# Configurar Autenticação de Certificado Múltiplo no FTD para RAVPN

## Contents



## Introdução

Este documento descreve o procedimento para usar a autenticação de vários certificados para cliente seguro no Firepower Threat Defense (FTD) gerenciado pelo FMC.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico de VPN de acesso remoto (RAVPN)
- Experiência com o Firepower Management Center (FMC)
- Conhecimento básico dos certificados X509

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD da Cisco - 7,6
- FMC da Cisco - 7.6
- Windows 11 com Cisco Secure Client 5.1.4.74

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

Antes da versão 7.0 do software, o FTD suporta autenticação baseada em certificado único, o que significa que o usuário ou a máquina podem ser autenticados, mas não ambos, para uma única tentativa de conexão.

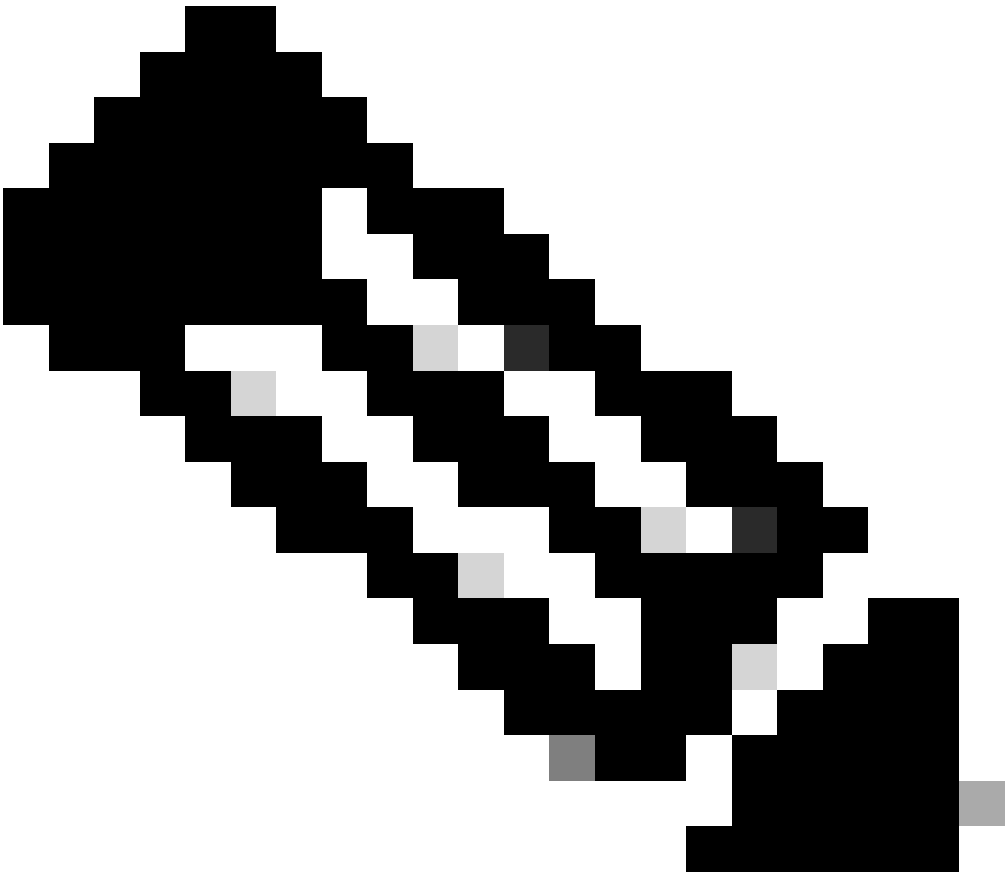
A autenticação baseada em vários certificados permite que a defesa contra ameaças valide o certificado da máquina ou do dispositivo, para garantir que o dispositivo seja um dispositivo emitido pela empresa, além de autenticar o certificado de identidade do usuário para permitir acesso VPN usando oCliente Segurodurante a fase SSL ou EAP IKEv2.

A autenticação de vários certificados limita o número de certificados a dois. O Cliente Seguro deve indicar suporte para autenticação de vários certificados. Se esse não for o caso, o gateway usa um dos métodos de autenticação herdados ou falha na conexão.Secure Clientversion 4.4.04030 ou posterior suporta a autenticação baseada em Multi-Certificado.

