FTDのローカル認証を使用したSSLセキュアクライアントの設定

内容

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上でローカル認証を使用して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 Secure Client(SVC)の設定
- FMCによるFirepowerオブジェクトの設定
- firepower上の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。

- CiscoFirepower脅威対策(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クライアントの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として定義することも、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することもできます。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が稼働する前は、FTD上のCisco Secure Clientローカル認証はCiscoFirepowerデバイスマネージャ(FDM)でのみ使用できました。

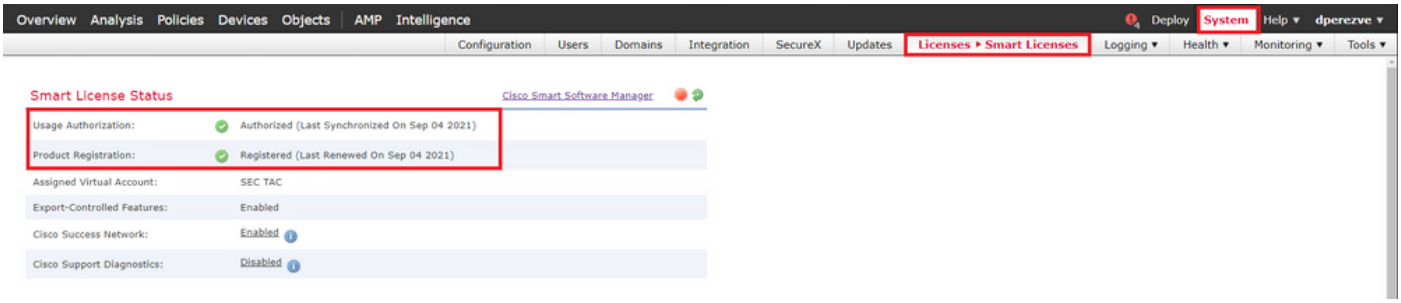
設定

コンフィギュレーション

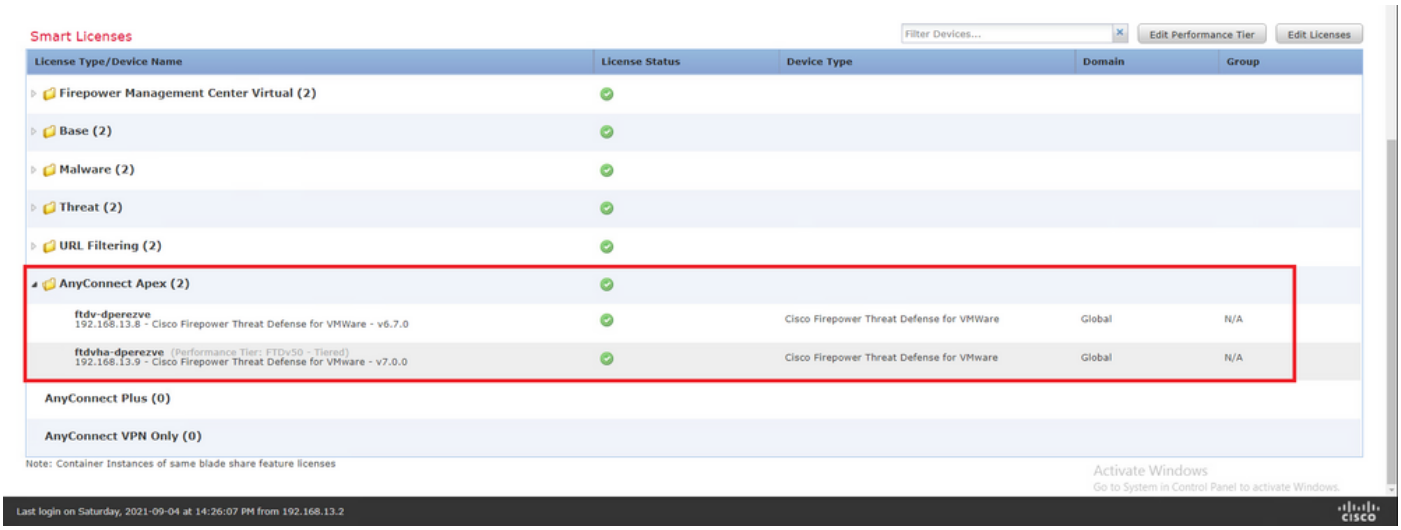
ステップ 1：ライセンスの確認

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。

FMCがスマートライセンスポータルに登録され、準拠していることを確認するには、System > Licenses > Smart Licensesの順に移動します。



