

FMCによって管理されるFTDでのセキュアなクライアント証明書認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[a. サーバ認証に使用する証明書の作成/インポート](#)

[b. 信頼できる/内部CA証明書の追加](#)

[c. VPNユーザのアドレスプールの設定](#)

[d. セキュアなクライアントイメージのアップロード](#)

[e. XMLプロファイルの作成およびアップロード](#)

[リモートアクセスVPNの設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、証明書認証を使用してFirepower Management Center(FMC)で管理されるFirepower Threat Defense(FTD)でリモートアクセスVPN(RVPN)を設定するプロセスについて説明します。

著者 : Cisco TACエンジニア、Dolly JainおよびRishabh Aggarwal

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。

- ・ 証明書の手動登録とSSLの基礎
- ・ FMC
- ・ リモートアクセスVPNの基本認証に関する知識
- ・ Entrust、Geotrust、GoDaddy、Thawte、VeriSignなどのサードパーティ認証局(CA)

使用するコンポーネント

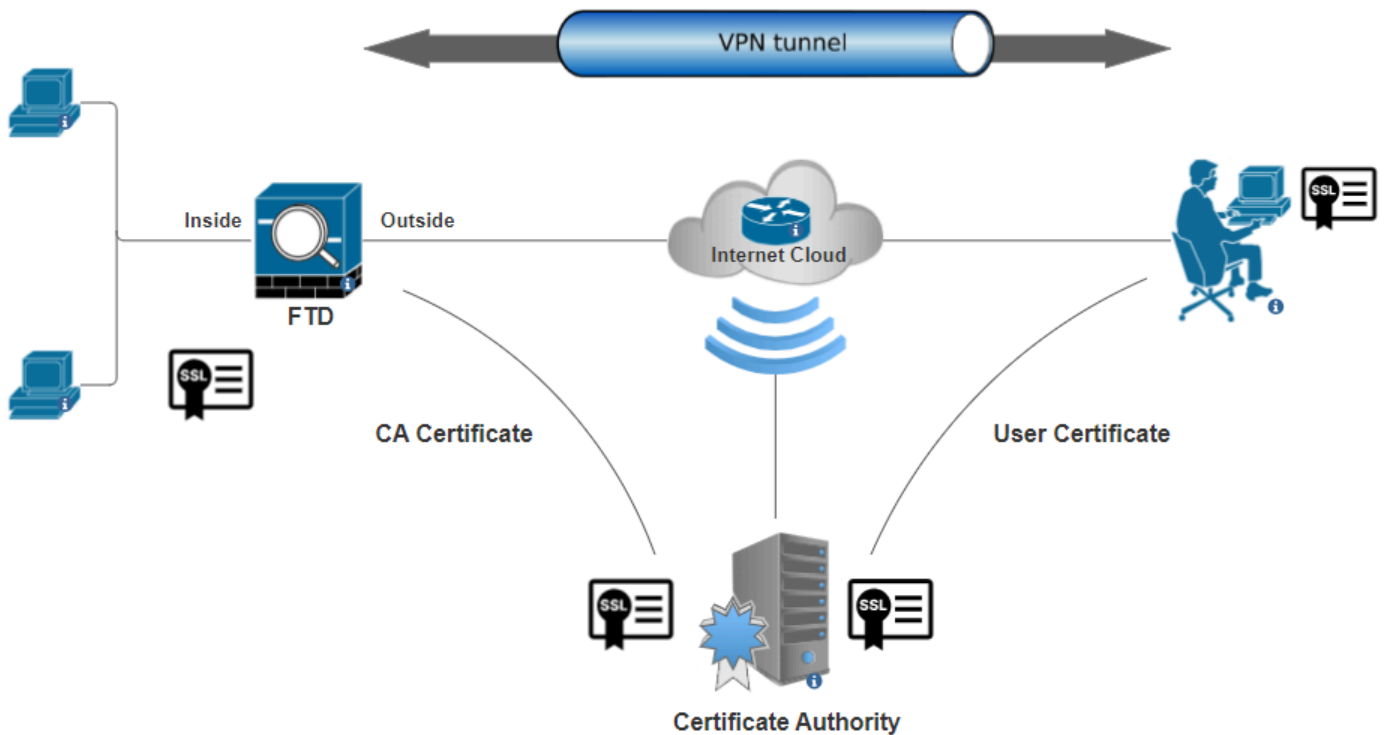
このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Secure Firepower Threat Defenseバージョン7.4.1
- Firepower Management Center (FMC) バージョン 7.4.1
- セキュア・クライアント・バージョン5.0.05040
- CAサーバとしてのMicrosoft Windows Server 2019