# Configurações

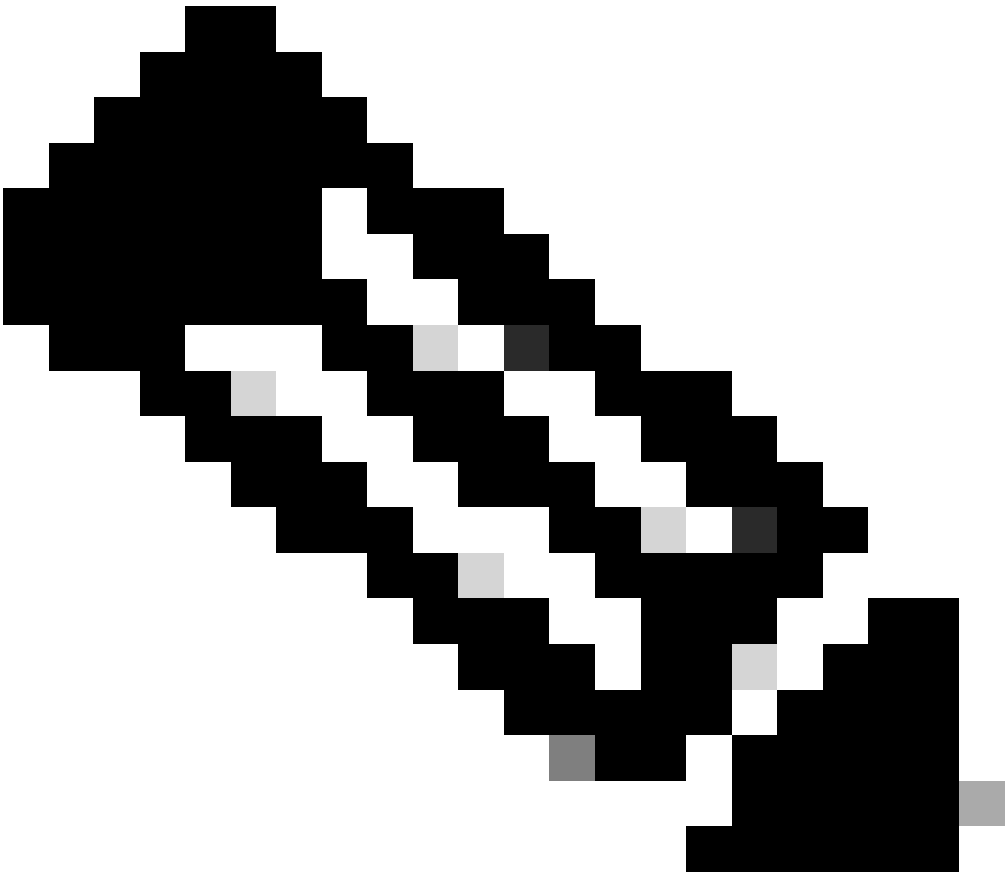
## Configuração no FTD

1. Navegue até Dispositivos > VPN > Acesso remoto.
2. Selecione a política de VPN de acesso remoto e clique em Editar.



Note: Se você não configurou uma VPN de acesso remoto, clique em Adicionar para criar uma nova política de VPN de acesso remoto.

3. Selecione e edite um Perfil de Conexão para configurar a autenticação de vários certificados.
4. Clique nas configurações de AAA e escolha Authentication Method como Client Certificate Only ou Client Certificate & AAA.



Note: Selecione o Servidor de autenticação se tiver selecionado o Certificado do cliente e o método de autenticação AAA.