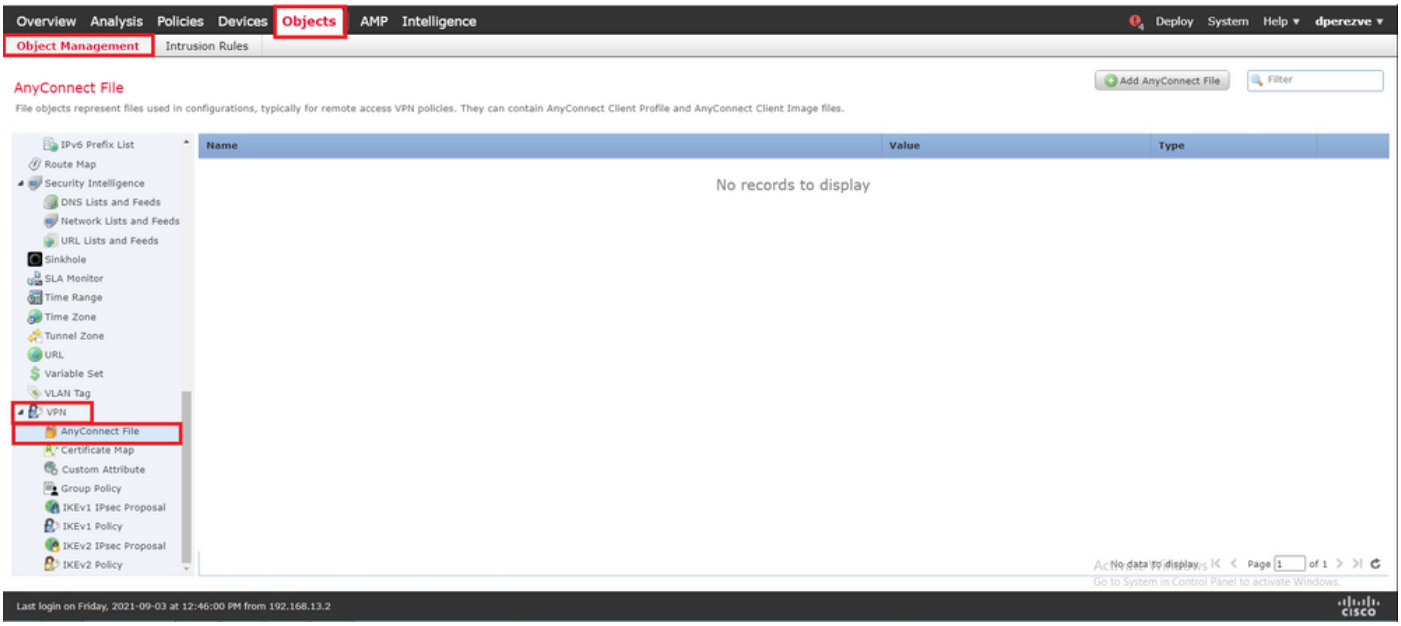
同じページで下にスクロールすると、スマートライセンスチャートの下部に、使用可能なCisco Secure Client(AnyConnect)ライセンスのタイプと、各ライセンスにサブスクライブされているデバイスが表示されます。手元のFTDが次のいずれかのカテゴリで登録されていることを確認します。



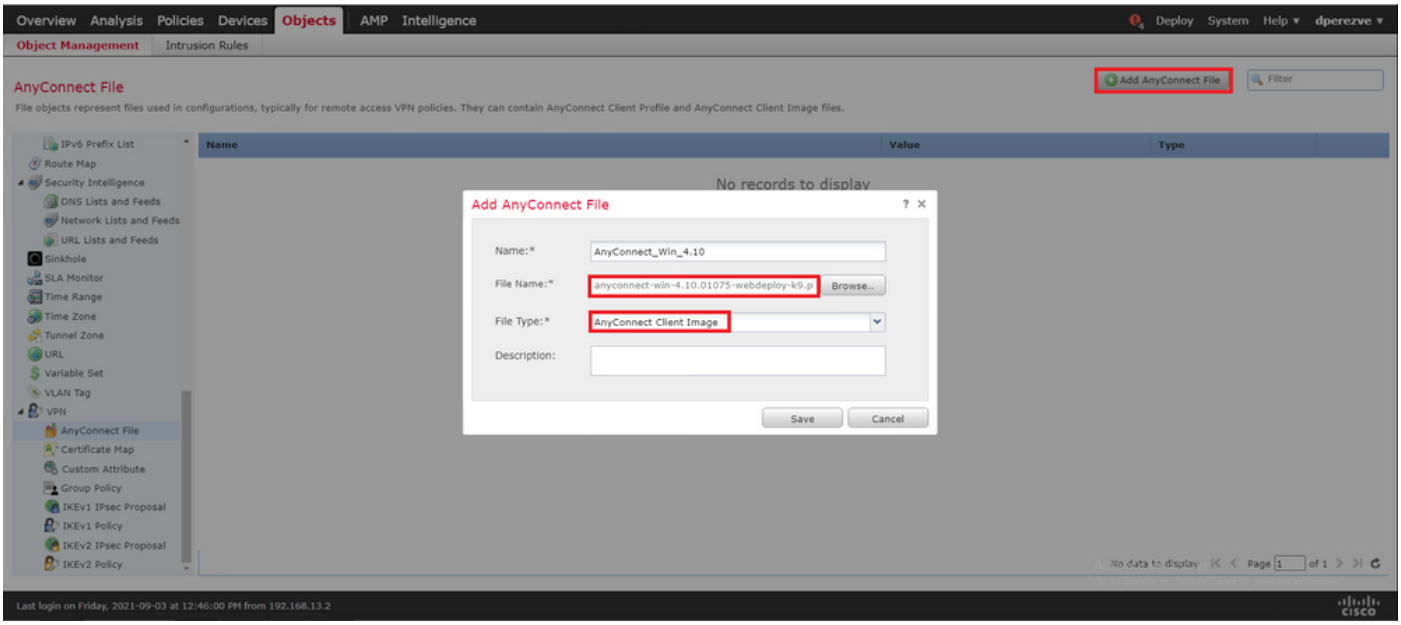
ステップ 2：FMCへのCisco Secure Clientパッケージのアップロード

