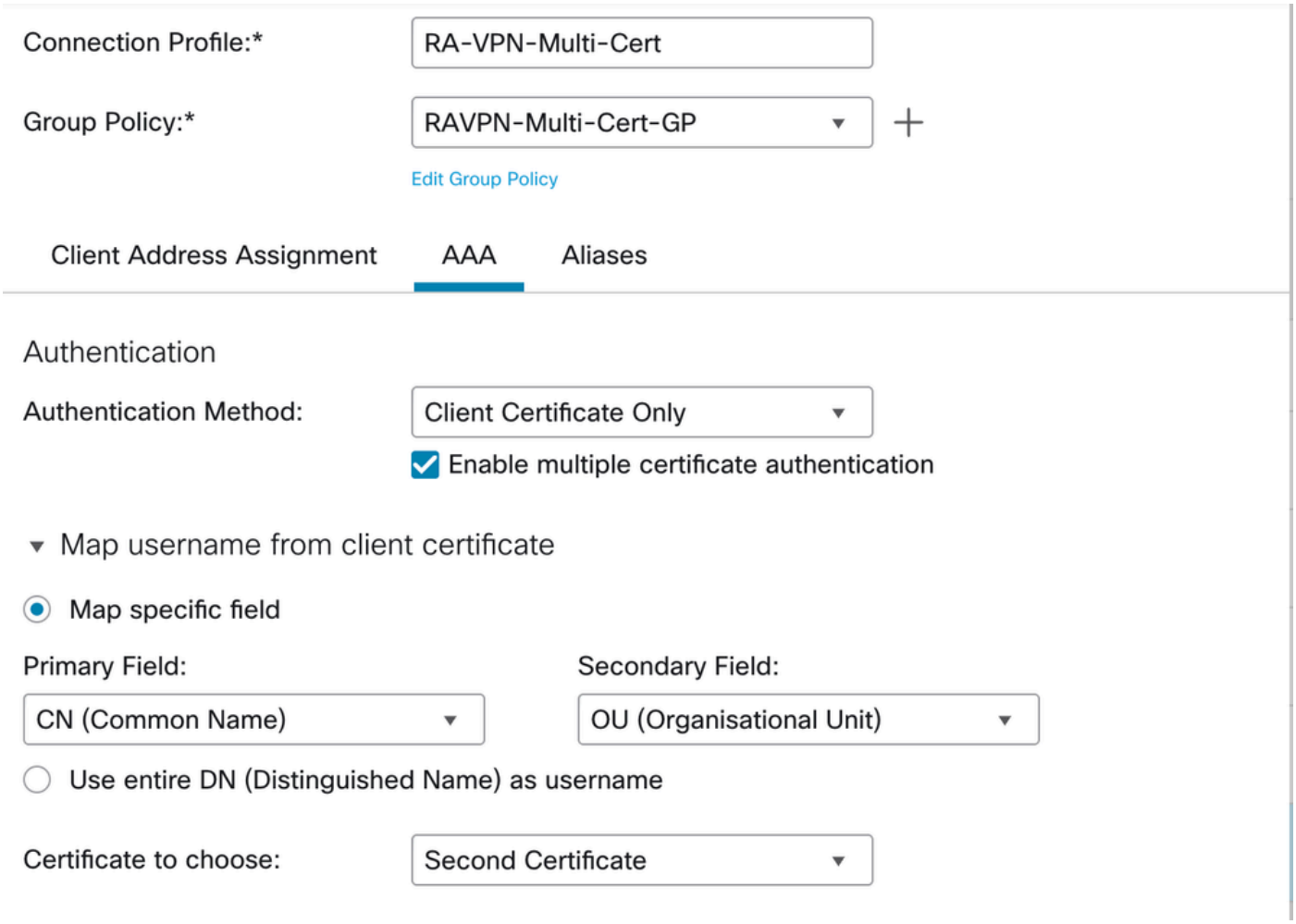
6. Elija uno de los certificados paraAsignar nombre de usuario del certificado de cliente:

   - Primer certificado: seleccione esta opción para asignar el nombre de usuario del certificado de equipo enviado desde el cliente VPN.
   - Segundo certificado: seleccione esta opción para asignar el nombre de usuario del certificado de usuario enviado desde el cliente.