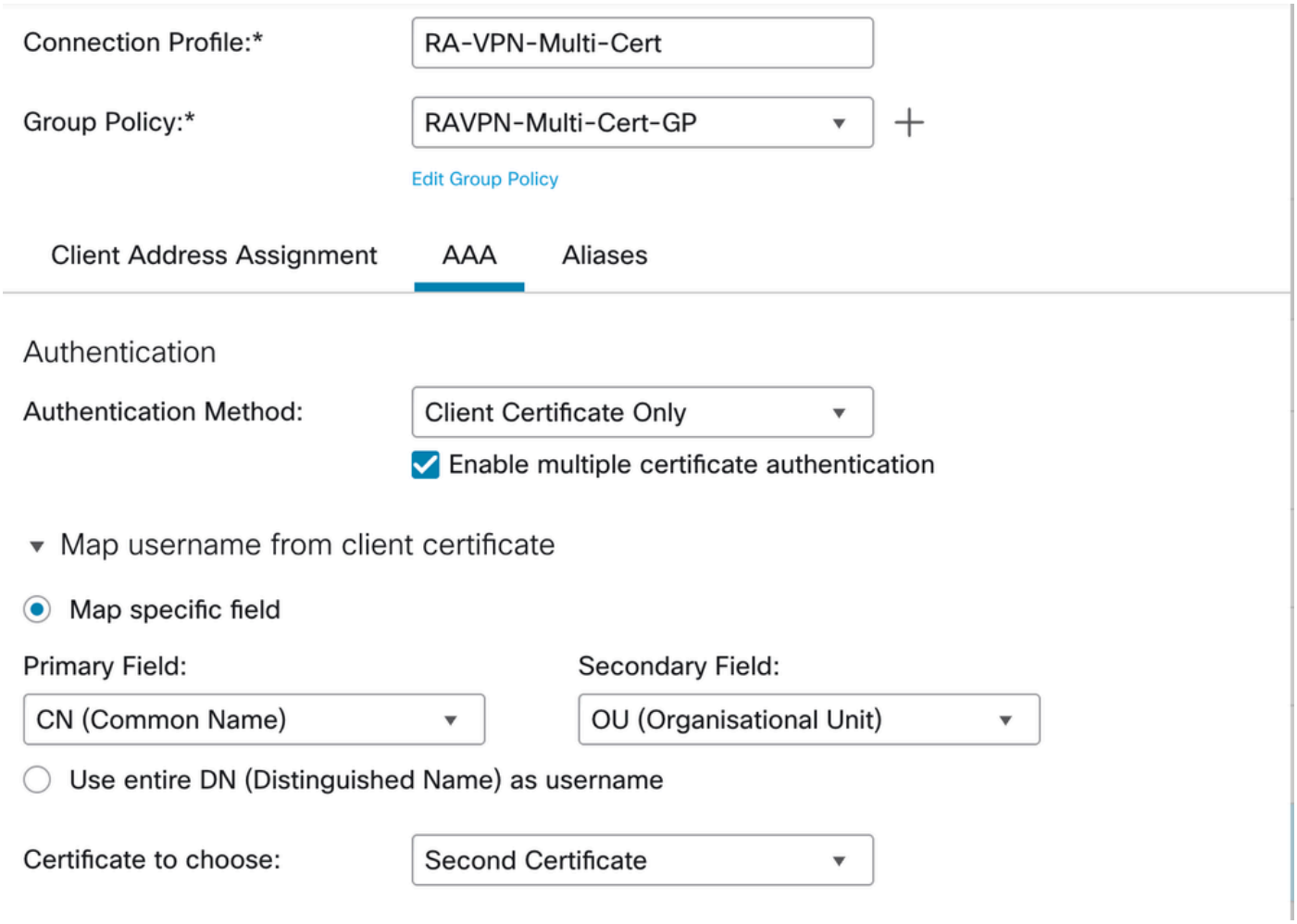
5. Marque a caixa de seleção Enable multiple certificate authentication.

6. Escolha um dos certificados para Mapear o nome de usuário do certificado do cliente:

   - First Certificate— Selecione esta opção para mapear o nome de usuário do certificado da máquina enviado do cliente VPN.
   - Segundo certificado — Selecione esta opção para mapear o nome de usuário do certificado de usuário enviado do cliente.