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。

設定

ネットワーク図



ネットワーク図

コンフィギュレーション

a.サーバ認証に使用する証明書の作成/インポート



注:FMCでは、CSRを生成する前にCA証明書が必要です。CSRが外部ソース (OpenSSLまたはサードパーティ) から生成される場合、手動の方法は失敗し、PKCS12証明書フォーマットを使用する必要があります。

ステップ 1 : に移動し Devices > CertificatesでAddをクリックします。Deviceを選択し、Cert Enrollmentの下のプラス記号 (+)をクリックします。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cancel

Add

証明書の登録の追加

ステップ 2 : CA Informationの下で、Enrollment TypeとしてManualを選択し、CSRの署名に使用する認証局(CA)証明書を貼り付けます。

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
HQYDVQQDEZXIEWRyYRw50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfl7J7ihLnTFbArj
N7ID-7...
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

CA情報の追加

ステップ 3 : Validation Usageで、IPsec Client, SSL ClientとSkip Check for CA flag in basic constraints of the CA Certificateを選択します。

ステップ 4 : Certificate Parametersで、サブジェクト名の詳細を入力します。

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Don't use FQDN in certificate

Include Device's IP Address:

Common Name (CN):

certauth.cisco.com

Organization Unit (OU):

TAC

Organization (O):

Cisco

Locality (L):

Bangalore

State (ST):

KA

Country Code (C):

IN

Email (E):

