

# FTDのローカル認証でSSLセキュアクライアントを設定する

## 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](#)

[設定](#)

[コンフィギュレーション](#)

[ステップ 1: ライセンスの確認](#)

[ステップ 2: Cisco Secure ClientPackageのFMCへのアップロード](#)

[ステップ 3: 自己署名証明書の生成](#)

[ステップ 4: FMCでのローカルレルムの作成](#)

[ステップ 5: SSL Cisco Secure Client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、Cisco FMCによって管理されるCisco FTDのローカル認証でCisco Secure Client ( Anyconnectを含む ) を設定する方法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。

- Firepower Management Center(FMC)によるSSLセキュアクライアント(SSL)の設定
- FMCによるFirePOWERオブジェクトの設定
- FirepowerでのSSL証明書

### 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 Firepower Threat Defense(FTD)バージョン7.0.0 ( ビルド94 )
- Cisco FMCバージョン7.0.0 ( ビルド94 )
- Cisco Secure Mobilityクライアント4.10.01075

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

この例では、Secure Sockets Layer(SSL)を使用して、FTDとWindows 10クライアント間にバーチャルプライベートネットワーク(VPN)を作成します。

リリース7.0.0以降、FMCによって管理されるFTDは、Cisco Secure Clientのローカル認証をサポートします。これは、プライマリ認証方式、またはプライマリ認証方式が失敗した場合のフォールバックとして定義できます。この例では、ローカル認証がプライマリ認証として設定されています。

このソフトウェアバージョンより前のバージョンでは、FTD上のCisco Secure Clientローカル認証は、Cisco Firepower Device Manager(FDM)でのみ使用できました。

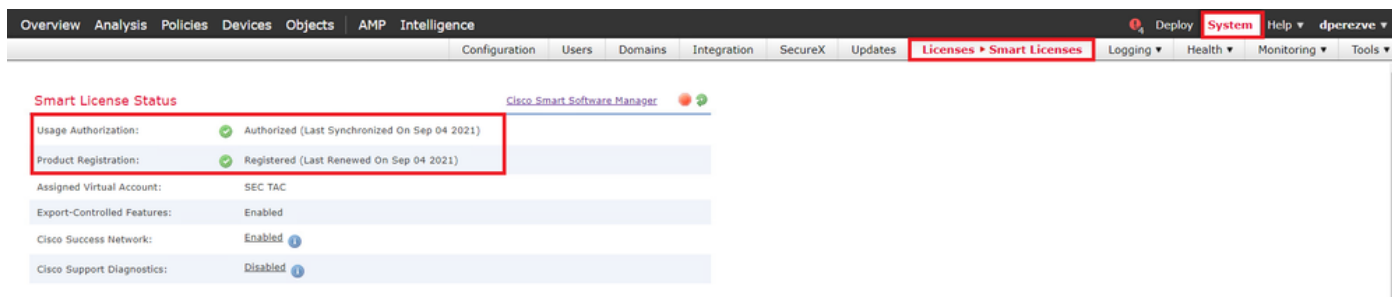
## 設定

### コンフィギュレーション

#### ステップ 1：ライセンスの確認

Cisco Secure Clientを設定する前に、FMCが登録され、スマートライセンシングポータルに準拠している必要があります。FTDに有効なPlus、Apex、またはVPN Onlyライセンスがない場合は、Cisco Secure Clientを導入できません。

System > Licenses > Smart Licensesの順に移動して、FMCが登録されていて、スマートライセンスポータルに準拠していることを確認します。



同じページを下にスクロールします。スマートライセンスのグラフの下部には、使用可能なCisco Secure Client(AnyConnect)ライセンスのタイプと、ライセンスにサブスクライブしているデバイスが表示されます。次のいずれかのカテゴリで、手元のFTDが登録されていることを確認します

。

Smart Licenses

Filter Devices... Edit Performance Tier Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (2)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (2)	✓			
ftdv-dperevze 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdva-dperevze (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMWare - v7.0.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

























Note: Container Instances of same blade share feature licenses

Activate Windows  
Go to System in Control Panel to activate Windows.

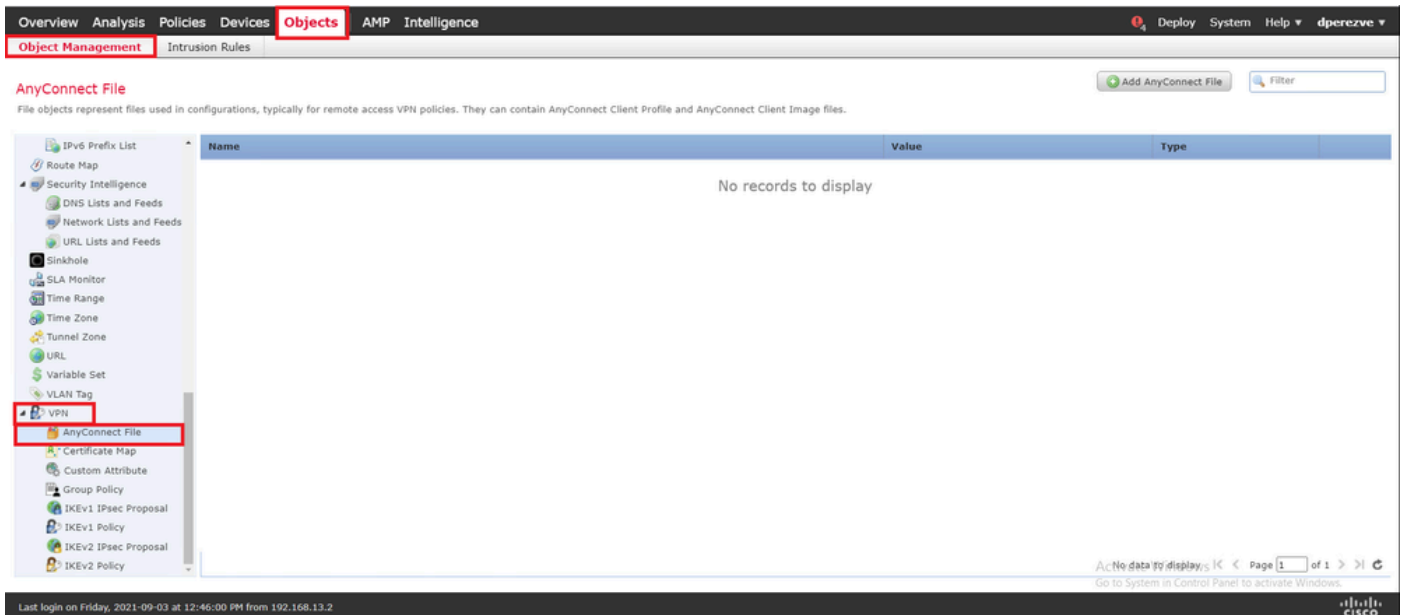
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