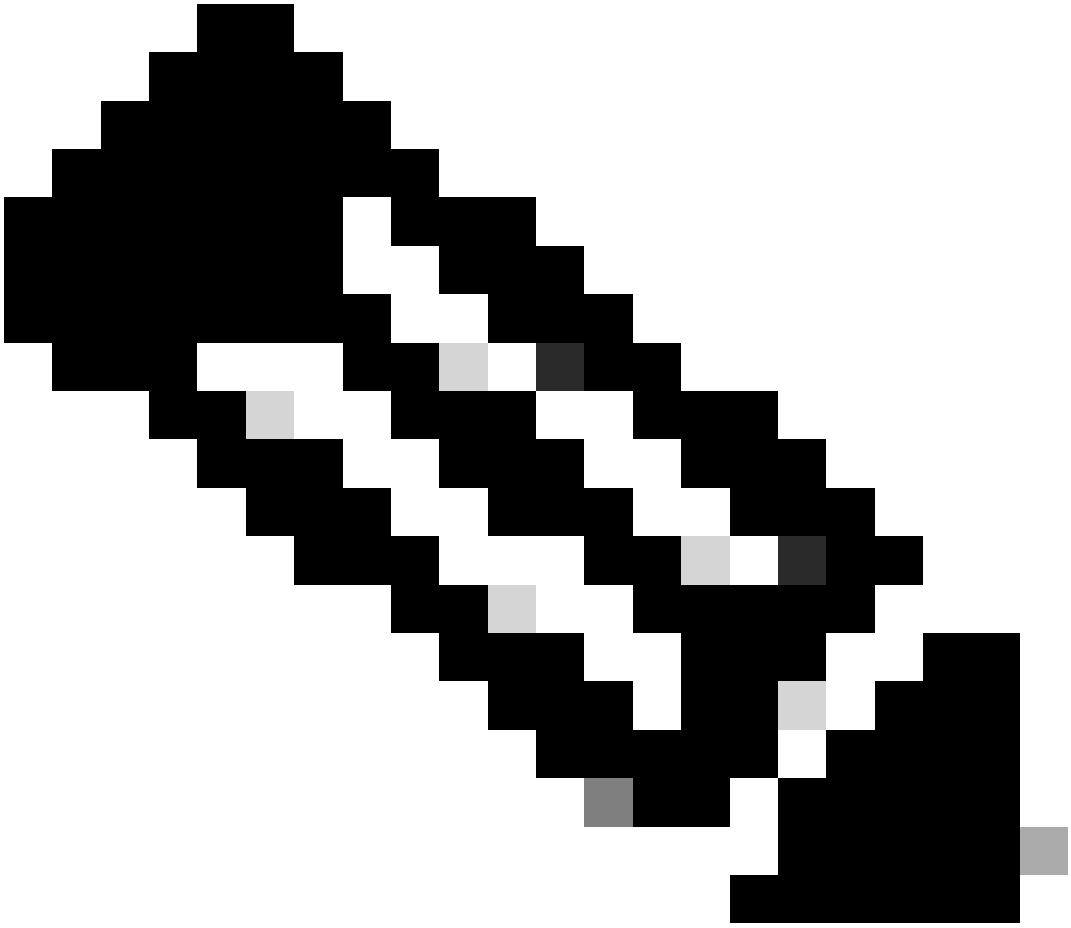
   O nome de usuário enviado do cliente é usado como o nome de usuário da sessão VPN quando a autenticação somente certificado está habilitada. Quando AAA e autenticação de certificado estão habilitados, o nome de usuário da sessão VPN é baseado na opção Prefill.

7. Se você selecionar a opção Mapear campo específico, que inclui o nome de usuário do certificado do cliente, os campos Primário e Secundário exibirão valores padrão: Nome comum (CN)e Unidade organizacional (OU)respectivamente.




Configurações AAA do Perfil de Conexão

8. Se você selecionar a opção Usar Nome Distinto (DN) inteiro como nome de usuário, o sistema recuperará automaticamente a identidade do usuário. Um nome distinto é uma identificação exclusiva, formada por campos individuais que podem ser usados como identificador ao corresponder usuários a um perfil de conexão. As regras DN são usadas para autenticação de certificado avançada.



Note: Se você tiver selecionado a autenticação Certificado de cliente e AAA, selecione a opção Prefill username from certificate on user login window para preencher previamente o nome de usuário secundário do certificado de cliente quando o usuário se conectar via módulo Secure Client VPN do Cisco Secure Client.

