

RAVPN用のFTDでの複数の証明書認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[FTDの設定](#)

[ユーザマシン上の証明書](#)

[確認](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、FMCによって管理されるFirepower Threat Defense(FTD)でセキュアクライアントの複数証明書認証(MCA)を使用する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- リモートアクセスVPN(RAVPN)の基本的な知識
- Firepower Management Center(FMC)の使用経験
- X509 証明書に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTD - 7.6
- Cisco FMC:7.6
- Cisco Secure Client 5.1.4.74がインストールされたWindows 11

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ソフトウェアバージョン7.0より前のFTDでは、単一の証明書ベースの認証がサポートされています。つまり、単一の接続を試みると、ユーザまたはマシンのどちらか一方を認証できますが、両方を認証することはできません。

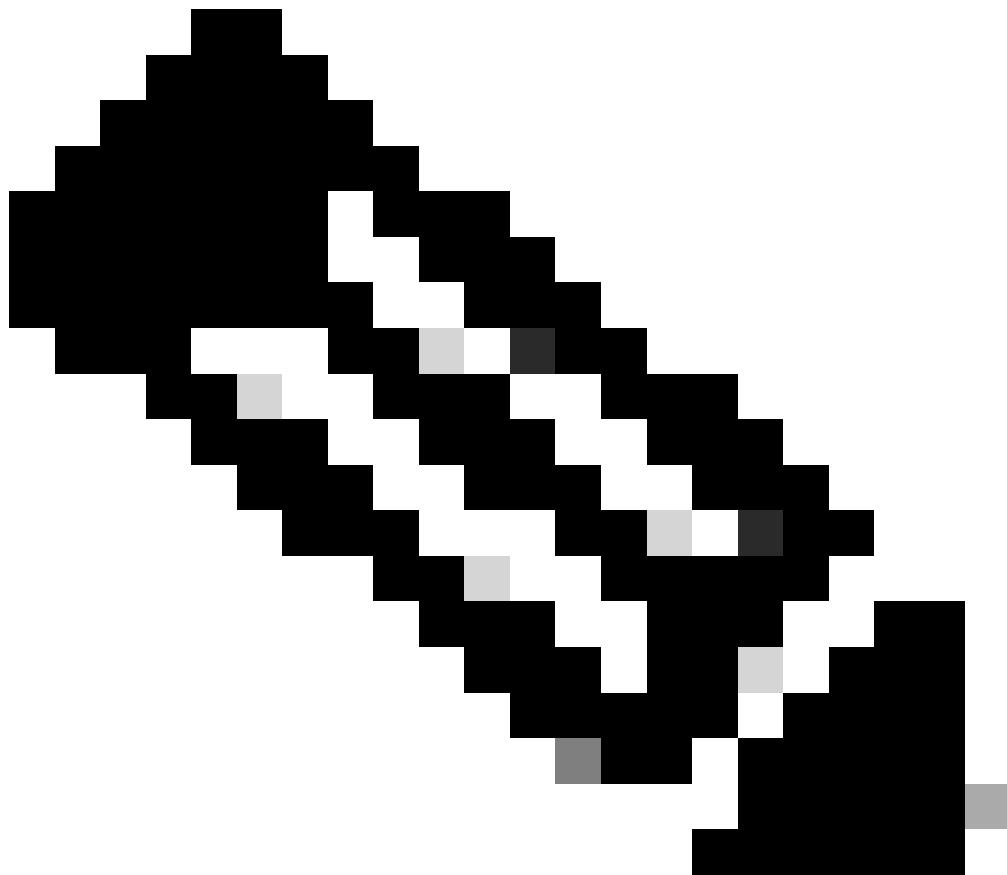
複数証明書ベースの認証では、SSLまたはIKEv2 EAPフェーズのセキュアクライアントを使用したVPNアクセスを許可するユーザのアイデンティティ証明書の認証に加えて、デバイスが企業発行のデバイスであることを確認するために、脅威防御でマシンまたはデバイスの証明書を検証できます。