## ステップ 2 : Cisco Secure Client/パッケージのFMCへのアップロード

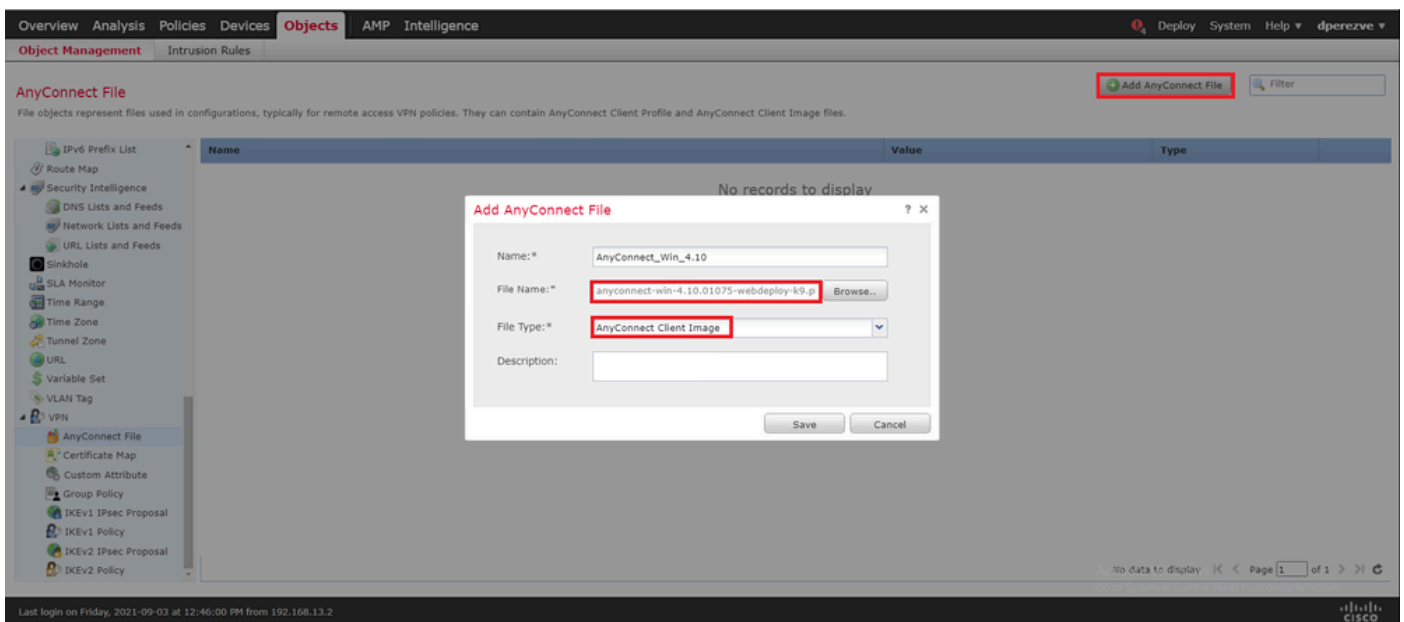
Windows用のCisco Secure Client(AnyConnect)ヘッドエンド導入パッケージを[cisco.com](https://www.cisco.com)からダウンロードします。

Application Programming Interface [API] (Windows) 	21-May-2021	141.72 MB	 
anyconnect-win-4.10.01075-vpnapi.zip <a href="#">Advisories</a> 			
AnyConnect Headend Deployment Package (Windows) 	21-May-2021	77.81 MB	 
anyconnect-win-4.10.01075-webdeploy-k9.pkg <a href="#">Advisories</a> 			
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files 	21-May-2021	34.78 MB	 
anyconnect-win-arm64-4.10.01075-predeploy-k9.zip <a href="#">Advisories</a> 			
AnyConnect Headend Deployment Package (Windows 10 ARM64) 	21-May-2021	44.76 MB	 
anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg <a href="#">Advisories</a> 			
Profile Editor (Windows) 	21-May-2021	10.90 MB	 
tools-anyconnect-win-4.10.01075-profileeditor-k9.msi <a href="#">Advisories</a> 			
AnyConnect Installer Transforms (Windows) 	21-May-2021	0.05 MB	 
tools-anyconnect-win-4.10.01075-transforms.zip <a href="#">Advisories</a> 			

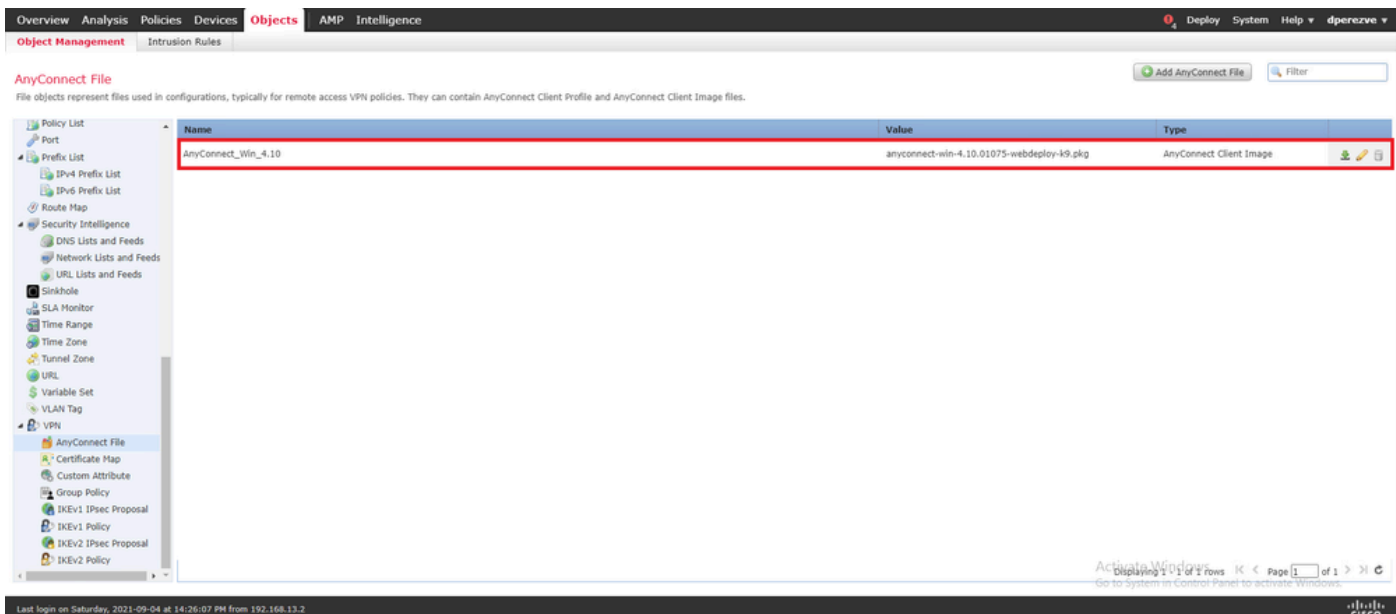
Cisco Secure Clientイメージをアップロードするには、Objects > Object Managementの順に選択し、目次でVPNカテゴリの下にあるCisco Secure Client Fileを選択します。



Add AnyConnect Fileボタンを選択します。Add AnyConnect Secure Client Fileウィンドウで、オブジェクトに名前を割り当て、Browse...を選択して、Cisco Secure Client/パッケージを選択します。最後に、ドロップダウンメニューでファイルタイプとしてAnyConnect Client Imageを選択します。