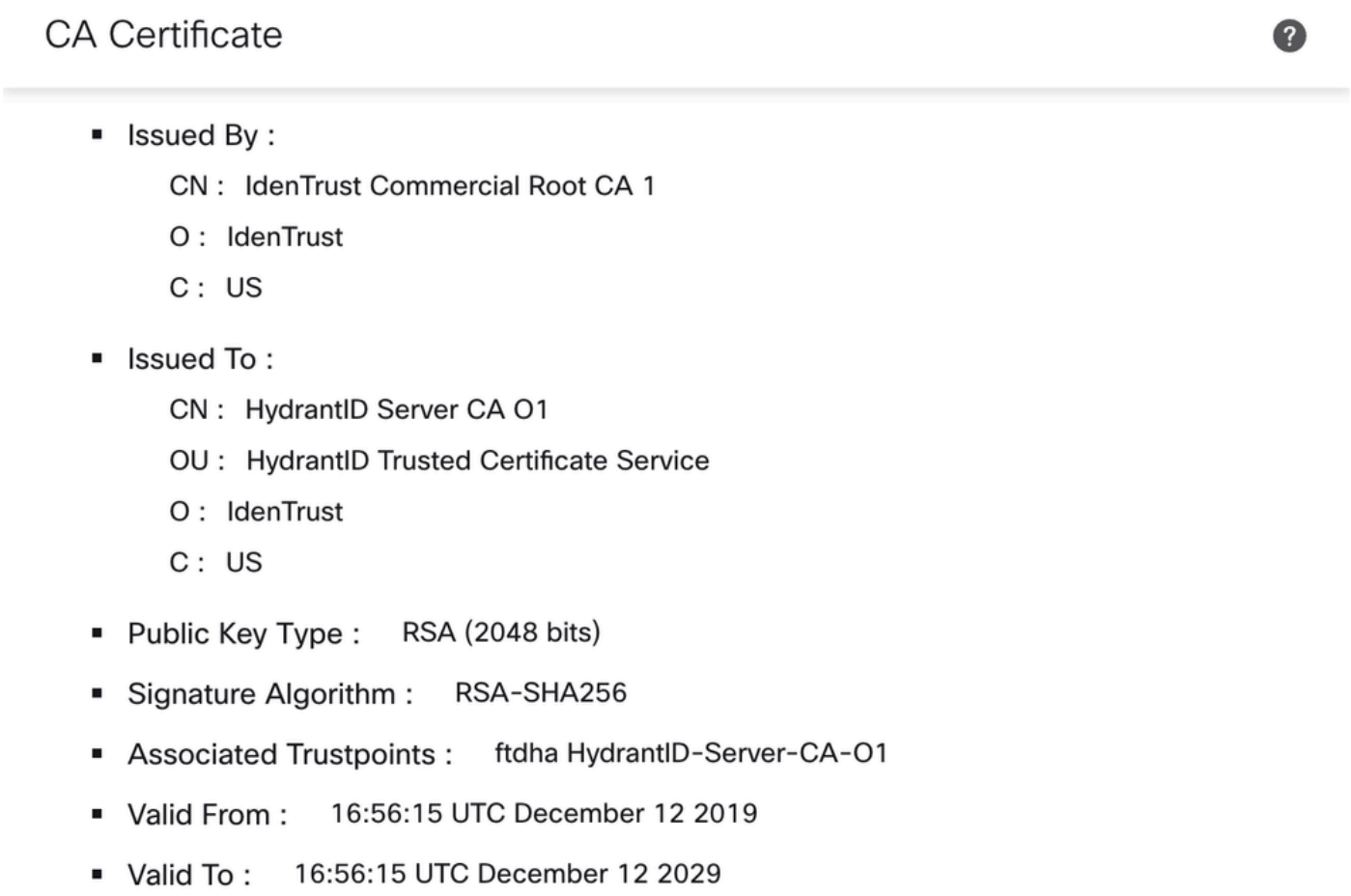
Ocultar nome de usuário na janela de login: O nome de usuário secundário é pré-preenchido a partir do certificado do cliente, mas oculto para o usuário para que ele não modifique o nome de usuário pré-preenchido.