現在、複数の証明書認証では、証明書の数が2つに制限されています。Secure Clientは、複数の証明書認証のサポートを示す必要があります。表示されていない場合は、ゲートウェイでレガシー認証方式のいずれかが使用されているか、接続が失敗しています。Secure Client version 4.4.04030以降では、複数証明書ベースの認証がサポートされています。

コンフィギュレーション

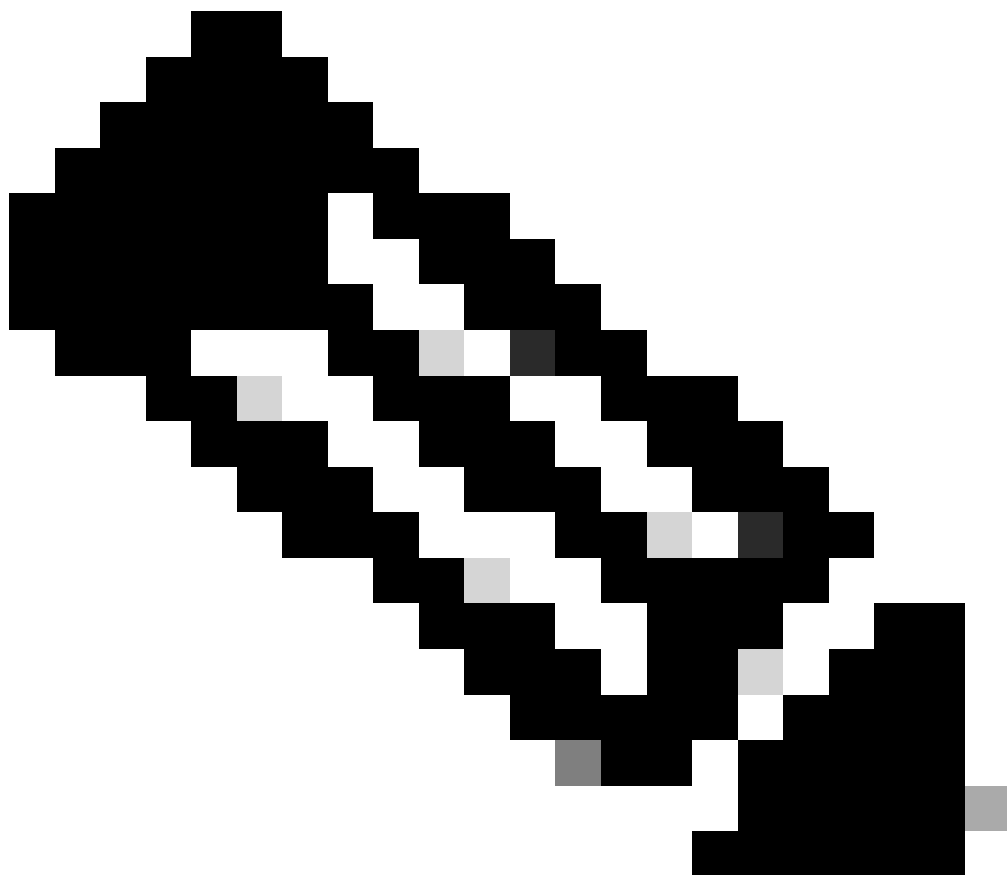
FTDの設定

1. Devices > VPN > Remote Accessの順に移動します。
2. Remote Access VPN policyを選択し、Editをクリックします。



注：リモートアクセスVPNを設定していない場合は、Addをクリックして新しいリモートアクセスVPNポリシーを作成します。

-
3. 接続プロファイルを選択して編集し、複数の証明書認証を設定します。
 4. AAA settingsをクリックし、Authentication Method as Client Certificate OnlyまたはClient Certificate & AAAを選択します。



注：クライアント証明書とAAA認証方式を選択している場合は、認証サーバを選択します。

-
5. Enable multiple certificate authenticationチェックボックスを選択します。
 6. 次のいずれかの証明書を選択して、クライアント証明書からユーザ名をマッピングします。
 - First Certificate:VPNクライアントから送信されたマシン証明書からユーザ名をマッピングする場合は、このオプションを選択します。
 - Second Certificate：クライアントから送信されたユーザ証明書からユーザ名をマッピングする場合は、このオプションを選択します。