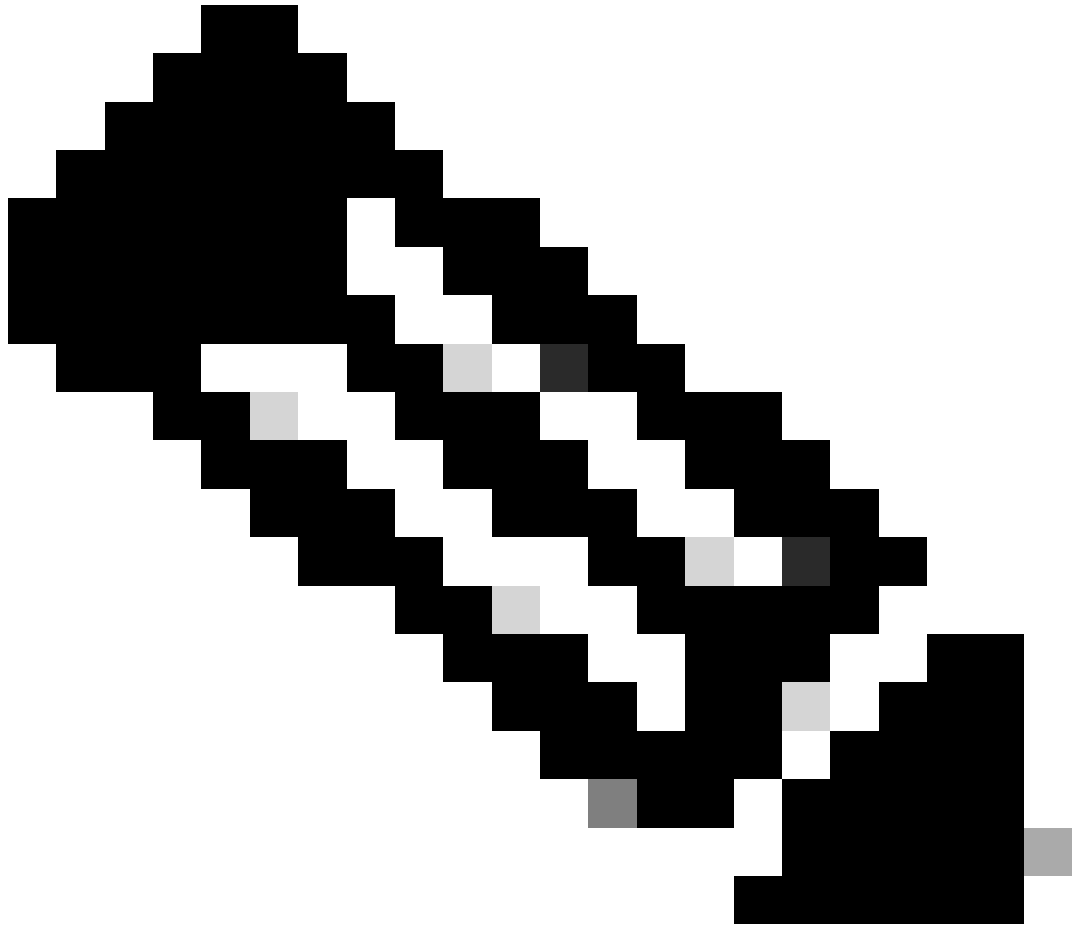
Include Device's Serial Number

Cancel

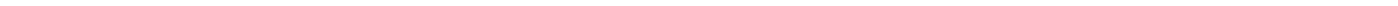
Save

証明書パラメータの追加

ステップ 5 : [Key]で、キー名とサイズを持つRSAのキータイプを選択します。 Saveをクリックします。



注:RSAキータイプの場合、最小キーサイズは2048ビットです。



Add Cert Enrollment



Name*
ssl_certificate

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
rsakey

Key Size:
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel **Save**

RSAキーの追加

手順 6 : Cert Enrollmentで、作成したばかりのドロップダウンからトラストポイントを選択してAddをクリックします。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

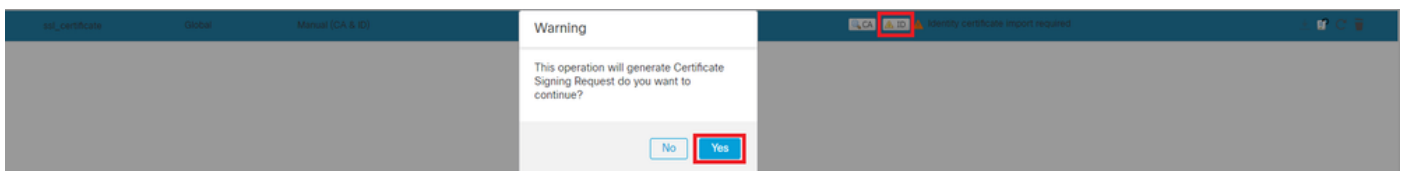
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

新しい証明書の追加

手順 7 : IDをクリックし、次にYesをクリックしてCSRを生成します。



CSR の生成

ステップ 8 : CSRをコピーし、認証局による署名を取得します。CAからID証明書が発行されたら、Browse Identity Certificateをクリックしてインポートし、Importをクリックします。

Import Identity Certificate



Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG  
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC  
SU4wggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK  
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO  
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP  
ppzi0uLlbVmb5iKQexllaur/e3PDeee3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

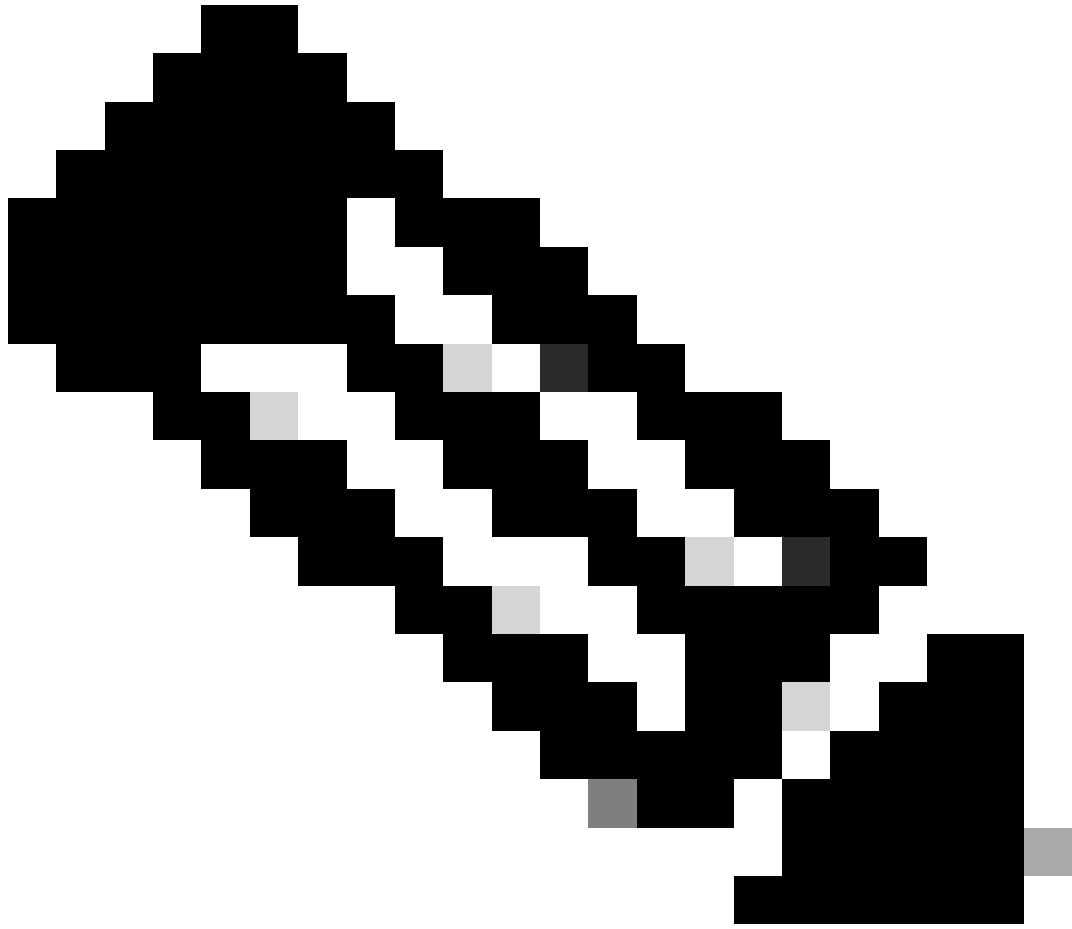
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)