---

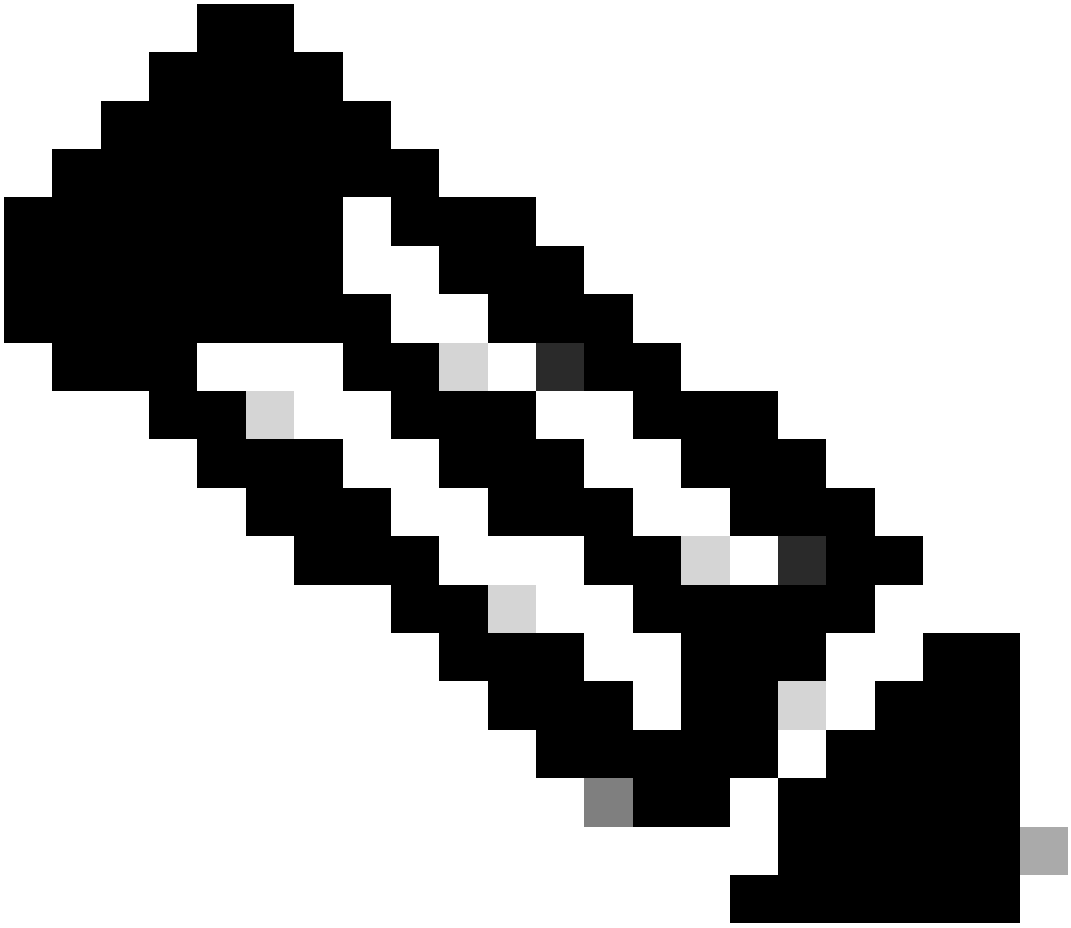
9. Para obter outras configurações detalhadas, consulte Configurar VPN de Acesso Remoto de Cliente Seguro (AnyConnect) no FTD.

10. Carregue os certificados CA do certificado de repositório do usuário e do certificado de repositório do computador no FTD para uma Validação bem-sucedida. Como neste cenário, o certificado de repositório do usuário e o certificado de repositório do computador são assinados pela mesma CA, a instalação dessa CA é suficiente. Se o certificado de armazenamento do usuário e o certificado de armazenamento do computador forem assinados por uma autoridade de

certificação diferente, os dois certificados dessa autoridade de certificação deverão ser carregados no FTD.