   El nombre de usuario enviado desde el cliente se utiliza como nombre de usuario de sesión VPN cuando la autenticación sólo de certificados está habilitada. Cuando se habilita la autenticación AAA y de certificados, el nombre de usuario de la sesión VPN se basa en la opción Prefill.

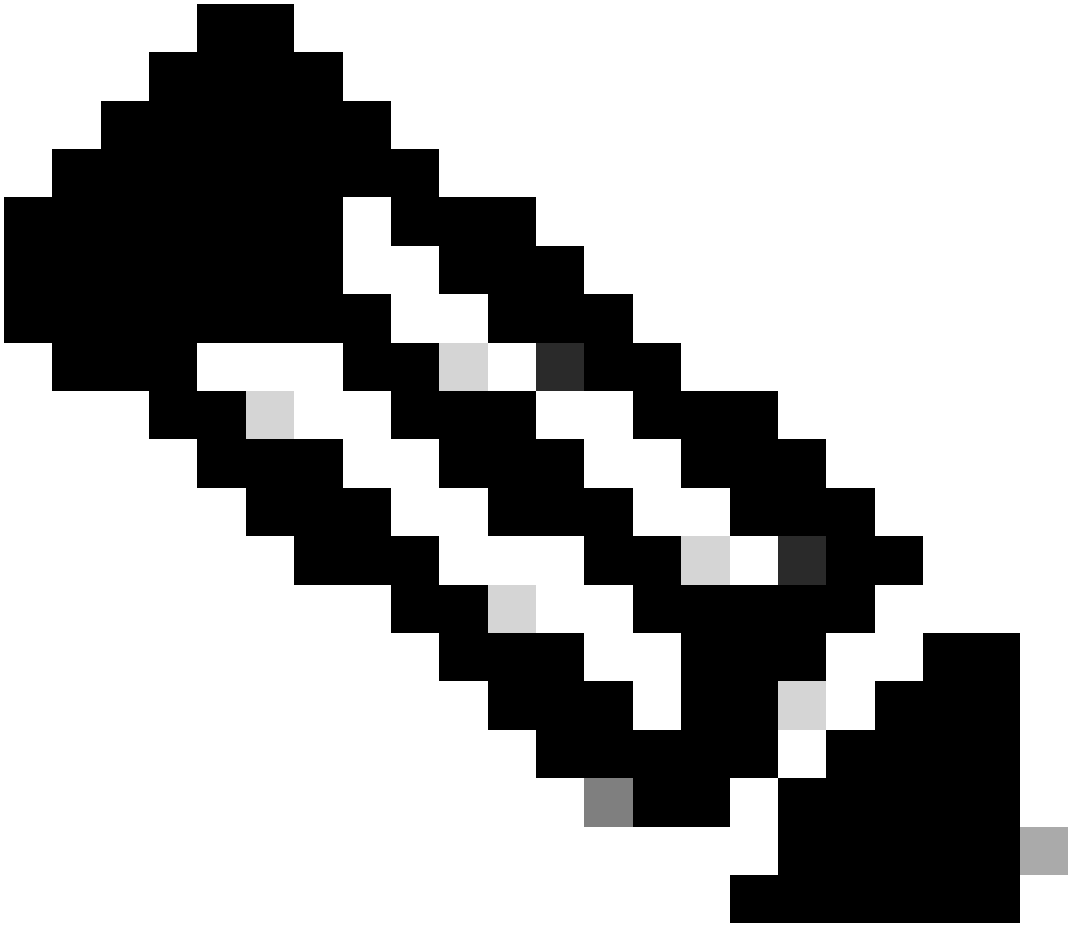
7. Si selecciona la opción de campo Asignar específico, que incluye el nombre de usuario del certificado de cliente, los campos Principal y Secundario muestran los valores

predeterminados: Nombre común (CN)y Unidad organizativa (OU)respectivamente.




Configuración AAA del perfil de conexión

8. Si selecciona la opción Utilizar Nombre Distinguido (DN) completo como nombre de usuario, el sistema recuperará automáticamente la identidad del usuario. Un nombre distintivo es una identificación única, formada por campos individuales que se pueden utilizar como identificador al hacer coincidir usuarios con un perfil de conexión. Las reglas DN se utilizan para la autenticación de certificados mejorada.