cisco.comからWindows向けCisco Secure Client(AnyConnect)ヘッドエンド導入パッケージをダウンロードします。

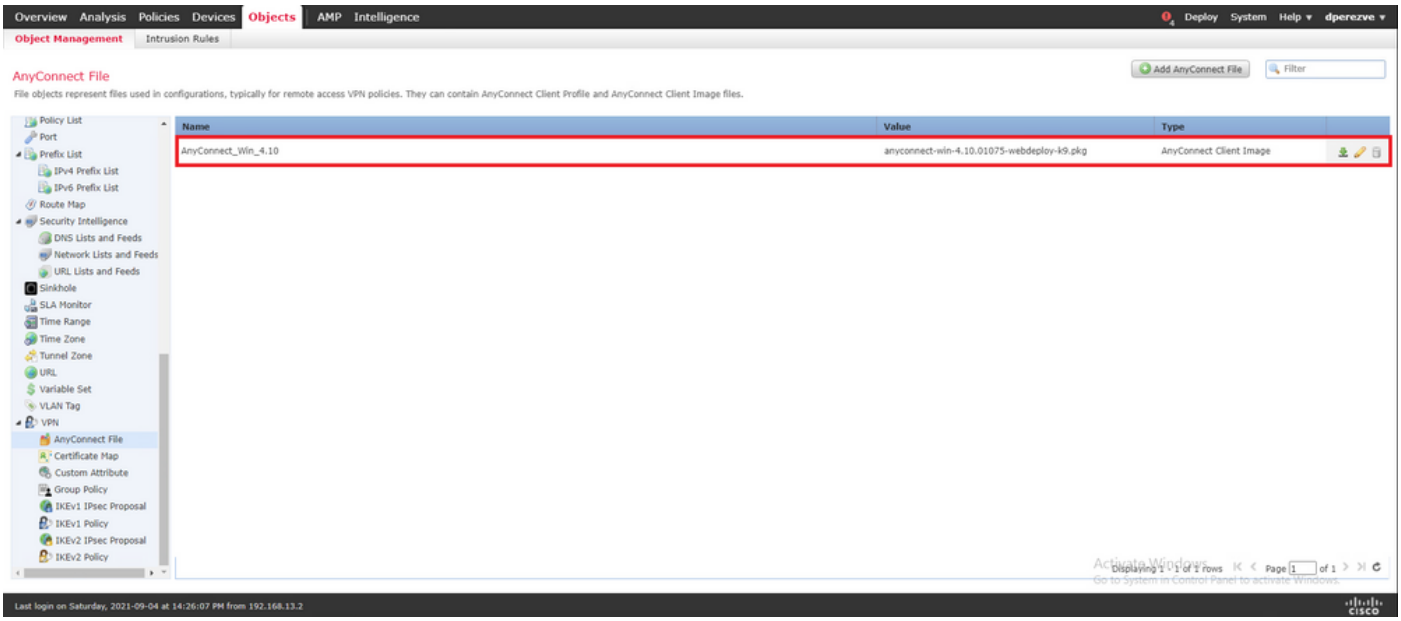
Cisco Secure Clientイメージをアップロードするには、Objects > Object Managementの順に移動し、目次でVPNカテゴリの下にあるCisco Secure Client Fileを選択します。



Add AnyConnect Fileボタンを選択します。Add AnyConnect Secure Client Fileウィンドウで、オブジェクトの名前を割り当て、Browse...を選択してCisco Secure Clientパッケージを選択し、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。