Certificado CA instalado no FTD pelo FMC

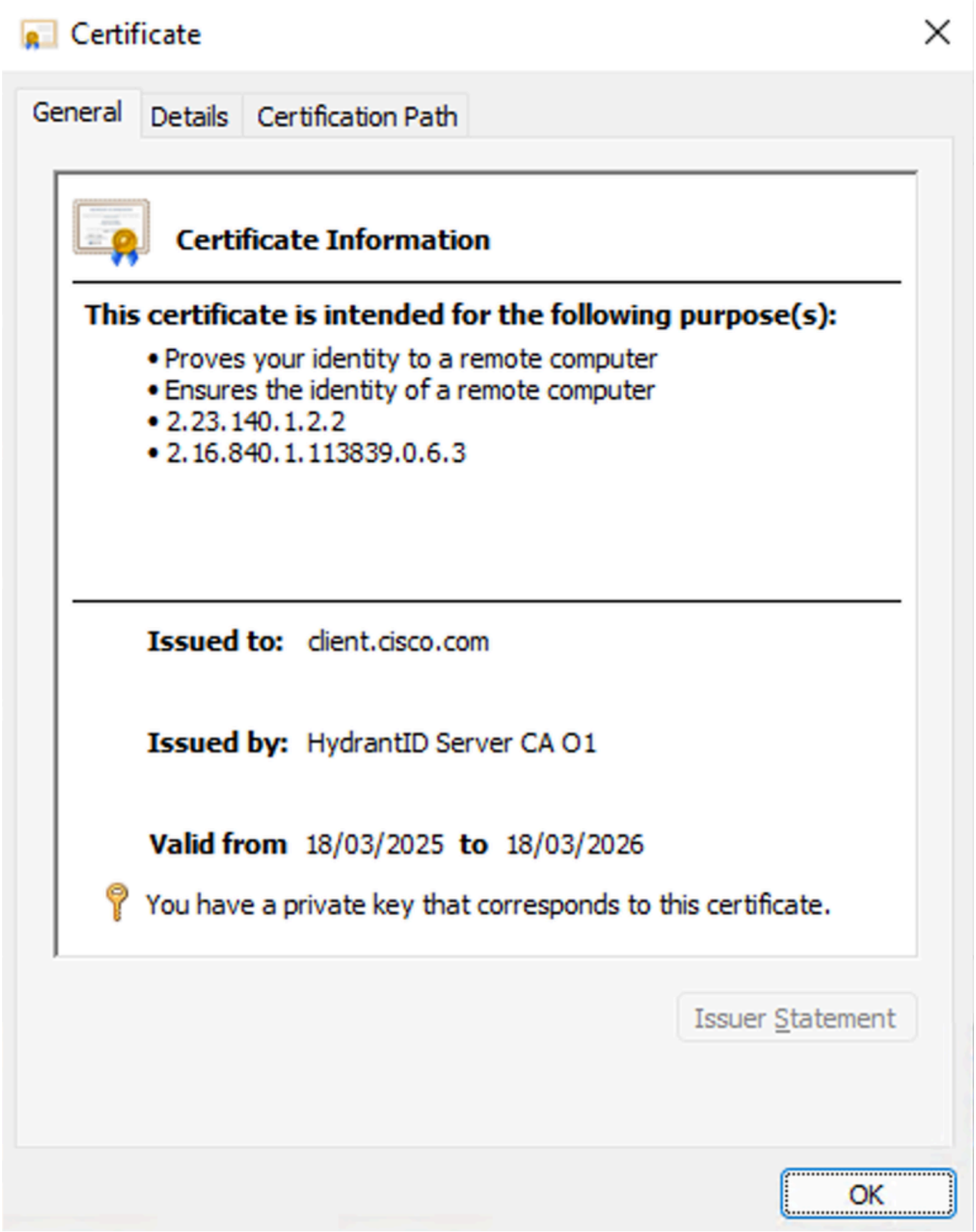


Note: O Perfil do cliente AnyConnect deve ter CertificateStore definido como All e CertificateStoreOverride definido como true se o usuário não tiver direitos de administrador.