証明書のみの認証が有効な場合、クライアントから送信されたユーザ名がVPNセッションユーザ名として使用されます。AAAおよび証明書認証が有効な場合、VPNセッションのユーザ名はプレフィルオプションに基づきます。

7. クライアント証明書からのユーザ名を含む、Map specific fieldオプションを選択した場合、PrimaryフィールドとSecondaryフィールドにはデフォルト値のCommon Name(CN)とOrganizational Unit(OU)がそれぞれ表示されます。

Connection Profile:*	RA-VPN-Multi-Cert	
Group Policy:*	RAVPN-Multi-Cert-GP ▼	+
	Edit Group Policy	
Client Address Assignment	AAA	Aliases

Authentication

Authentication Method:

Client Certificate Only ▼

☒ Enable multiple certificate authentication

▼ Map username from client certificate

☒ Map specific field

Primary Field:

CN (Common Name) ▼

Secondary Field:

OU (Organisational Unit) ▼

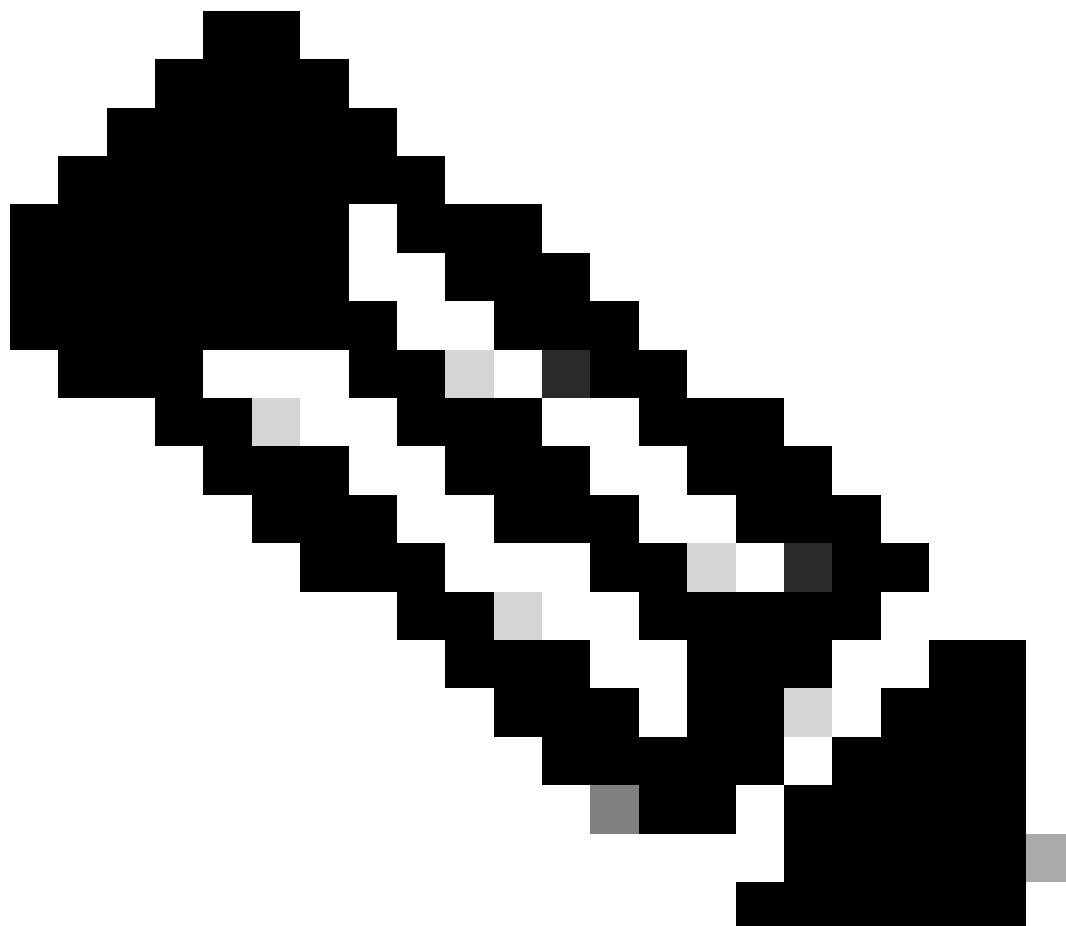
☐ Use entire DN (Distinguished Name) as username