注:ID証明書の発行に時間がかかる場合は、後でステップ7を繰り返すことができます。これにより、同じCSRが生成され、ID証明書をインポートできます。

b.信頼できる/内部CA証明書の追加

注：ステップ(a)で使用した認証局(CA)の「サーバ認証に使用する証明書の作成/インポート」でもユーザ証明書を発行している場合は、ステップ(b)「信頼できる/内部CA証明書の追加」は省略できます。同じCA証明書を再度追加する必要はなく、同様に削除する必要もあります。同じCA証明書を再度追加すると、トラストポイントは「validation-usage none」で設定されるため、RAVPNの証明書認証に影響を与える可能性があります。

ステップ 1：Devices > Certificatesに移動し、Addをクリックします。

Deviceを選択し、Cert Enrollmentの下のプラス記号(+)をクリックします。

ここでは、「auth-risagar-ca」を使用してID/ユーザ証明書を発行します。

General

Details

Certification Path



Certificate Information

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

- All issuance policies
- All application policies

Issued to: auth-risaggar-ca

Issued by: auth-risaggar-ca

Valid from 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

auth-risaggar-ca (認可を受ける必要がある)

ステップ 2 : トラストポイント名を入力し、ManualCA information で登録タイプとして選択します。

ステップ 3 : pem形式CA Onlyの信頼された/内部CA証明書を確認して貼り付けます。

ステップ 4 : チェックSkip Check for CA flag in basic constraints of the CA CertificateしてSaveをクリックします。

Add Cert Enrollment ?

Internal_CA

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGV  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel Save

トラストポイントの追加

ステップ 5 : Cert Enrollmentで、作成したばかりのドロップダウンからトラストポイントを選択してAddをクリックします。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name: Internal_CA
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Cancel

Add

内部CAの追加

手順 6 : 前の手順で追加した証明書は次のとおりです。

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	↑ ↓ ↻ 🗑
-------------	--------	------------------	-------------	-------	---------

追加された証明書

c. VPNユーザのアドレスプールの設定

ステップ 1 : Objects > Object Management > Address Pools > IPv4 Poolsに移動します。

ステップ 2 : 名前とIPv4アドレス範囲をマスクで入力します。

Edit IPv4 Pool



Name*

vpn_pool

Description

IPv4 Address Range*

10.20.20.1-10.20.20.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

Save

IPv4プールの追加

d.セキュアなクライアントイメージのアップロード

ステップ 1: [シスコソフトウェア](#) サイトから、OSに従ってwebdeployセキュアクライアントイメージをダウンロードします。

ステップ 2: Objects > Object Management > VPN > Secure Client File > Add Secure Client Fileに移動します。