## Certificados no Computador do Usuário

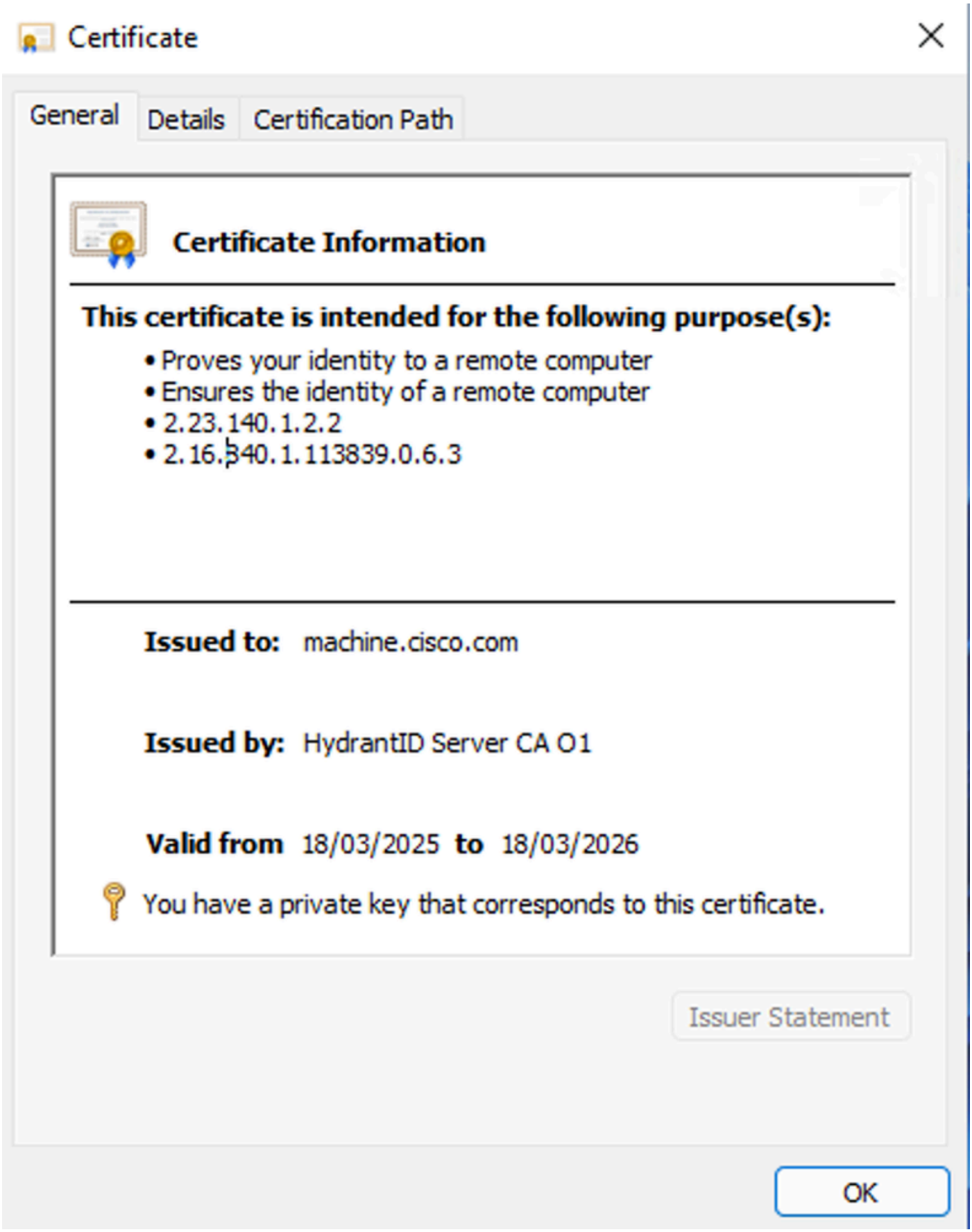
O computador do usuário que deve se conectar a este perfil de conexão deve ter certificados válidos instalados no repositório do Usuário e no repositório do Computador.

Certificado do Repositório de Usuários:




Certificado de Armazenamento de Usuário

Certificado do Repositório do Computador:




Certificado de armazenamento do computador

## Verificar

1. Verifique a configuração do perfil de conexão a partir da CLI do 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. Execute este comando para verificar a conexão:

<#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
```

O nome de usuário client.cisco.comé recuperado do Certificado de repositório de usuário CN, pois o nome de usuário do mapa do Segundo Certificado é selecionado na seção AAA. Se a opção Primeiro certificado for selecionada, o nome de usuário será recuperado do certificado de armazenamento da máquina, que é machine.cisco.com.

# Troubleshooting

1. Verifique se os certificados válidos estão presentes no repositório de Certificados do Usuário e no repositório de Certificados do Computador.

2. Colete depurações no FTD para verificar logs relacionados à validação de certificado usando debug crypto ca 14.
3. Revise o DART na máquina do usuário.

Logs do DART do cenário de trabalho:

<#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**

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.