Saveボタンを選択します。オブジェクトをオブジェクトリストに追加する必要があります。



### ステップ 3 : 自己署名証明書の生成

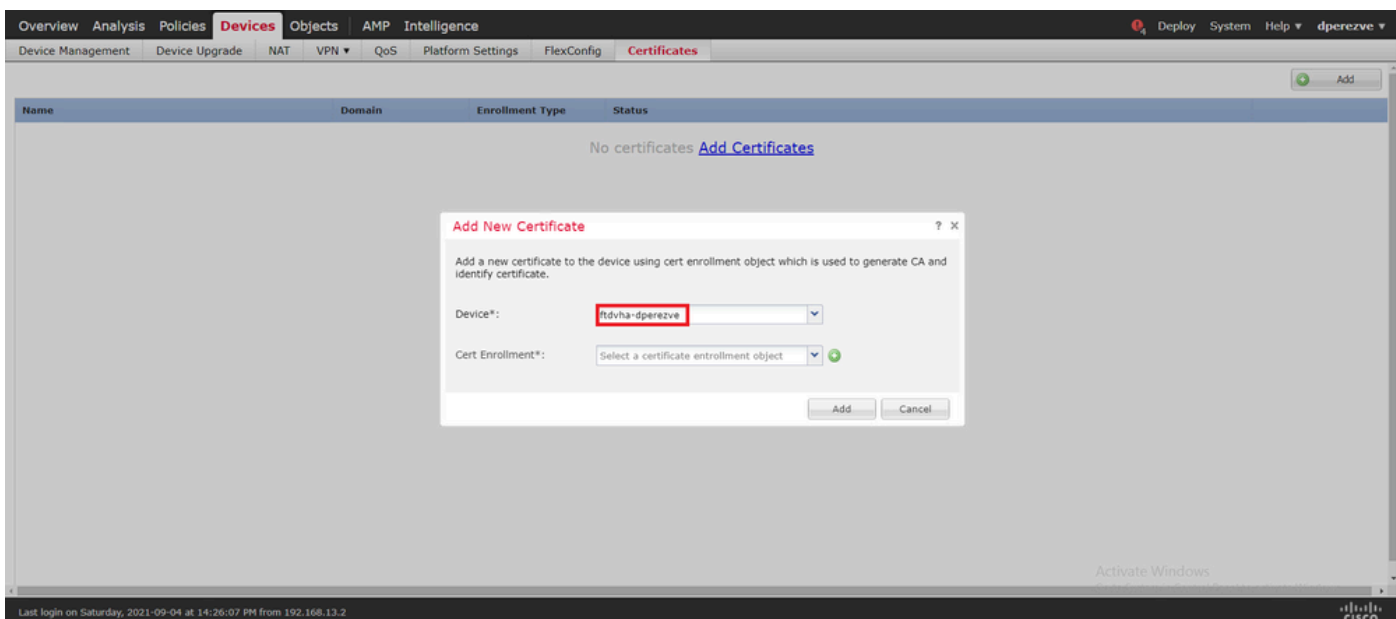
SSL Cisco Secure Client(AnyConnect)では、VPNヘッドエンドとクライアント間のSSLハンドシェイクで使用する有効な証明書が1つ必要です。

 注：この例では、この目的のために自己署名証明書が生成されます。また、自己署名証明書の他に、内部認証局(CA)または既知のCAのいずれかによって署名された証明書をアップロードすることもできます。

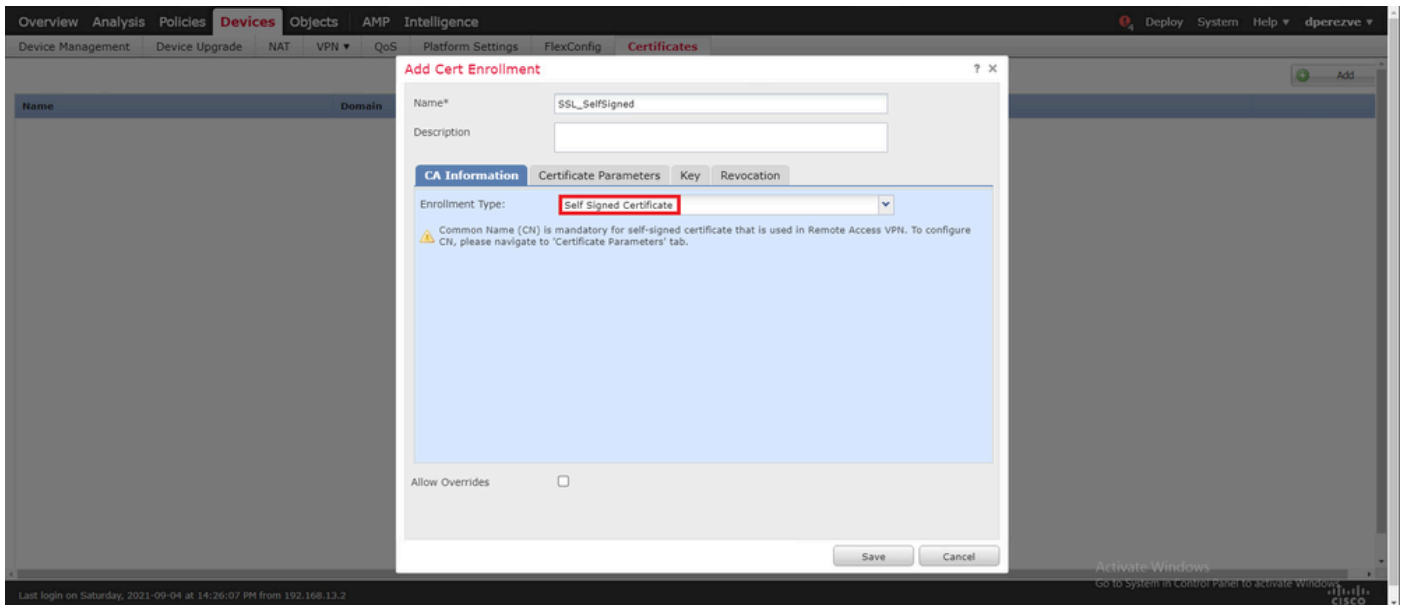
自己署名証明書を作成するには、Devices > Certificatesの順に移動します。



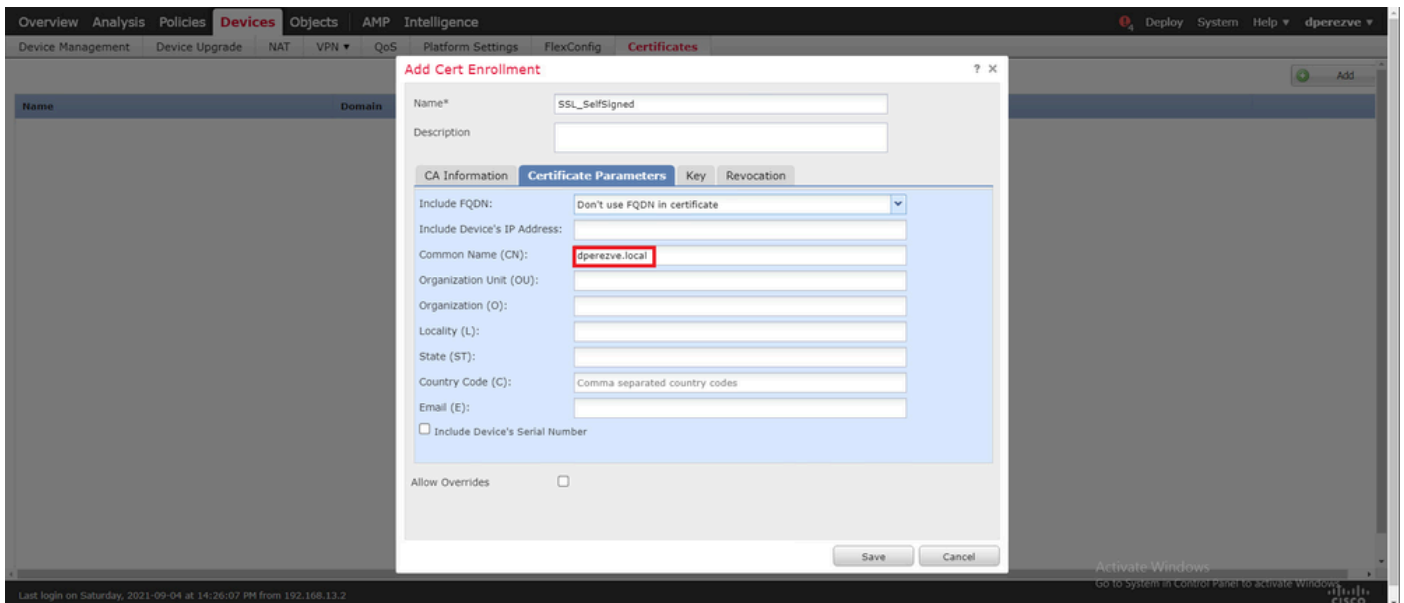
Addボタンを選択します。次に、Add New CertificateウィンドウのDeviceドロップダウンメニューにリストされているFTDを選択します。