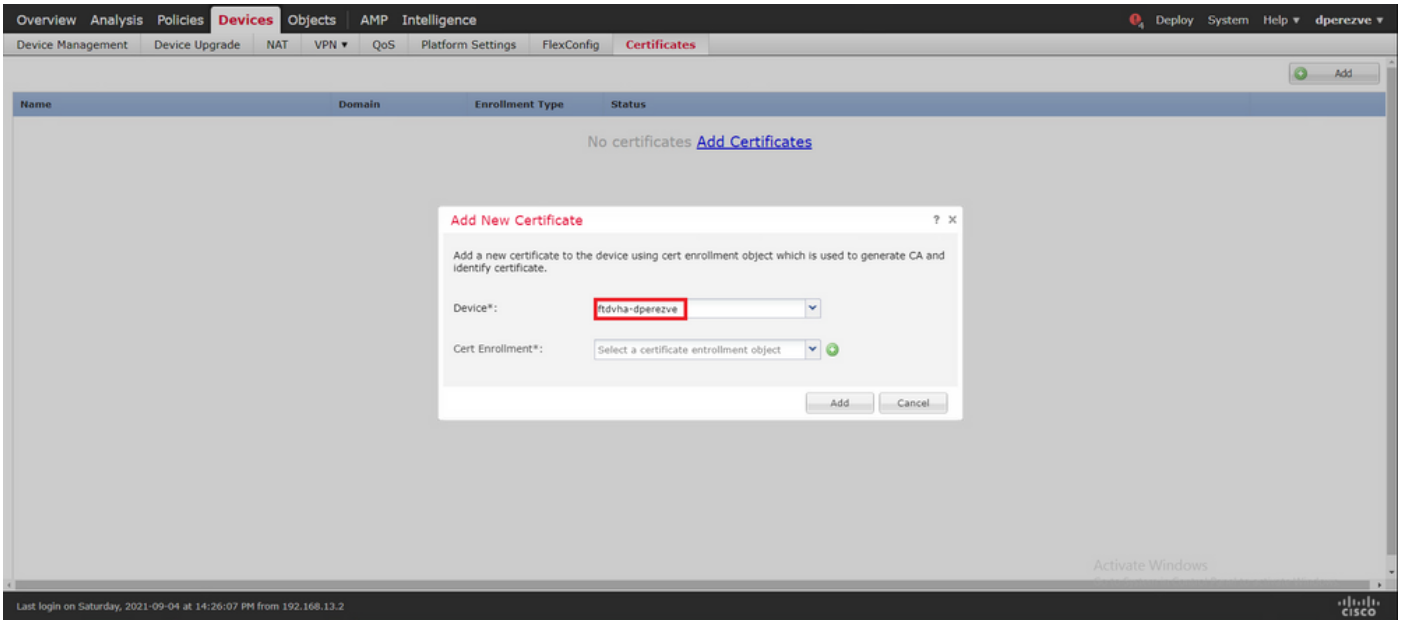
ステップ 3：自己署名証明書の生成

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。

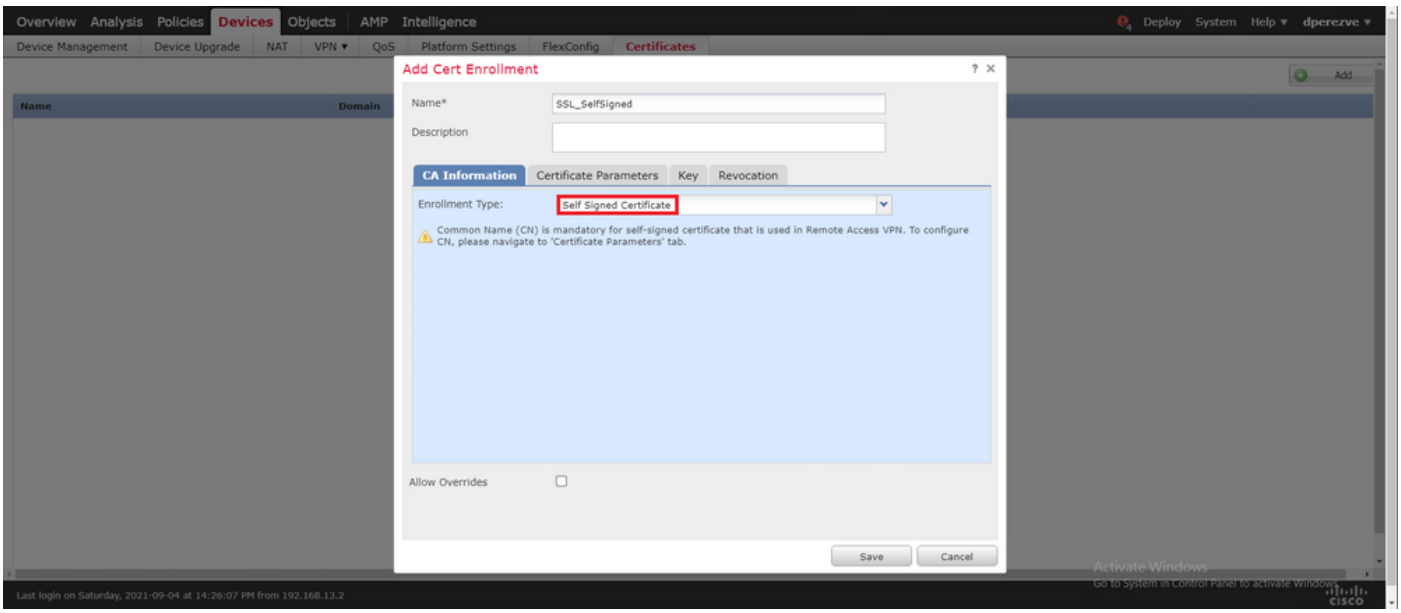
注：この例では、この目的のために自己署名証明書が生成されます。ただし、自己署名証明書に加えて、内部認証局(CA)または既知のCAのいずれかによって署名された証明書をアップロードすることもできます。

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

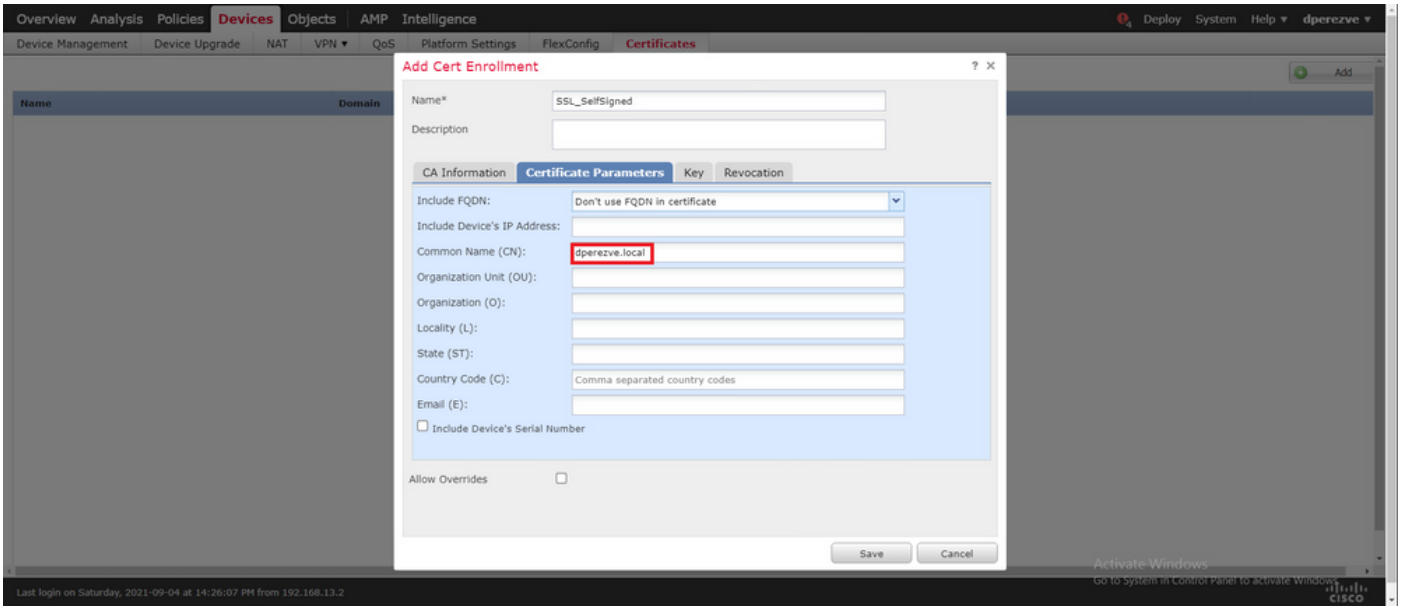
Addボタンを選択します。次に、Add New CertificateウィンドウのDeviceドロップダウンメニューから手元のFTDを選択します。



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、オブジェクトに名前を割り当て、Enrollment Typeドロップダウンメニューから Self Signed Certificateを選択します。



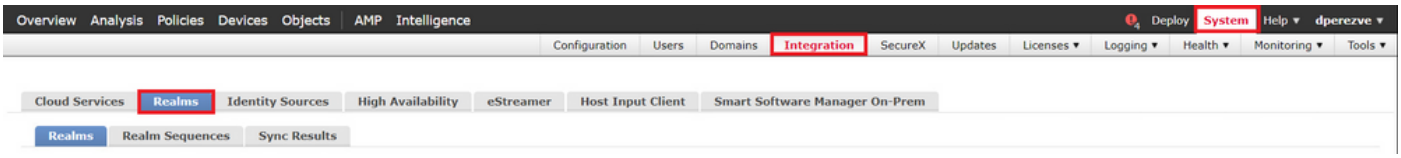
最後に、自己署名証明書の場合は、共通名(CN)が必要です。CNを定義するには、Certificate Parametersタブに移動します。