ステップ 3: 名前を入力し、ディスクからSecure Clientファイルを選択します。

ステップ 4: ファイルタイプとしてSecure Client Imageを選択し、Saveをクリックします。

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

安全なクライアントイメージの追加

e. XMLプロファイルの作成およびアップロード

ステップ 1 : Secure Clientを[Ciscoソフトウェア](#)サイトProfile Editorからダウンロードしてインストールします。

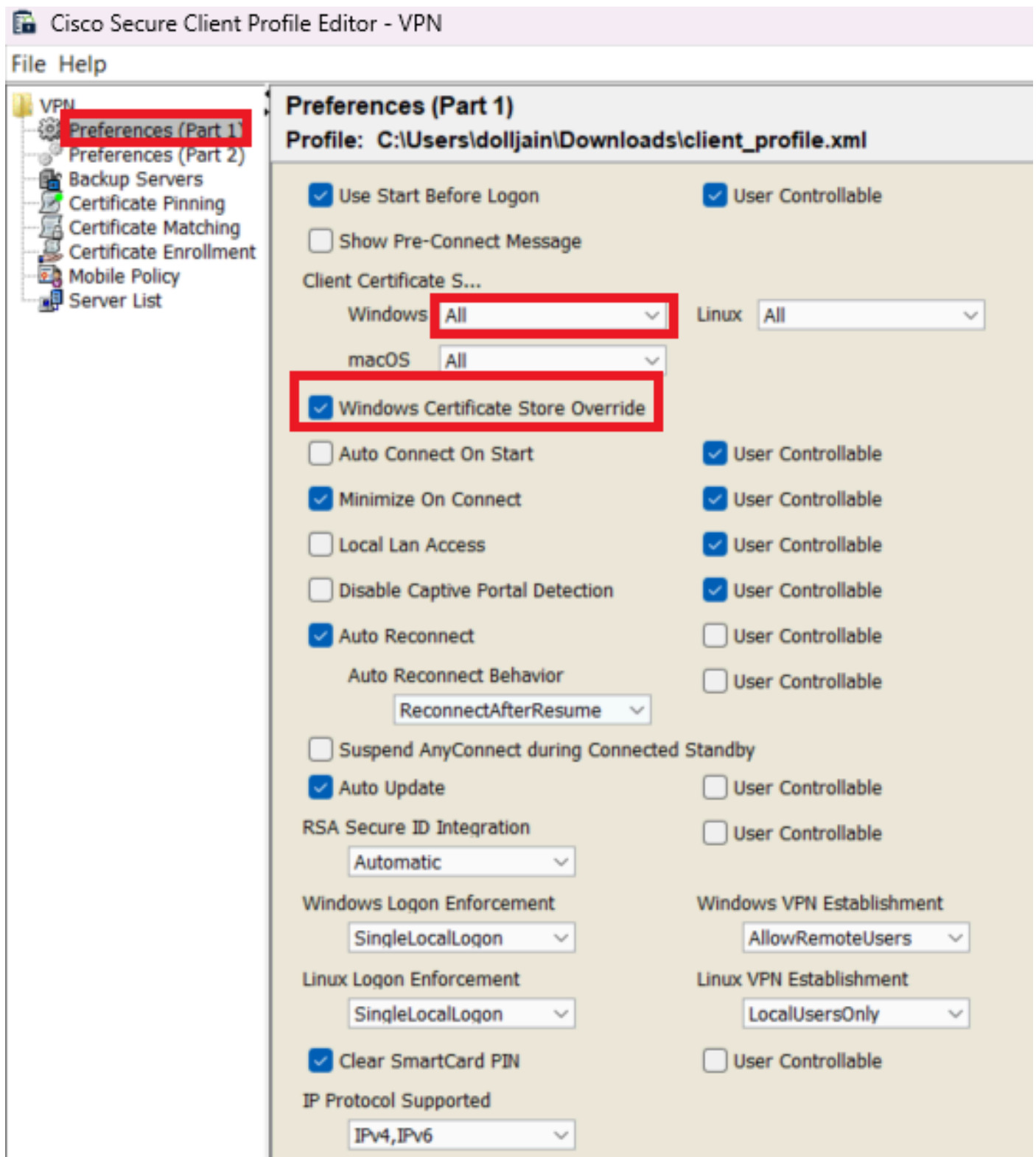
ステップ 2 : 新しいプロファイルを作成し、「Client Certificate Selection」ドロップダウンから「All」を選択します。主に、Secure Clientが証明書の保存と読み取りに使用できる証明書ストアを制御します。

その他に、次の2つのオプションがあります。

- マシン : セキュアクライアントは、Windowsのローカルマシンの証明書ストアでの証明書ルックアップに制限されます。
- User:Secure Clientは、ローカルのWindowsユーザ証明書ストアでの証明書ルックアップに制限されています。

証明書ストアのオーバーライドをTrueとして設定します。

これにより、管理者はSecure Clientに対して、クライアント証明書認証のためにWindowsマシン（ローカルシステム）証明書ストア内の証明書を使用するように指示できます。証明書ストアの上書きはSSLにのみ適用されます。SSLでは、接続はデフォルトでUIプロセスによって開始されます。IPSec/IKEv2を使用する場合、セキュアクライアントプロファイルのこの機能は適用されません。



基本設定を追加（パート1）

ステップ3:（オプション）ユーザに認証証明書の選択を求めるプロンプトが表示されないようにするため、Disable Automatic Certificate Selectionのチェックマークを外します。