Add Cert Enrollmentボタン ( 緑色の+記号 ) を選択して、新しい登録オブジェクトを作成します。ここで、Add Cert Enrollmentウィンドウでオブジェクトの名前を割り当て、Enrollment TypeドロップダウンメニューからSelf Signed Certificateを選択します。



最後に、自己署名証明書の場合は、共通名(CN)が必要です。Certificate Parametersタブに移動して、CNを定義します。

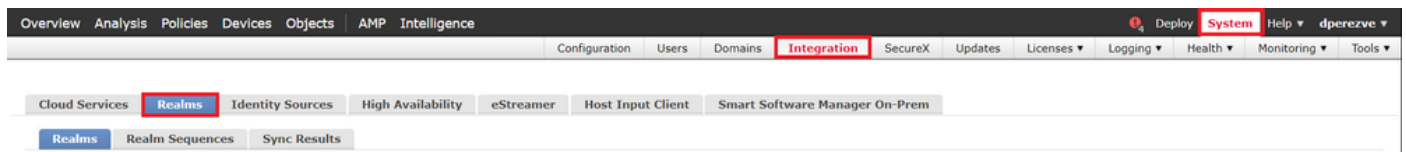


SaveボタンとAddボタンをクリックします。数秒後、新しい証明書を証明書リストに追加する必要があります。

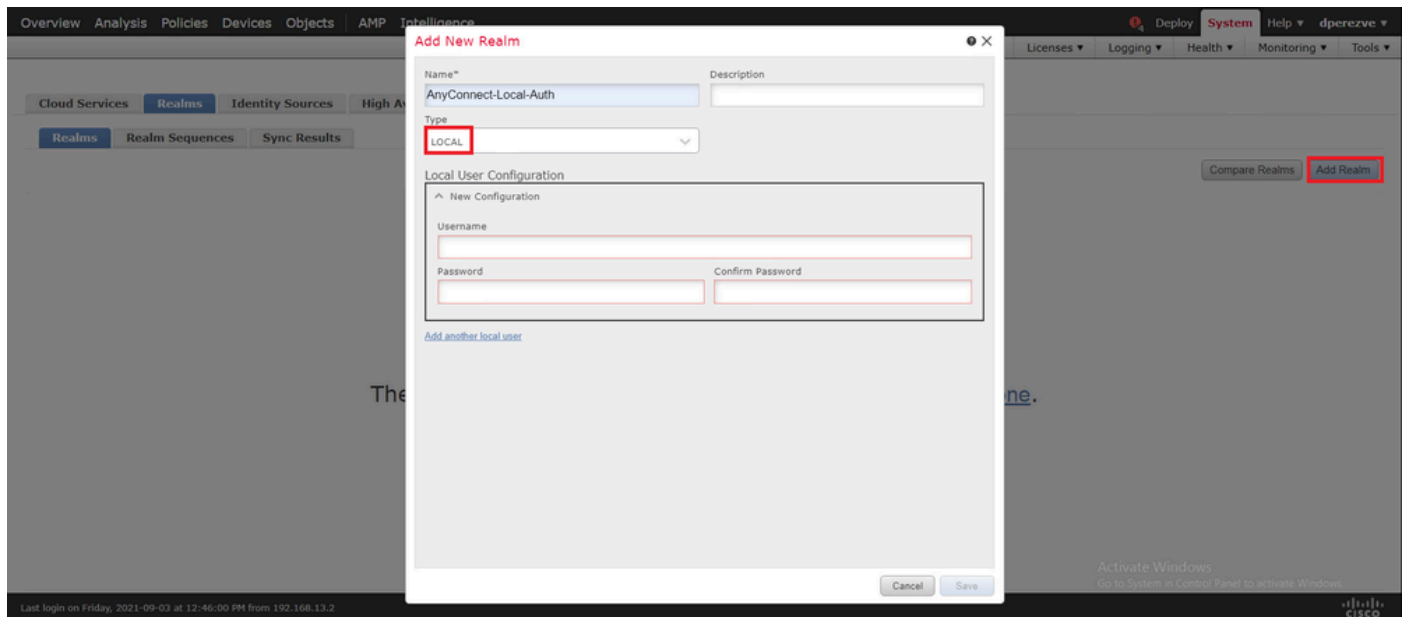


ステップ 4 : FMCでのローカルレルムの作成


ローカルユーザデータベース及び各パスワードは、ローカルレルムに格納される。ローカルレルムを作成するには、System > Integration > Realmsの順に移動します。