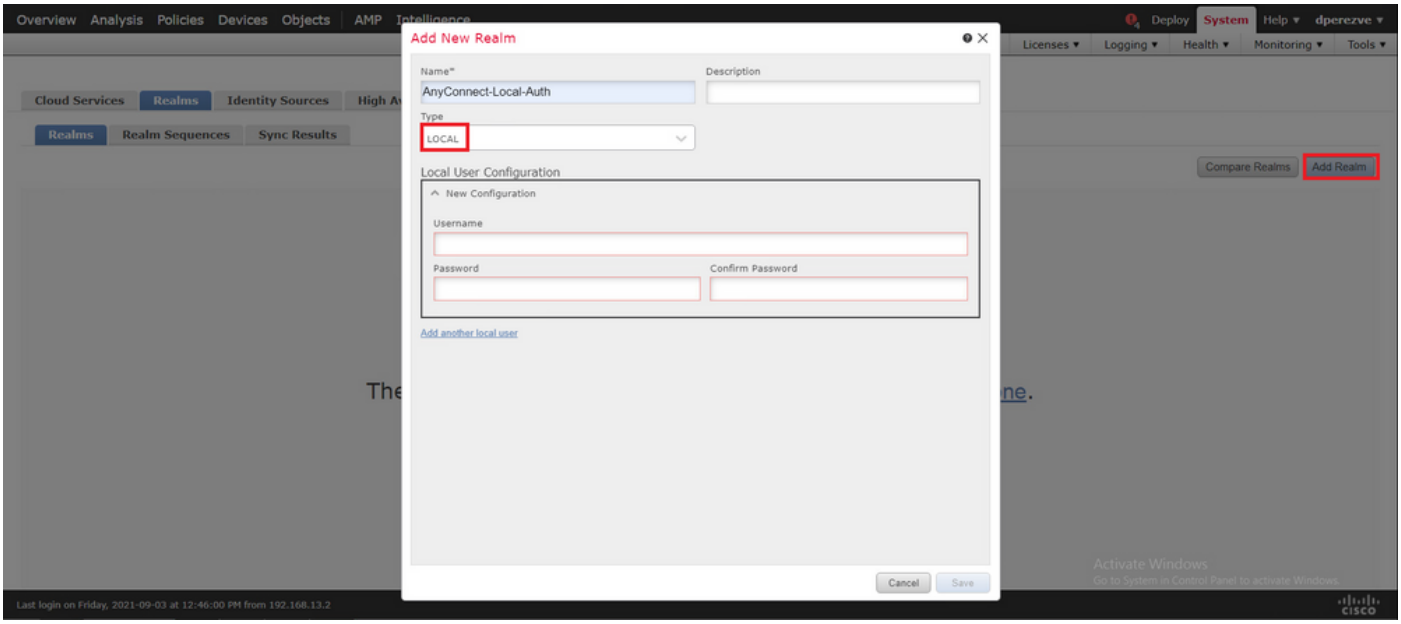
SaveボタンとAddボタンを選択します。数秒後に、新しい証明書を証明書リストに追加する必要があります。

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、ローカル領域に格納される。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。

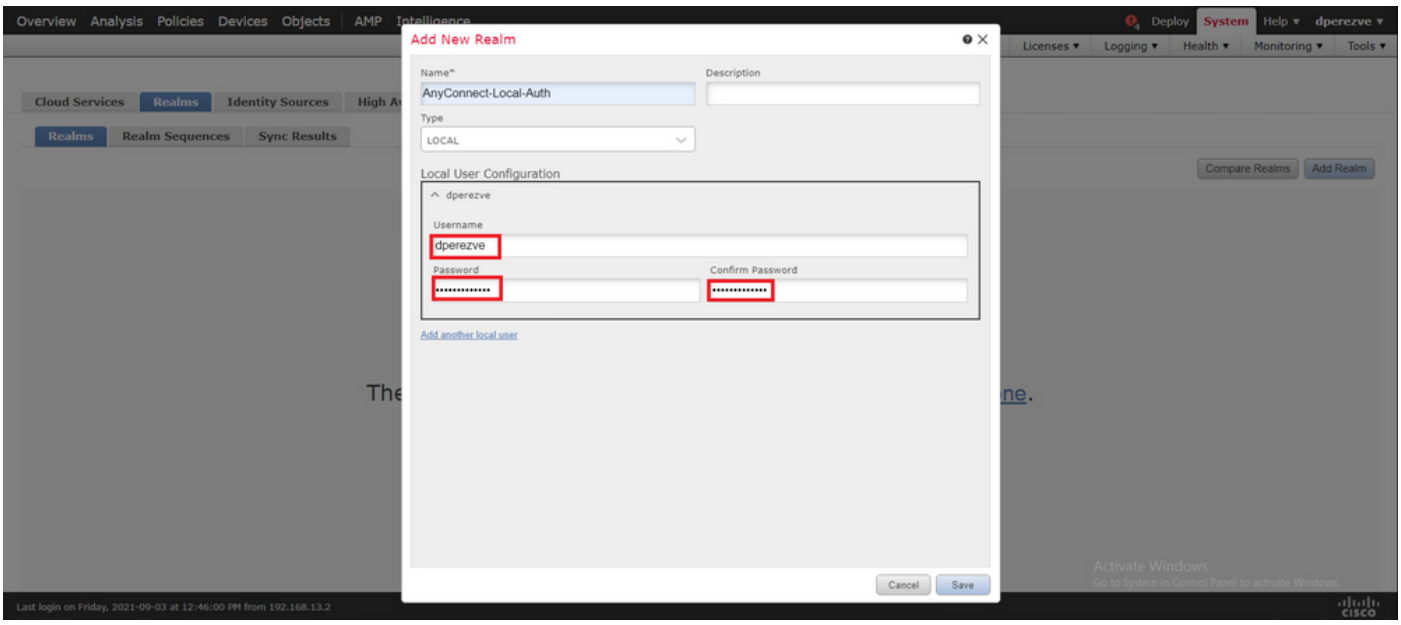


Add Realmボタンを選択します。Add New Realmウィンドウで、名前を割り当て、Typeドロップダウンメニューから**LOCAL**オプションを選択します。