- VPN
- Preferences (Part 1)
- Preferences (Part 2)**
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

Disable Automatic Certificate Selection

User Controllable

Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Untrusted Network Policy

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Authentication Timeout (seconds)

注：このACLは、セキュアクライアントが内部リソースにセキュアルートを追加するために使用します。

ステップ 2：Devices > VPN > Remote Accessに移動し、Addをクリックします。

ステップ 3：プロファイルの名前を入力し、FTDデバイスを選択してNextをクリックします。

The screenshot shows the 'Remote Access VPN Policy Wizard' interface. At the top, there are five steps: 1. Policy Assignment, 2. Connection Profile, 3. Secure Client, 4. Access & Certificate, and 5. Summary. The current step is 'Targeted Devices and Protocols'. Below this, there is a text box for 'Name:*' containing 'RAVPN', which is highlighted with a red box. There is also a 'Description:' text box. Under 'VPN Protocols:', both 'SSL' and 'IPsec-IKEv2' are checked. The 'Targeted Devices:' section is divided into 'Available Devices' and 'Selected Devices'. 'Available Devices' lists 'FTD-A-7.4.1', 'FTD-B-7.4.0', and 'FTD-ZTNA-7.4.1'. 'FTD-A-7.4.1' is selected and highlighted in blue. 'Selected Devices' shows 'FTD-A-7.4.1' with a trash icon. An 'Add' button is located between the two device lists. On the right side, there is a 'Before You Start' section with instructions on authentication servers, secure client packages, and device interfaces.

プロファイル名の追加

ステップ 4：Connection Profile Nameコマンドを入力し、Authentication, Authorization and Accounting (AAA ; 認証、認可、アカウントリング) の下のAuthentication Method asClient Certificate Only(認証方式)を選択します。

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

認証方法の選択

ステップ 5 : Client Address Assignmentの下のUse IP Address Pools をクリックし、以前に作成したIPv4アドレスプールを選択します。


Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) **i**

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

クライアントアドレス割り当ての選択

手順 6 : グループポリシーを編集します。

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

グループポリシーの編集

手順 7 : General > Split Tunnelingに移動し、Tunnel networks specified belowを選択して、Split Tunnel Network List Typeの下にある Standard Access Listを選択します。

先ほど作成したACLを選択します。

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List Extended Access List

Standard Access List:

Split_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

スプリットトンネリングの追加

ステップ 8 : Secure Client > Profileに移動し、を選択Client Profileし、Saveをクリックします。

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:

Anyconnect_Profile-5-0-05040 +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

セキュアクライアントプロファイルの追加

ステップ 9 : Nextをクリックし、Secure Client Imageを選択してNextをクリックします。

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows

安全なクライアントイメージの追加

ステップ 10 : Network Interface for VPN Accessを選択し、Device Certificatesを選択してsysopt permit-vpnにチェックマークを入れ、Nextをクリックします。

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +
 Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

VPNトラフィックのアクセスコントロールの追加

ステップ 11最後に、すべての設定を確認して、Finishをクリックします。

Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

リモートアクセスVPNポリシーの設定

ステップ 12 リモートアクセスVPNの初期設定が完了したら、作成した接続プロファイルを編集してAliasesに進みます。

ステップ 13 プラスアイコン(+)をクリックしてgroup-aliasを設定します。

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth


Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR following URLs, system

URL	
-----	--

Edit Alias Name

Alias Name:

 Enabled

Cancel OK

Cancel Save

グループエイリアスの編集

ステップ 14 : プラスアイコン(+)をクリックしてgroup-urlを設定します。クライアントプロファイルで以前に設定したのと同じグループURLを使用します。

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

Client Address Assignment AAA **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off.

Edit URL Alias

URL Alias:

certauth

Enabled

Cancel OK

URL Alias:

Configure the list of URL aliases. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

Cancel Save

グループURLの編集

ステップ 15 : Access Interfacesの順に移動します。SSL設定でInterface TrustpointおよびSSL Global Identity Certificateを選択します。