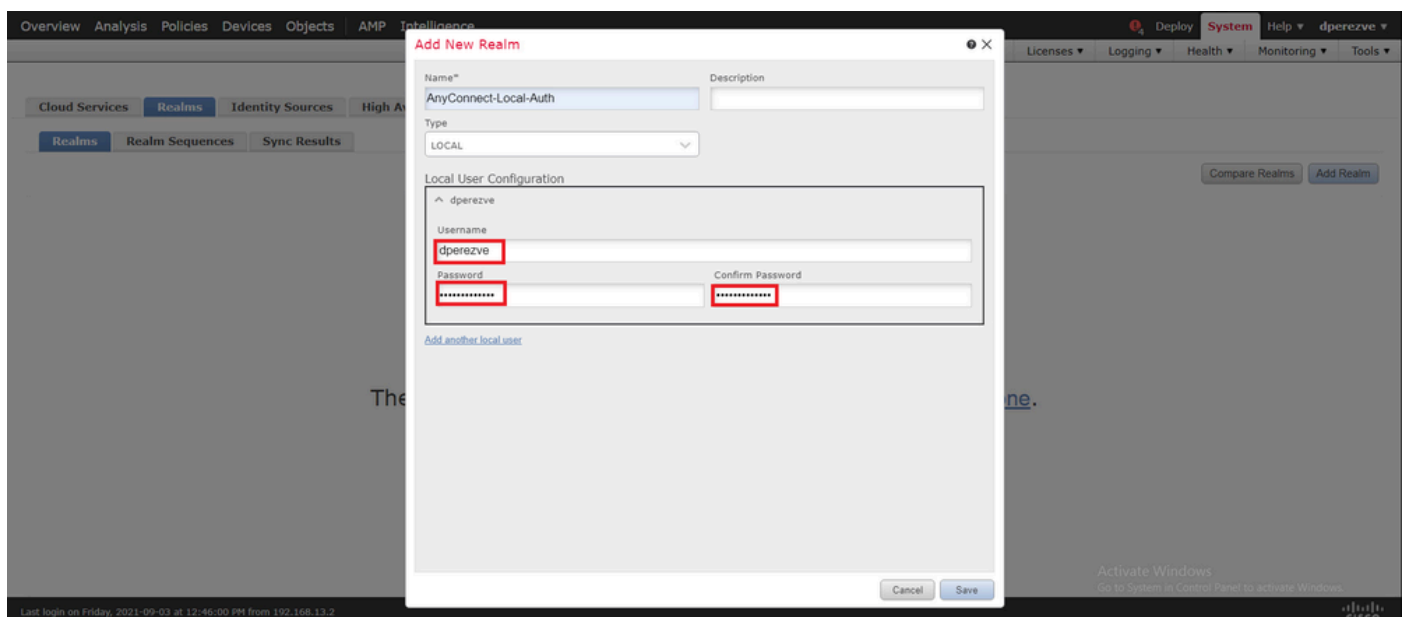


Add Realmボタンを選択します。Add New Realmウィンドウで、名前を割り当て、TypeドロップダウンメニューからLOCALオプションを選択します。