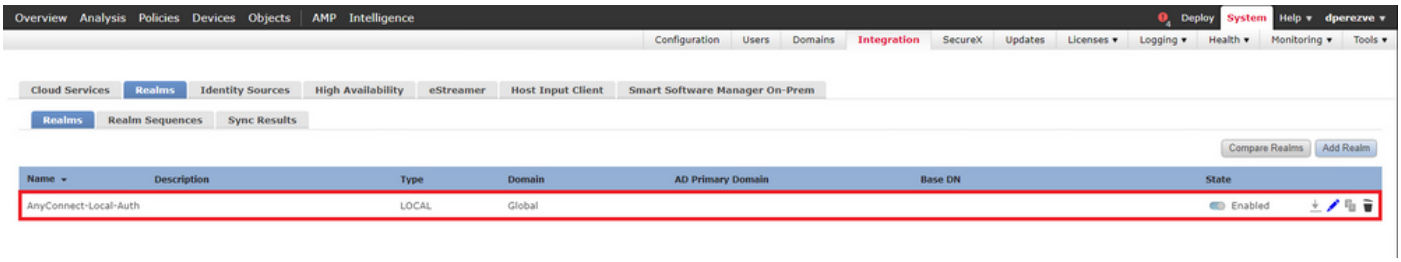


ユーザアカウントとパスワードは、Local User Configurationセクションで作成します。

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。

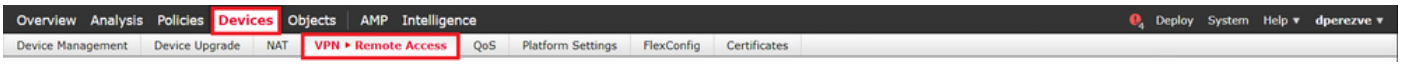


変更を保存し、新しいレルムを既存のレルムのリストに追加する必要があります。

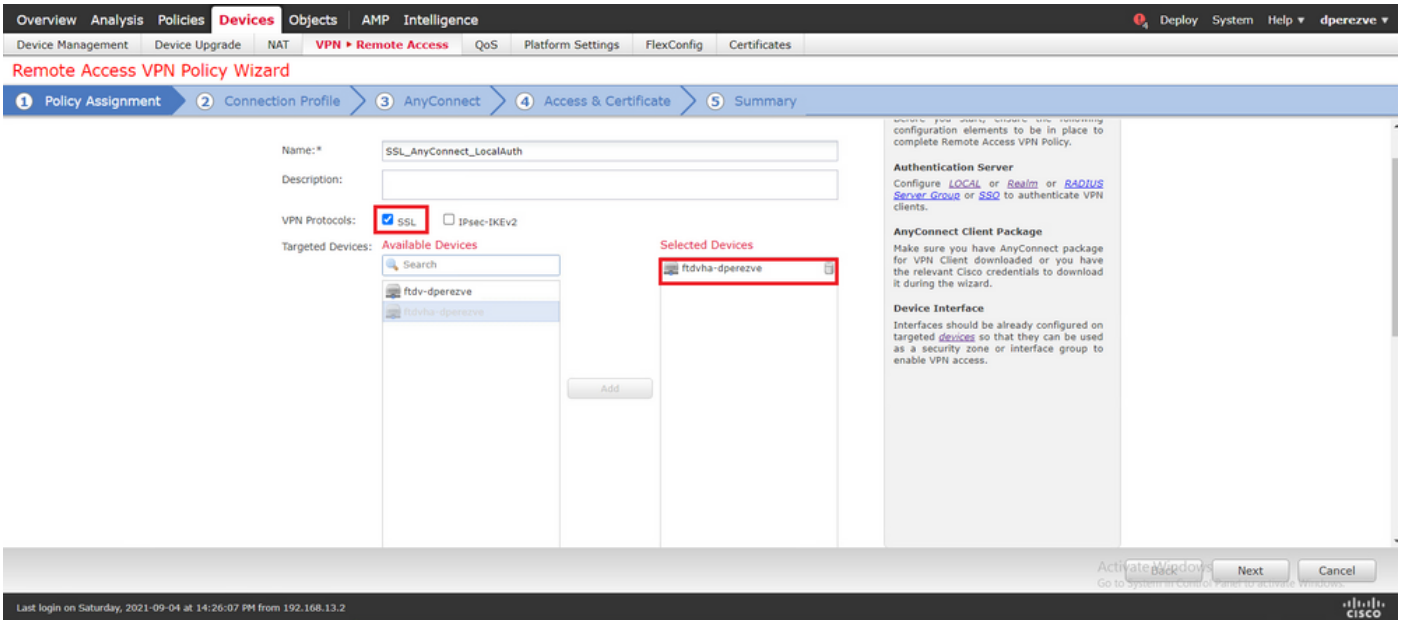


ステップ 5：SSL Cisco Secure Clientの設定