Nota: Si ha seleccionado la autenticación Certificado de cliente y AAA, seleccione la opción Prefill username from certificate on user login window para rellenar previamente el nombre de usuario secundario del certificado de cliente cuando el usuario se conecte a través del módulo Secure Client VPN de Cisco Secure Client.

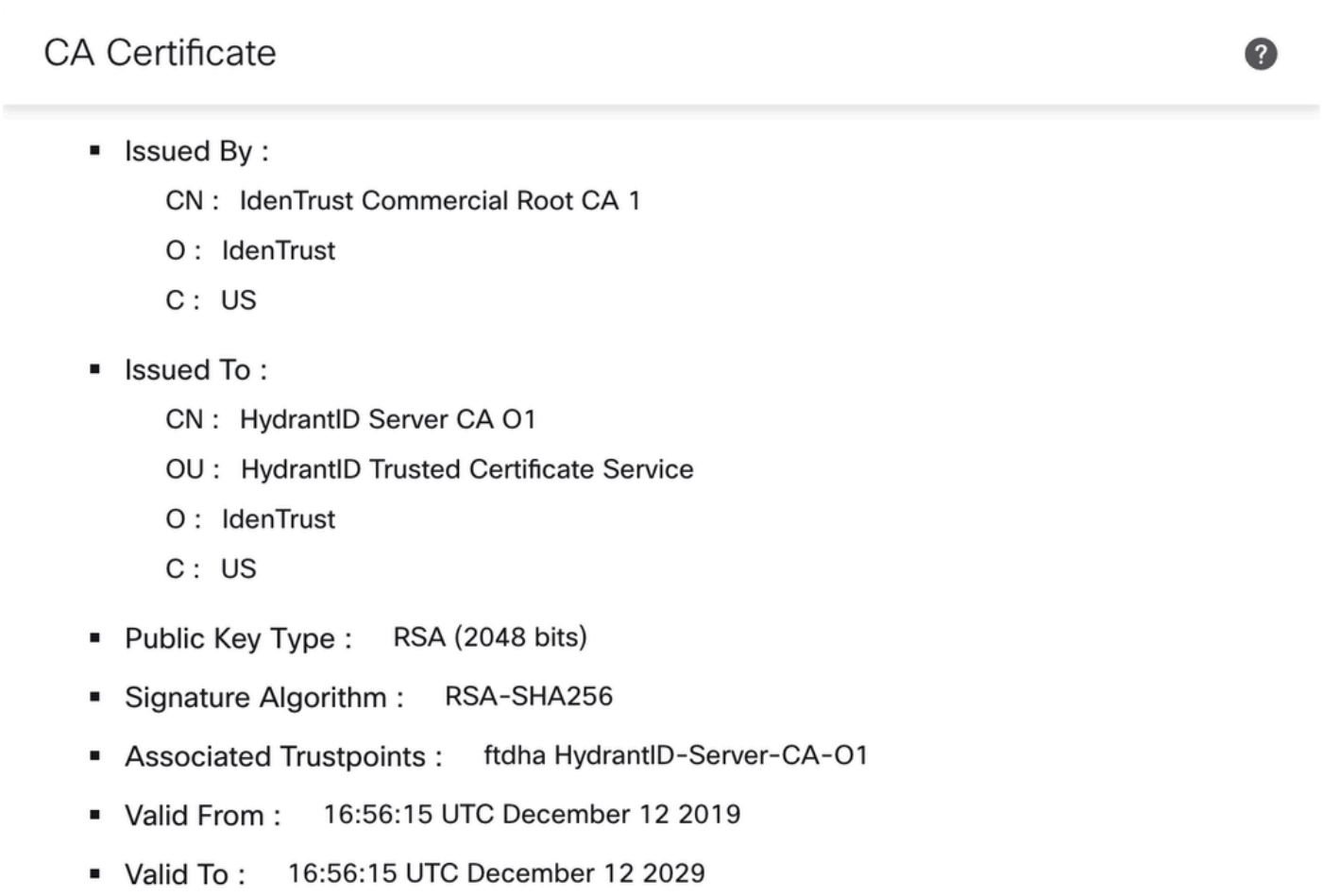
Ocultar nombre de usuario en la ventana de inicio de sesión: El nombre de usuario secundario se rellena previamente a partir del certificado de cliente, pero se oculta al usuario para que éste no modifique el nombre de usuario relleno previamente.