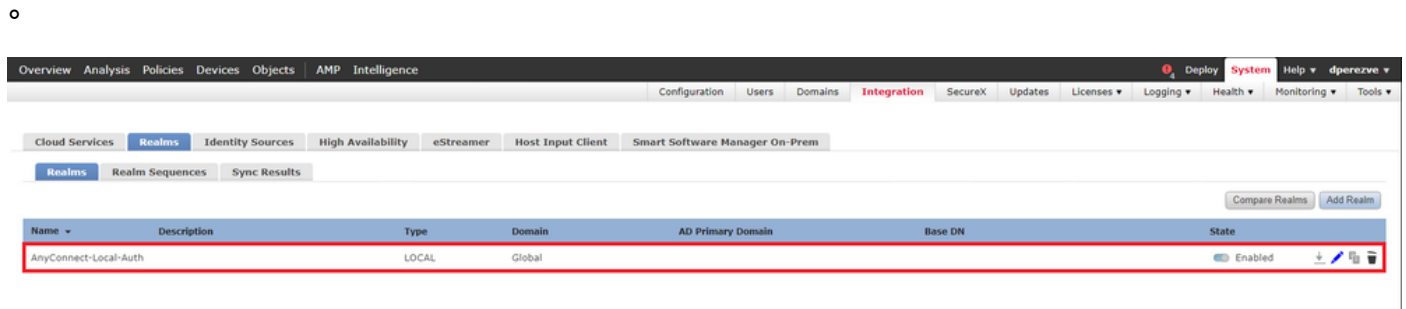


ユーザアカウントとパスワードは、Local User Configurationセクションで作成します。

 注：パスワードには、大文字、小文字、数字、特殊文字が少なくとも1つ含まれている必要があります。

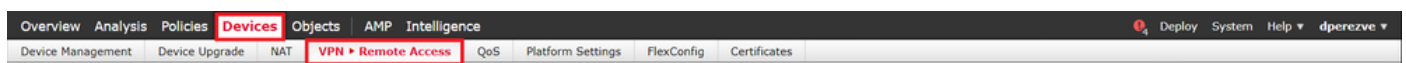


変更を保存し、Add Realmをクリックして、既存のレルムのリストに新しいレルムを追加します

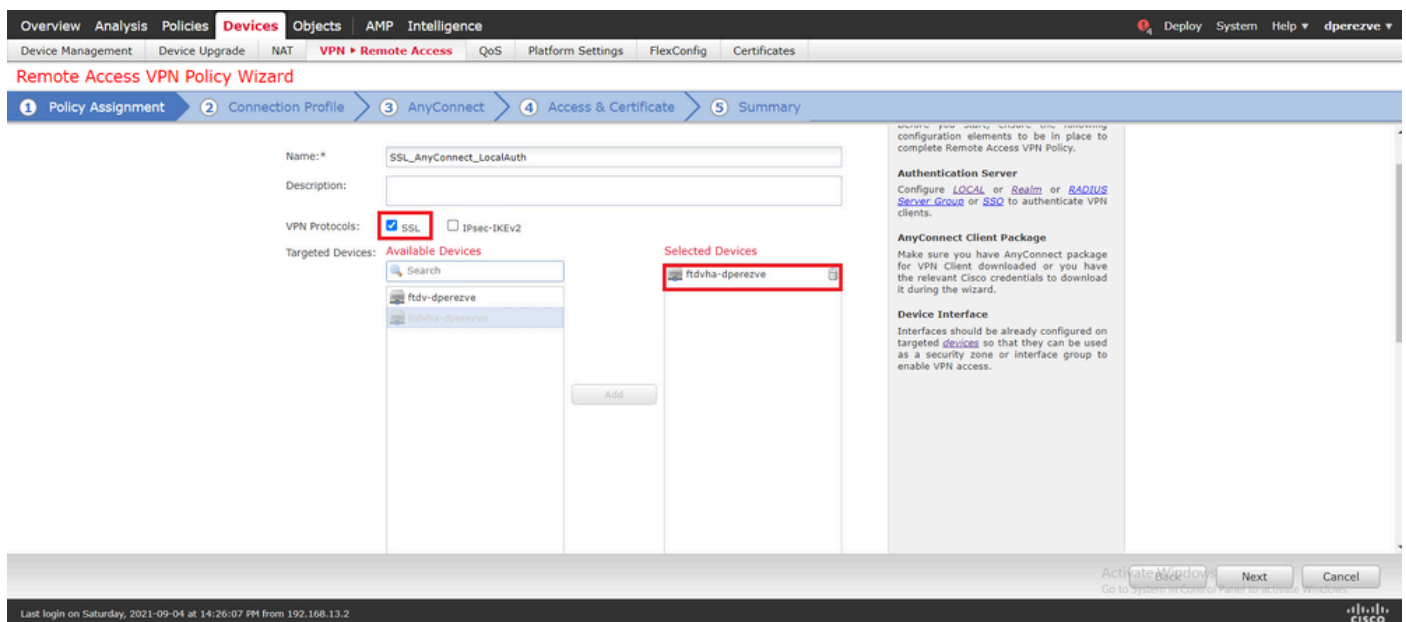


## ステップ 5 : SSL Cisco Secure Clientの設定

SSL Cisco Secure Clientを設定するには、Devices > VPN > Remote Accessの順に移動します。

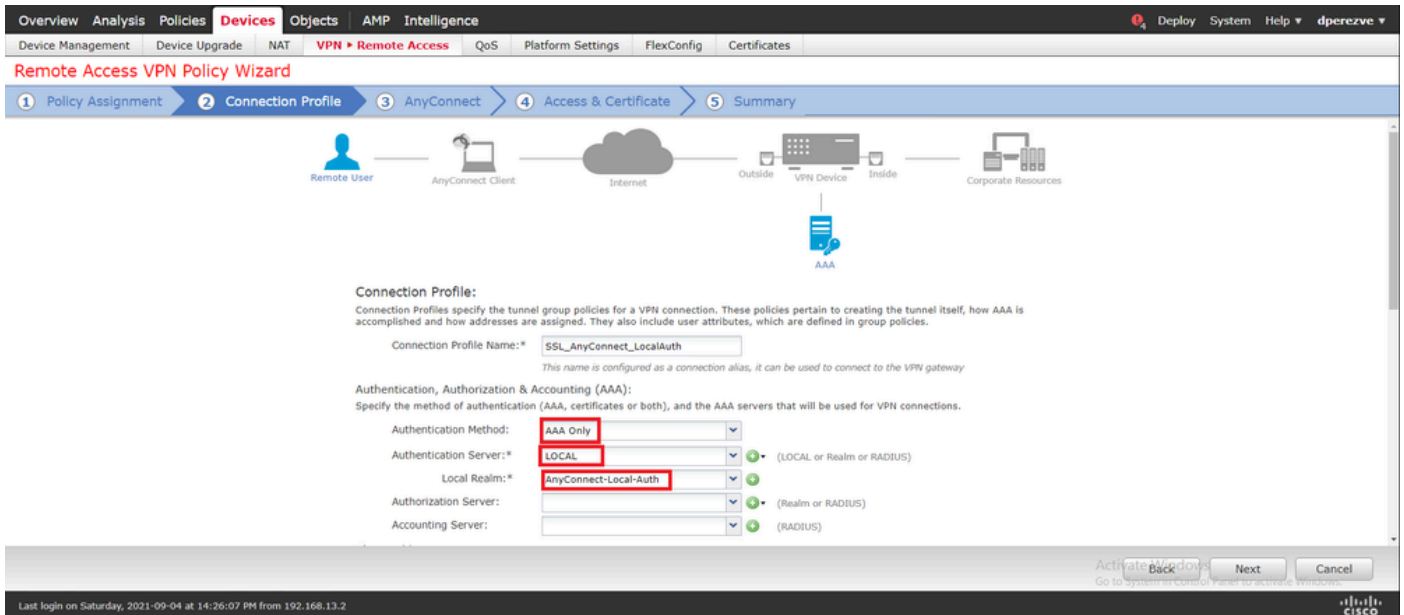


Addボタンをクリックして、新しいVPNポリシーを作成します。接続プロファイルの名前を定義し、「SSL」チェックボックスを選択して、ターゲット・デバイスとしてリストされているFTDを選択します。すべてがリモートアクセスVPNポリシーウィザードのポリシー割り当てセクションで設定されている必要があります。

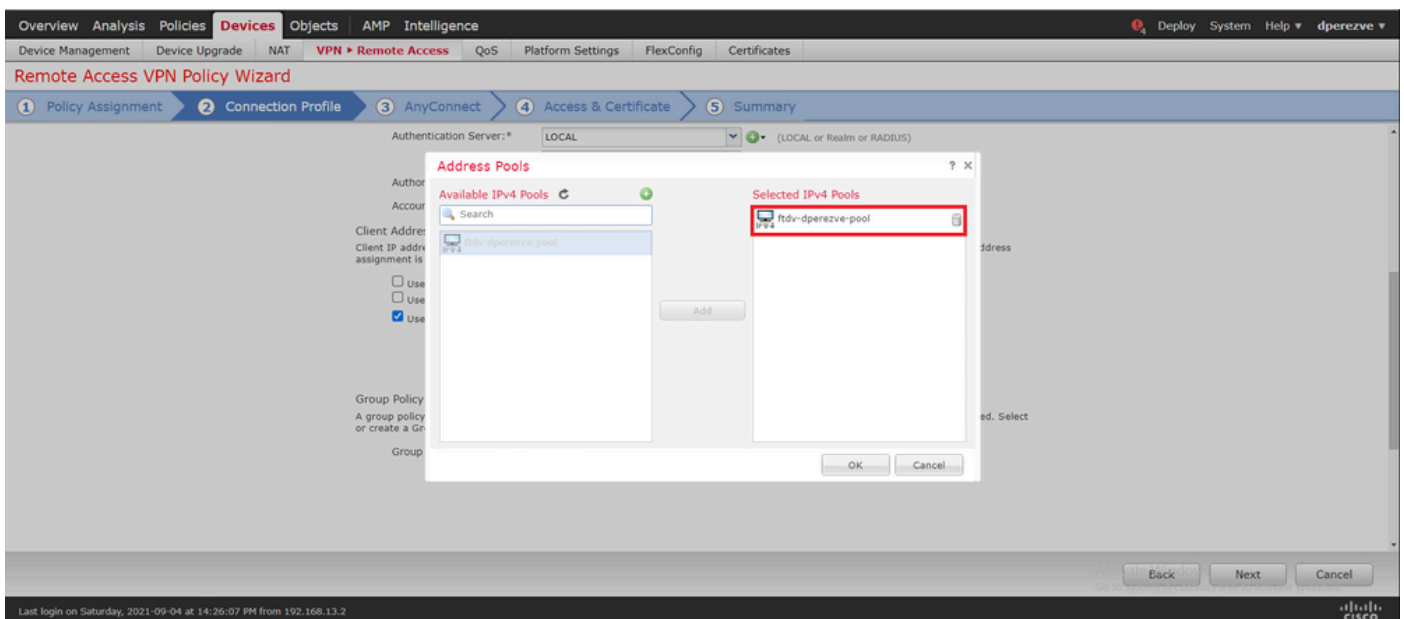


Nextを選択して、Connection Profile設定に移動します。接続プロファイルの名前を定義し、認証方式としてAAA Onlyを選択します。次に、Authentication ServerドロップダウンメニューでLOCALを選択し、最後にLocal Realmドロップダウンメニューでステップ4で作成したローカルレルムを選択します。