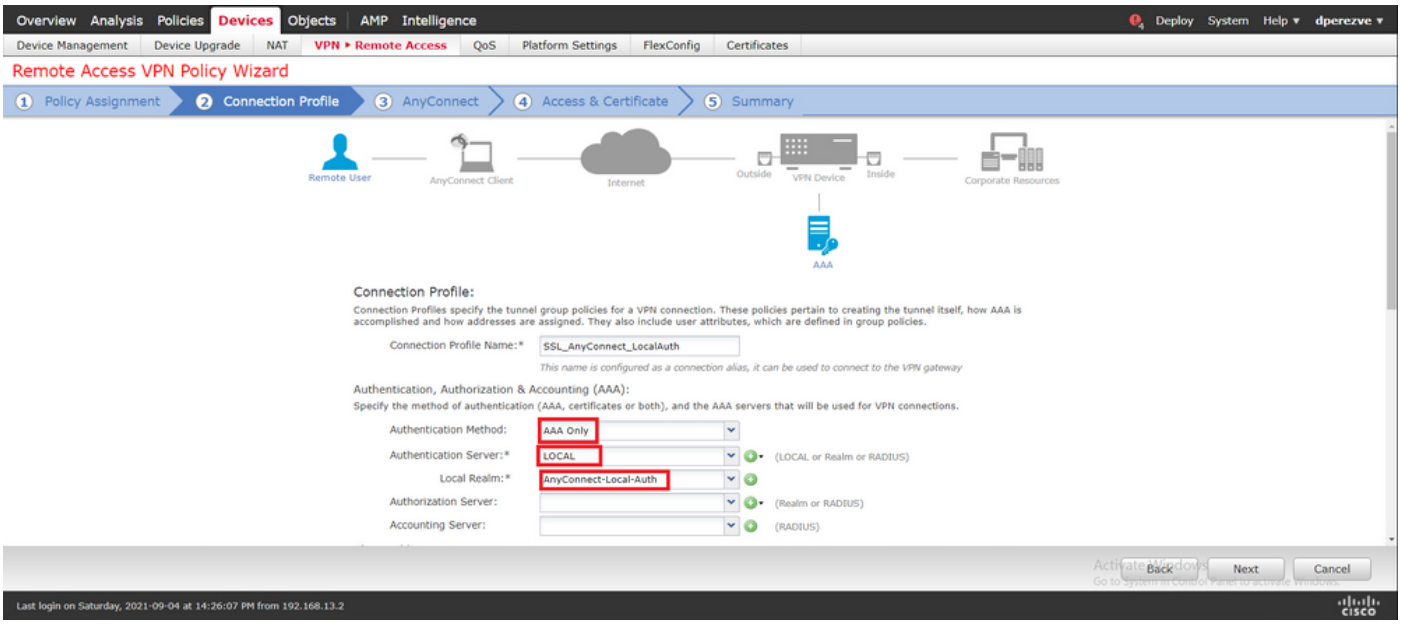
SSL Cisco Secure Clientを設定するには、Devices > VPN > Remote Accessの順に移動します。



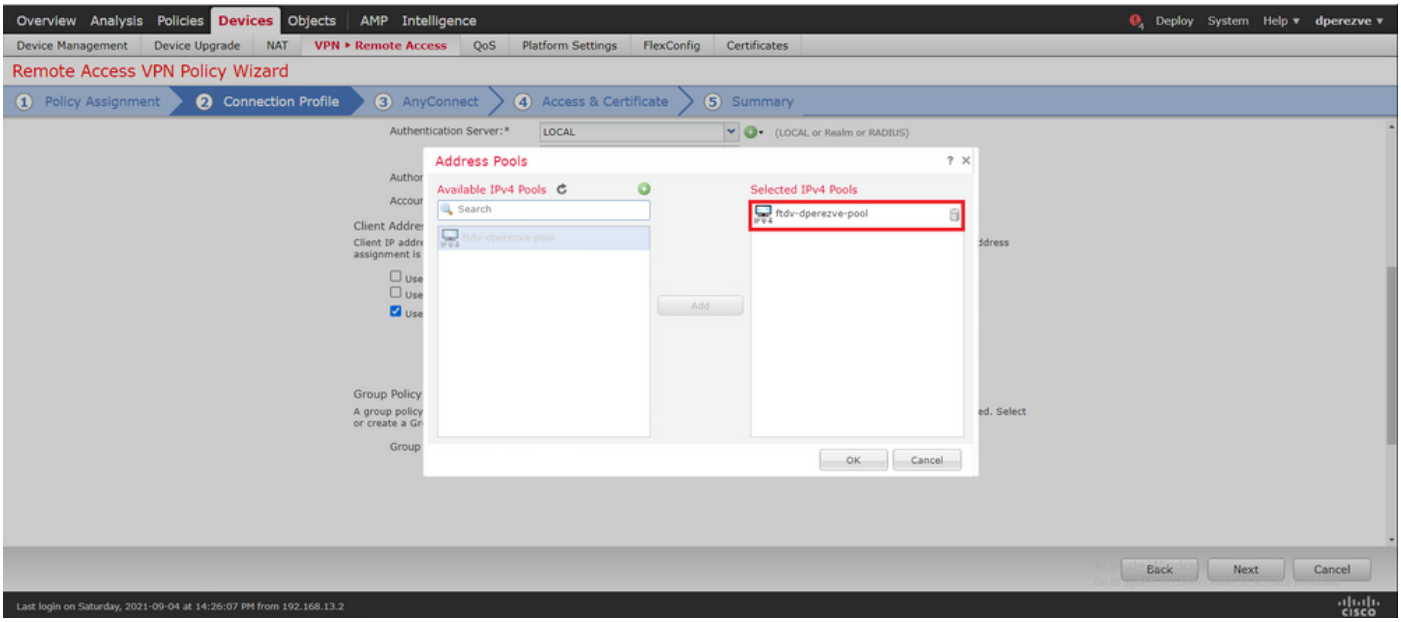
Addボタンを選択して、新しいVPNポリシーを作成します。接続プロファイルの名前を定義し、SSLチェックボックスを選択して、ターゲットデバイスとして手元のFTDを選択します。すべての設定は、リモートアクセスVPNポリシーウィザードのポリシー割り当てセクションで行う必要があります。