Certificate to choose:

Second Certificate ▼

接続プロファイルのAAA設定

8. 「識別名(DN)全体をユーザー名として使用」オプションを選択した場合、システムは自動的にユーザーIDを取得します。識別名は、ユーザを接続プロファイルと照合する際に識別子として使用できる個々のフィールドで構成される一意の識別子です。DNルールは、拡張証明書認証に使用されます。



注:Client Certificate & AAA authenticationを選択した場合、ユーザがCisco Secure ClientのSecure Client VPNモジュールを介して接続するときに、クライアント証明書のセカンダリユーザ名をプリフィルするためにPrefill username from certificate on user login windowオプションを選択します。

ログインウィンドウでユーザ名を非表示にする：セカンダリユーザ名はクライアント証明書から事前入力されますが、ユーザが事前入力されたユーザ名を変更しないようにユーザには表示されません。

9. その他の詳細な設定については、『[FTDでのセキュアクライアント\(AnyConnect\)リモートアクセスVPNの設定](#)』を参照してください。

10. 検証が成功するように、ユーザストア証明書とマシンストア証明書のCA証明書をFTDにアップロードします。このシナリオでは、ユーザストア証明書とマシンストア証明書は同じCAによって署名されるため、1つのCAをインストールするだけで十分です。ユーザストア証明書とマシンストア証明書が異なるCAによって署名されている場合、これらのCA証明書の両方をFTDにアップロードする必要があります。

- 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

FMCからFTDにインストールされたCA証明書



注：ユーザに管理者権限がない場合、AnyConnectクライアントプロファイルの CertificateStoreをAllに設定し、CertificateStoreOverrideをtrueに設定する必要があります。

ユーザマシン上の証明書

この接続プロファイルに接続しようとしているユーザマシンには、ユーザーストアとマシンストアに有効な証明書がインストールされている必要があります。

ユーザーストアからの証明書：

General

Details

Certification Path

**Certificate Information****This certificate is intended for the following purpose(s):**

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2
- 2.16.840.1.113839.0.6.3

Issued to: client.cisco.com**Issued by:** HydrantID Server CA O1**Valid from** 18/03/2025 **to** 18/03/2026

You have a private key that corresponds to this certificate.

Issuer Statement

OK

ユーザーストア証明書

コンピューターストアからの証明書 :

General Details Certification Path

**Certificate Information****This certificate is intended for the following purpose(s):**

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2
- 2.16.840.1.113839.0.6.3

Issued to: machine.cisco.com**Issued by:** HydrantID Server CA O1**Valid from** 18/03/2025 **to** 18/03/2026

You have a private key that corresponds to this certificate.

Issuer Statement

OK

1. FTD CLIから接続プロファイル設定を確認します。

<#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. 次のコマンドを実行して、接続を確認します。

<#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

TCP Src Port : 53927

Hashing : none

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

AAAセクションでMap username from Second Certificateが選択されているため、ユーザストア証明書CNからユーザ名client.cisco.comが取得されます。First Certificateを選択した場合、ユーザ名はmachine.cisco.comのマシンスストア証明書から取得されます。

トラブルシュート

1. 有効な証明書がユーザー証明書ストアとコンピューター証明書ストアに存在することを確認してください。
2. debug crypto ca 14を使用してFTDでデバッグを収集し、証明書の検証に関連するログを確認

認します。

3. ユーザマシンからDARTを確認します。

作業シナリオのDARTログ：

<#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 01
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 01
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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。