---

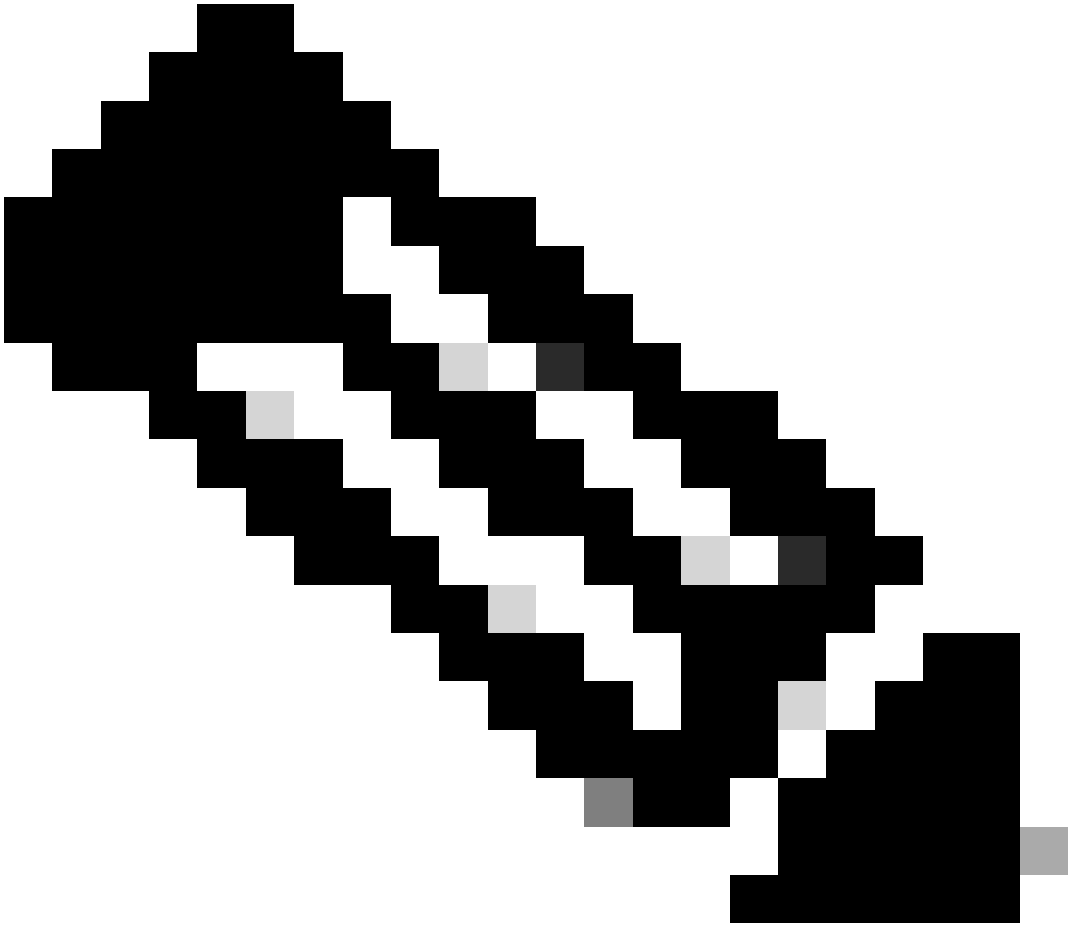
9. Para obtener más información sobre la configuración, consulte Configuración de VPN de acceso remoto de Secure Client (AnyConnect) en FTD.

10. Cargue los certificados de CA del certificado del almacén de usuarios y el certificado del almacén de máquinas en el FTD para que la validación sea correcta. Dado que, en este escenario, el certificado del almacén de usuarios y el certificado del almacén de equipos están firmados por la misma CA, basta con instalar esa CA. Si el certificado del almacén de usuarios y el certificado del almacén de equipos están firmados por una CA diferente, ambos certificados de

CA se deben cargar en el FTD.