RAVPN

Enter Description

Connection Profile **Access Interfaces** Advanced

Local Realm: cisco-local Policy Assignments (1) Dynamic Access Policy: None

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: ssl_certificate

Note: Ensure the port used in VPN configuration is not used in other services

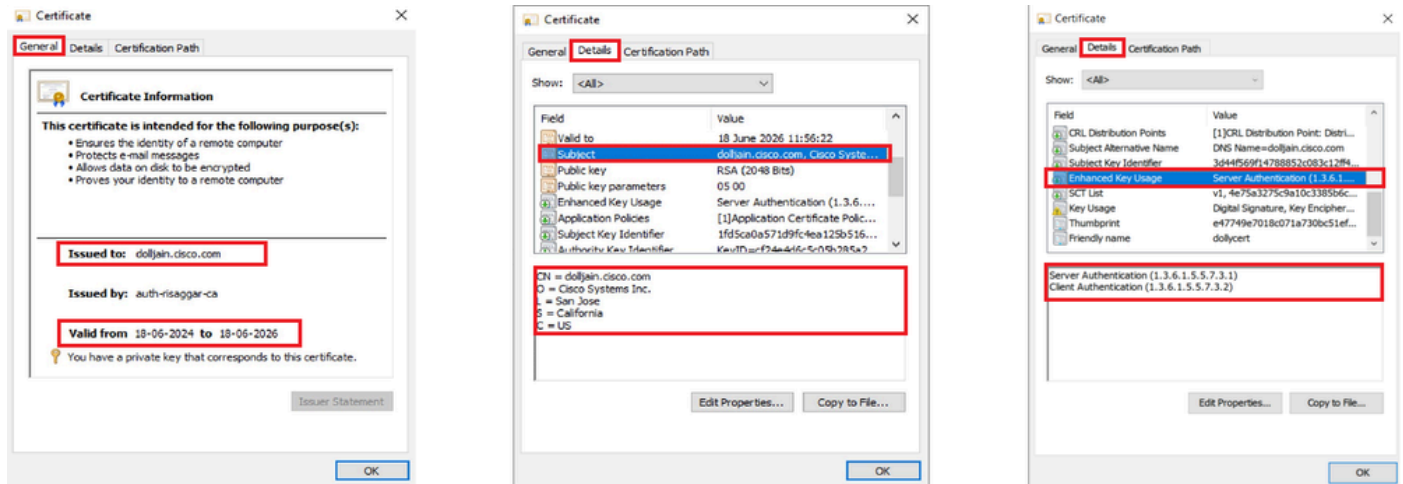
アクセスインターフェイスの編集

ステップ 16 : をクリックしてSave、これらの変更を展開します。

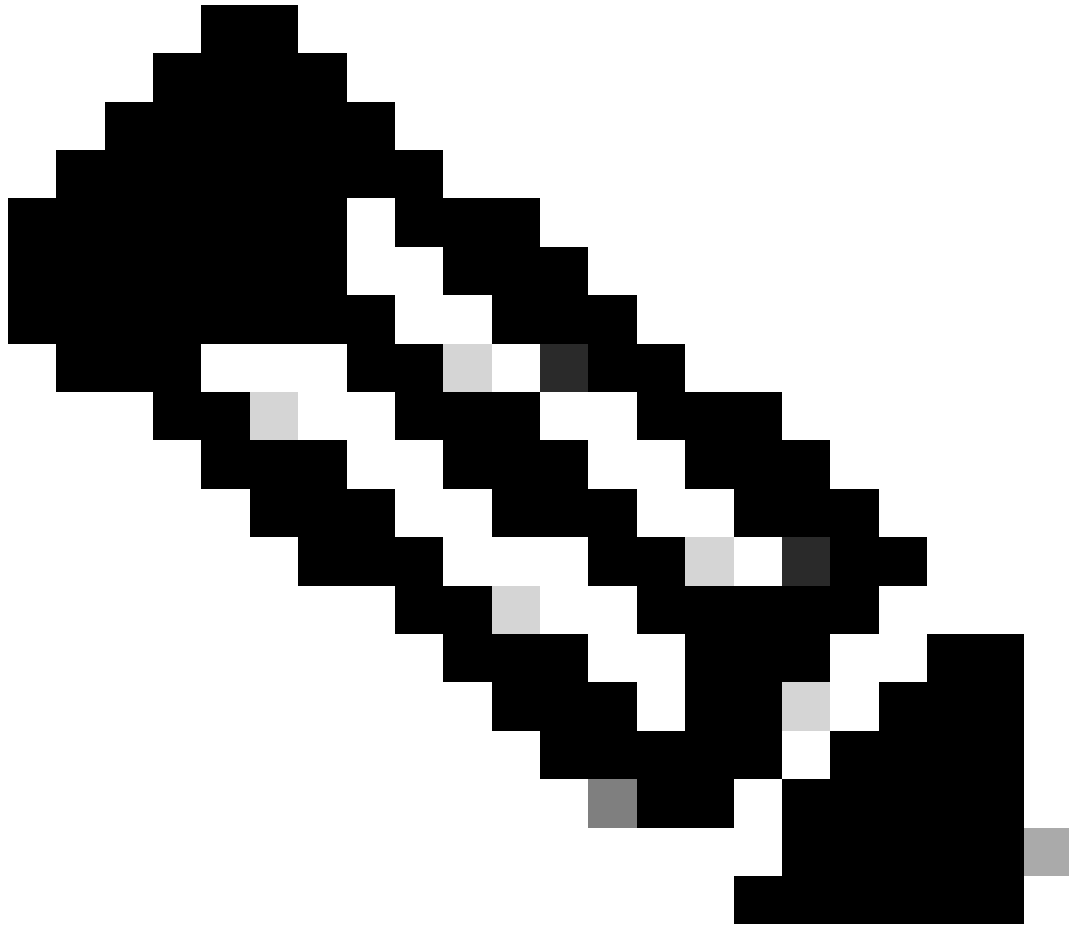
確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. セキュリティで保護されたクライアントPCには、有効な日付、サブジェクト、およびEKUが設定された証明書がユーザのPCにインストールされている必要があります。この証明書は、前述のように、FTDにインストールされている証明書を持つCAによって発行される必要があります。ここでは、IDまたはユーザ証明書が「auth-risagar-ca」によって発行されます。