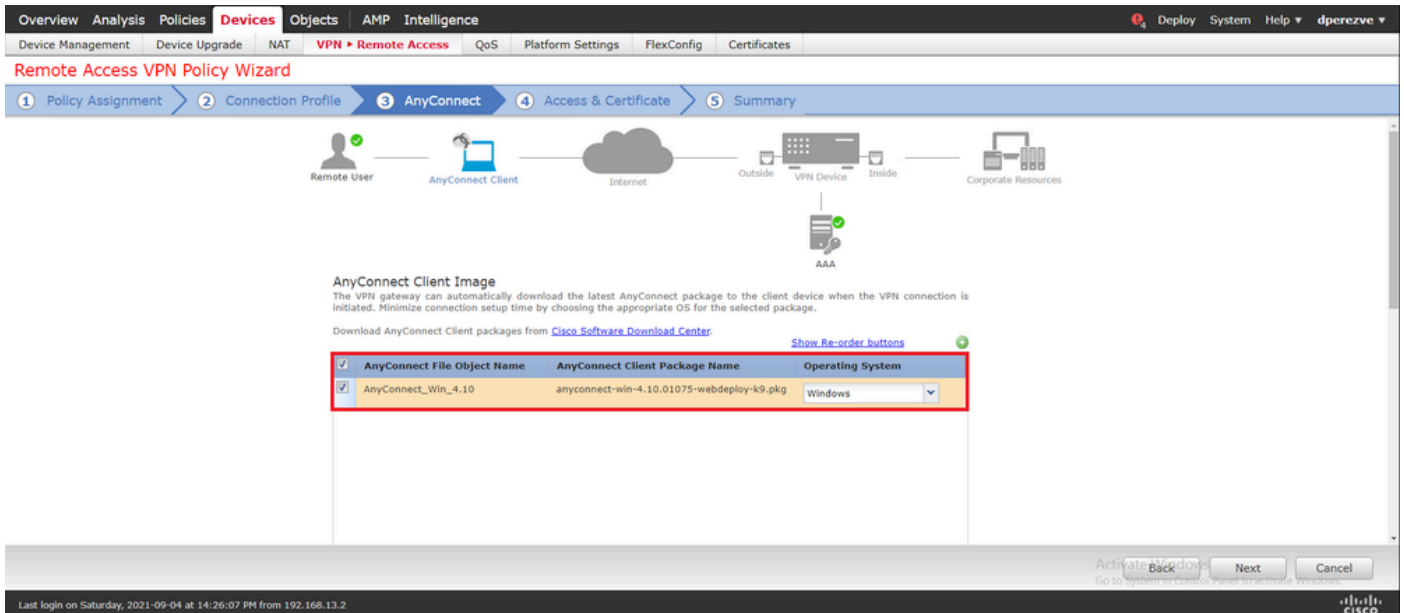




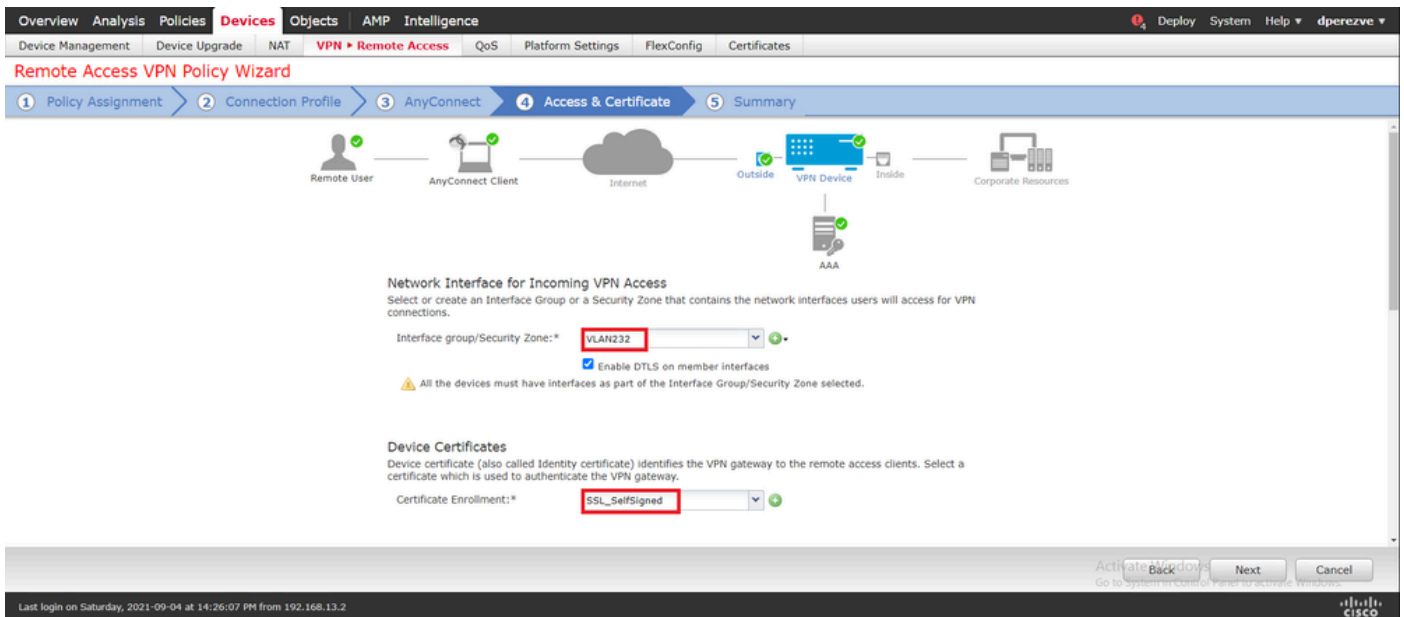
同じページを下にスクロールし、IPv4 Address Poolセクションにある鉛筆アイコンをクリックして、Cisco Secure Clientが使用するIPプールを定義します。



Nextをクリックして、AnyConnectセクションに移動します。ここで、ステップ2でアップロードしたCisco Secure Clientイメージを選択します。



Nextをクリックして、Access & Certificateセクションに移動します。Interface group/Security Zoneドロップダウンメニューで、Cisco Secure Client(AnyConnect)を有効にする必要があるインターフェイスを選択します。次に、Certificate Enrollmentドロップダウンメニューで、手順3で作成した証明書を選択します。



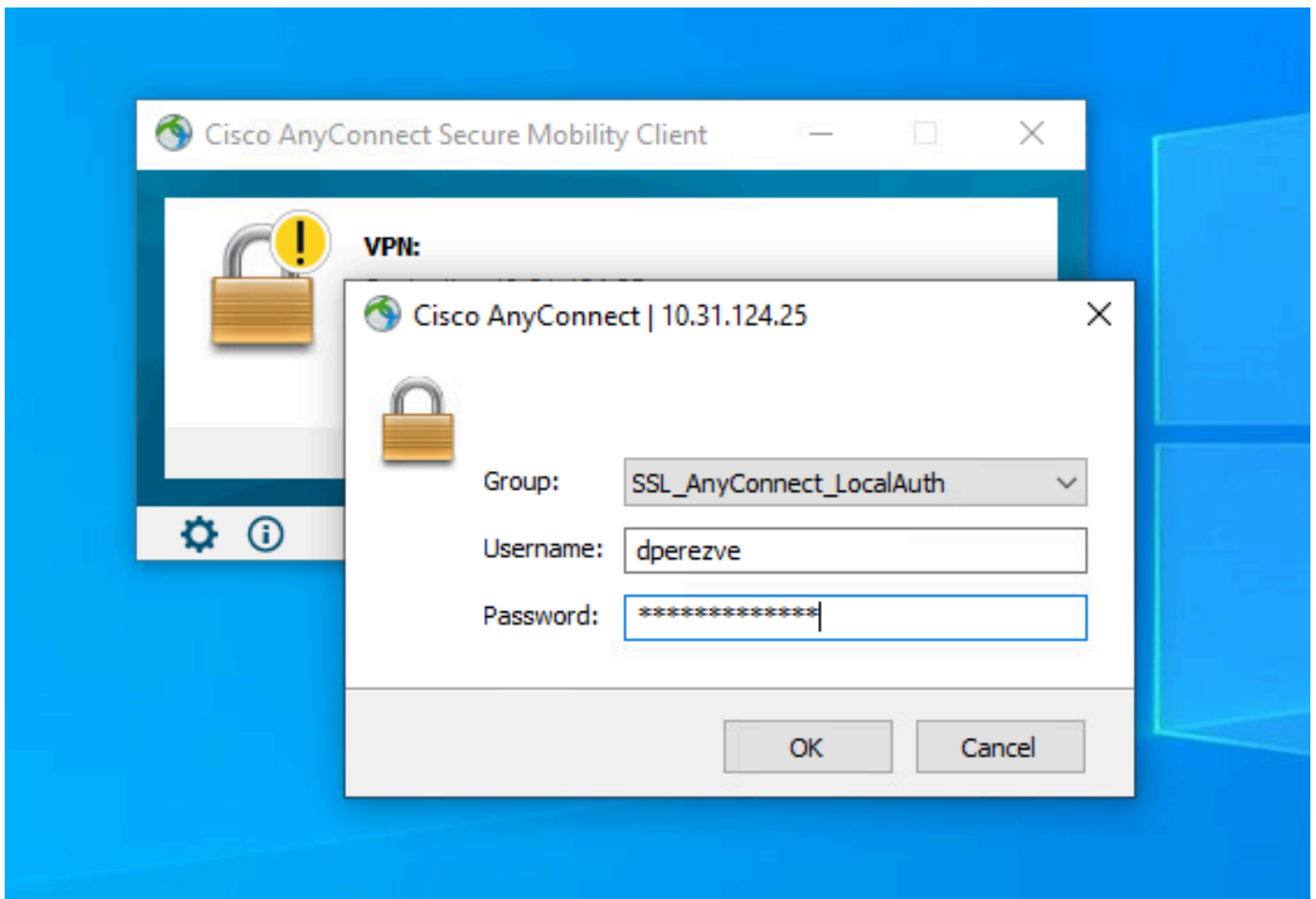
最後に、Nextをクリックして、Cisco Secure Clientの設定の要約を表示します。