Certificado de CA instalado en FTD desde FMC

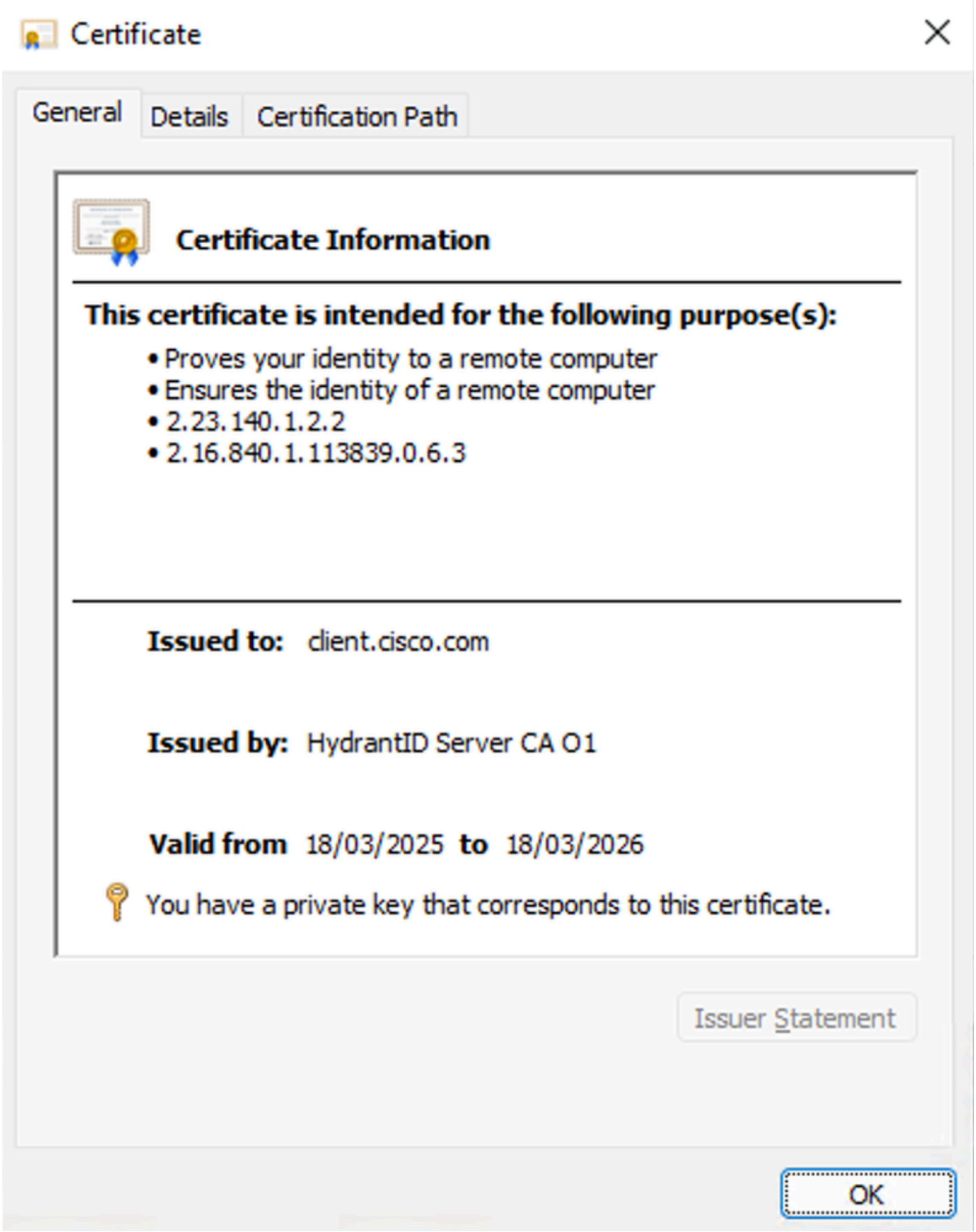


Nota: El perfil de cliente de AnyConnect debe tener CertificateStore establecido en All y CertificateStoreOverride establecido en true si el usuario no tiene derechos de administrador.