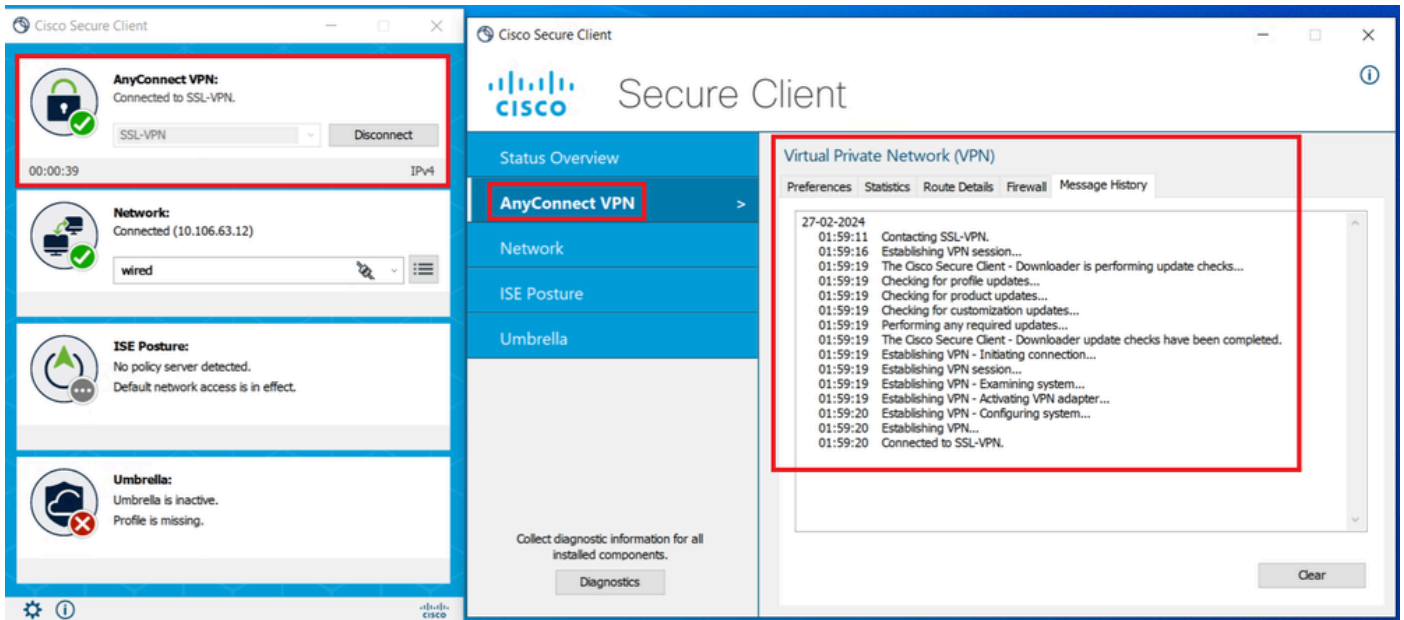


証明書の概要



注：クライアント証明書には、「Client Authentication」拡張キー使用法(EKU)が含まれている必要があります。

2. セキュアクライアントは接続を確立する必要があります。



セキュアクライアント接続の成功

3. show vpn-sessiondb anyconnectを実行して、使用されているトンネルグループの下でアクティブユーザの接続の詳細を確認します

。

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

1. デバッグは、FTDの診断CLIから実行できます。

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. 一般的な問題については、この[ガイド](#)を参照してください。

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。