すべての設定が正しければ、Finishをクリックして変更をFTDに展開します。

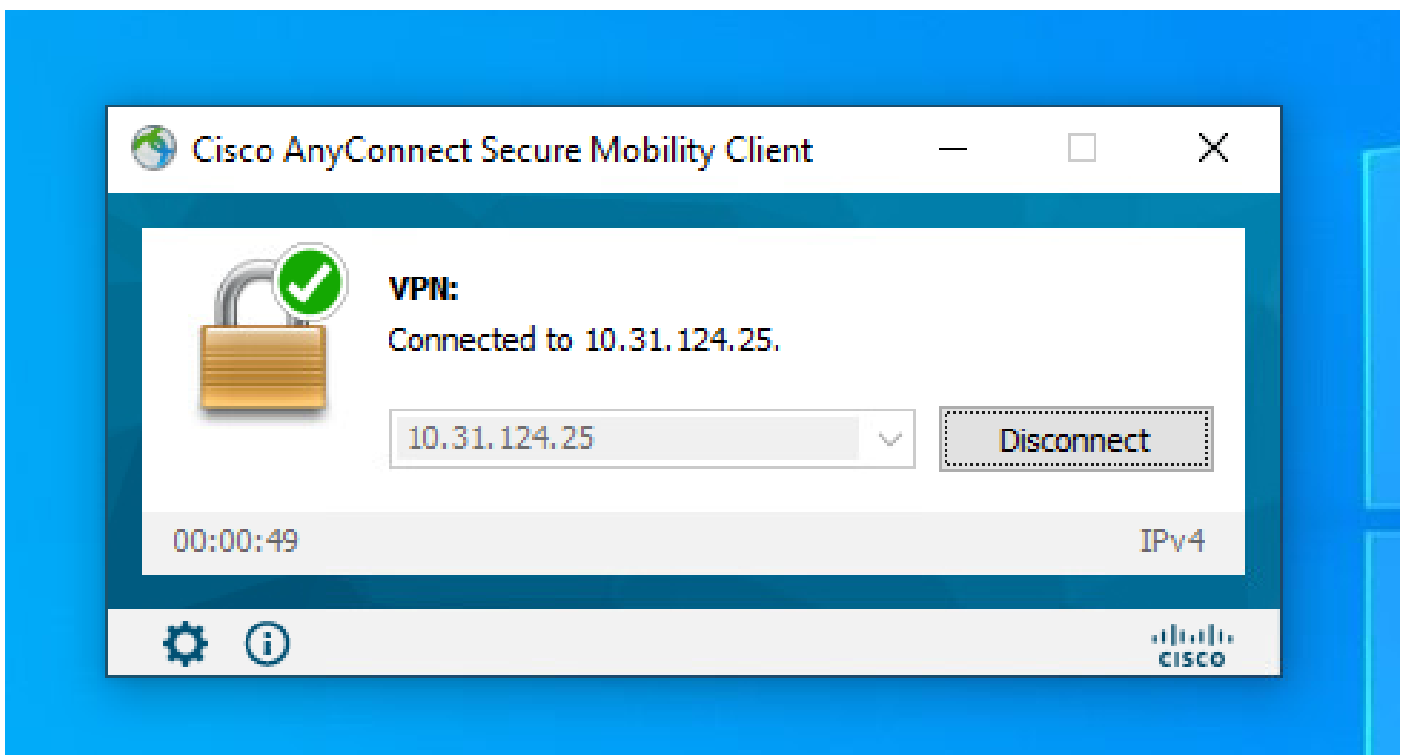
Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dpereze	dpereze		FTD		Sep 7, 2021 2:44 PM		Pending

## 確認

導入が成功したら、WindowsクライアントからFTDへのCisco AnyConnectセキュアモバイルクライアント接続を開始します。認証プロンプトで使用するユーザ名とパスワードは、ステップ4で作成したものと同一である必要があります。



クレデンシャルがFTDによって承認されると、Cisco AnyConnectセキュアモビリティクライアントアプリケーションは接続状態を表示する必要があります。



FTDから、`show vpn-sessiondb anyconnect`コマンドを実行して、ファイアウォールで現在アクテ

IPv4なCisco Secure Clientセッションを表示できます。

```
firepower# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : dperezve                Index      : 8
Assigned IP   : 172.16.13.1          Public IP  : 10.31.124.34
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 15756                Bytes Rx   : 14606
Group Policy  : DfltGrpPolicy
Tunnel Group  : SSL_AnyConnect_LocalAuth
Login Time    : 21:42:33 UTC Tue Sep 7 2021
Duration      : 0h:00m:30s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN       : none
Audt Sess ID  : 00000000000080006137dcc9
Security Grp  : none                Tunnel Zone : 0
```

## トラブルシュート

FTDでdebug webvpn anyconnect 255コマンドを実行し、FTDのSSL接続フローを確認します。

```
firepower# debug webvpn anyconnect 255
```

Cisco Secure Clientデバッグの他に、TCPパケットキャプチャでも接続フローを確認できます。これは、接続が成功し、WindowsクライアントとFTD間の通常の3つのハンドシェイクが完了した後、暗号の同意に使用されるSSLハンドシェイクが完了した例です。

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of captured packets. A red box highlights the first four packets, which are the initial steps of an SSL/TLS handshake:

- 13: 3.331822 10.31.124.34 → 10.31.124.25 TCP 66 51300 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1
- 14: 3.332733 10.31.124.25 → 10.31.124.34 TCP 60 443 → 51300 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
- 16: 3.335655 10.31.124.34 → 10.31.124.25 TLSv1.2 247 Client Hello
- 17: 3.341963 10.31.124.25 → 10.31.124.34 TCP 60 443 → 51300 [ACK] Seq=1 Ack=194 Win=32768 Len=0

The bottom pane shows the packet details for the selected packets, including the TLSv1.2 Client Hello and Server Hello messages. The status bar at the bottom indicates that the capture was performed on interface 'Dwice100P'.

プロトコルのハンドシェイク後、FTDはローカルレルムに保存された情報を使用してクレデンシャルを検証する必要があります。

DARTバンドルを収集し、さらに調査するためにCisco TACに連絡します。

## 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。