## Certificados en el equipo del usuario

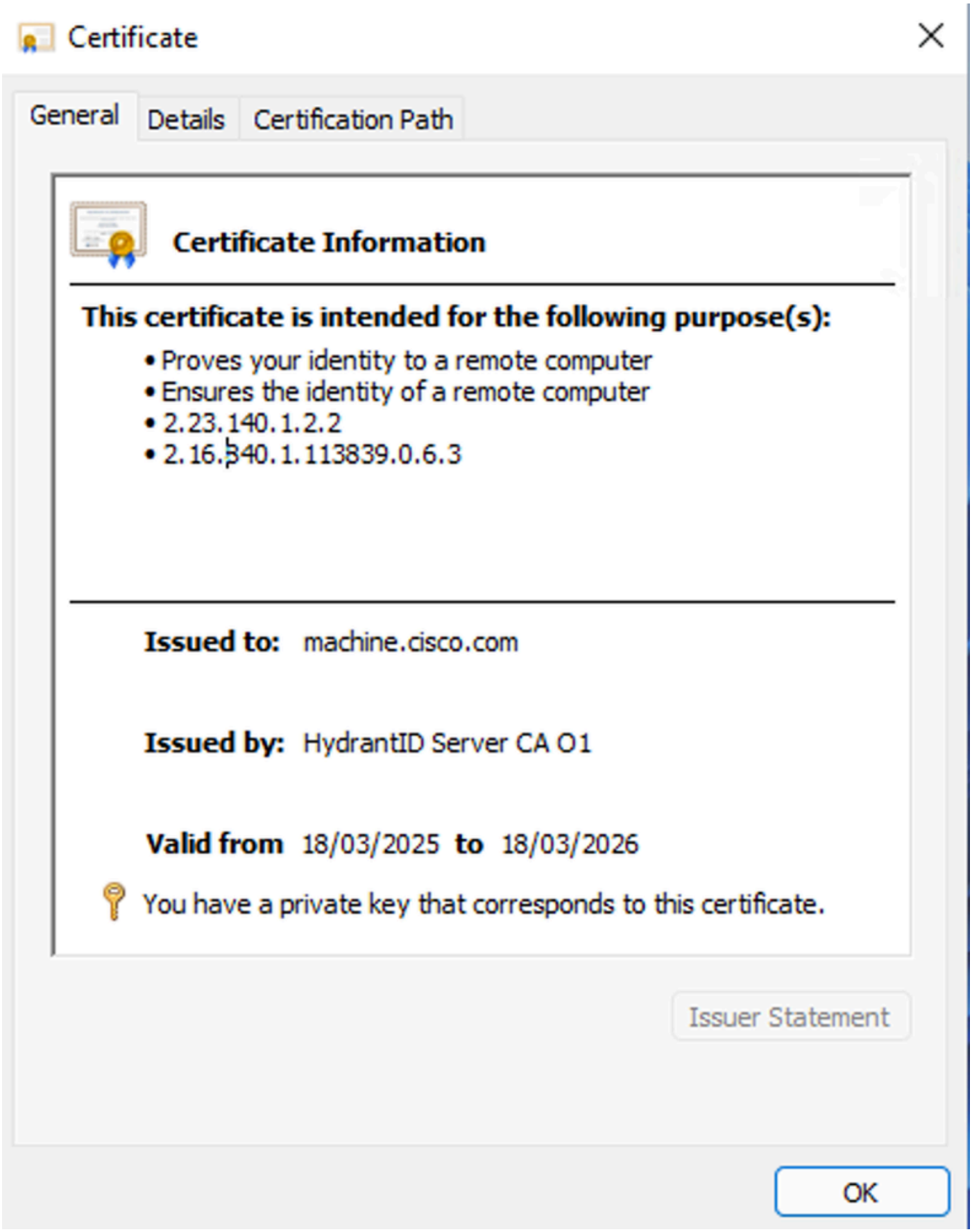
El equipo del usuario que se supone que debe conectarse a este perfil de conexión debe tener certificados válidos instalados en el almacén de usuarios y en el almacén del equipo.

Certificado del almacén de usuarios:




Certificado del almacén de usuarios

Certificado del almacén de máquinas:




Certificado de almacén de máquinas

## Verificación

1. Verifique la configuración del perfil de conexión desde la CLI de 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. Ejecute este comando para verificar la conexión:

<#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
```

El nombre de usuario client.cisco.com se recupera del certificado de almacén de usuario CN como nombre de usuario de mapa del segundo certificado se selecciona en la sección AAA. Si se selecciona Primer certificado, el nombre de usuario se recupera del certificado del almacén de la máquina, que es machine.cisco.com.

# Troubleshoot

1. Asegúrese de que haya certificados válidos en el almacén de certificados de usuario y en el almacén de certificados de equipo.

2. Recopile los debugs en FTD para verificar los registros relacionados con la validación de certificados usando debug crypto ca 14.
3. Revisar DART desde el equipo del usuario.

Registros de DART desde el escenario de trabajo:

<#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**

****************************************

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).