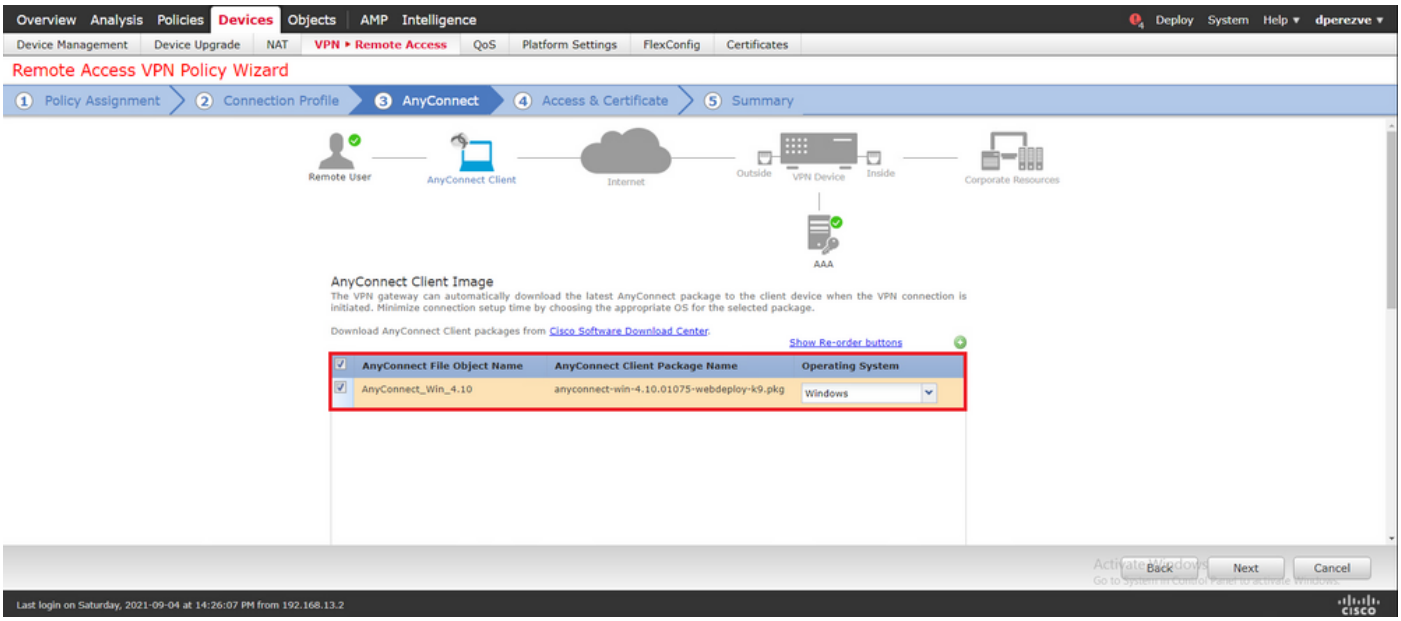
Nextを選択して、Connection Profile設定に移動します。接続プロファイルの名前を定義し、認証方式としてAAA Onlyを選択します。次に、Authentication Serverドロップダウンメニューから LOCALを選択し、最後にLocal Realmドロップダウンメニューからステップ4で作成したローカルレルムを選択します。



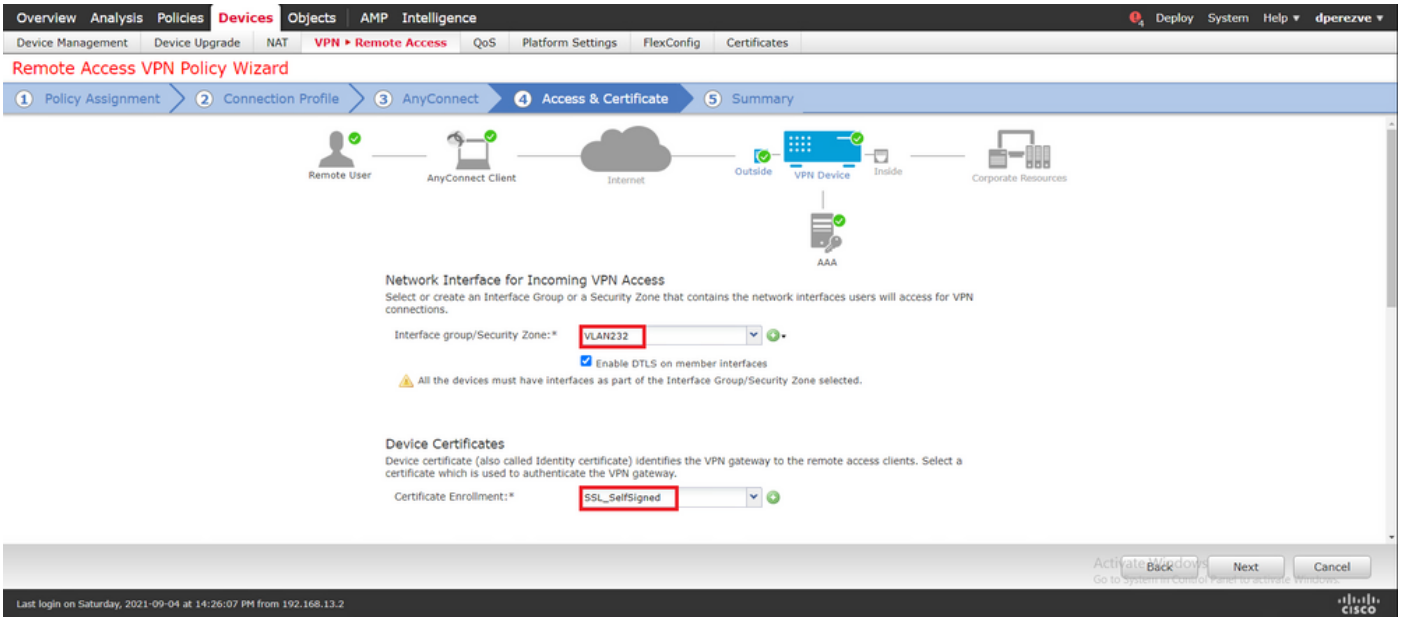
同じページでスクロールダウンして、IPv4 Address Poolセクションの鉛筆アイコンを選択し、Cisco Secure Clientで使用されるIPプールを定義します。



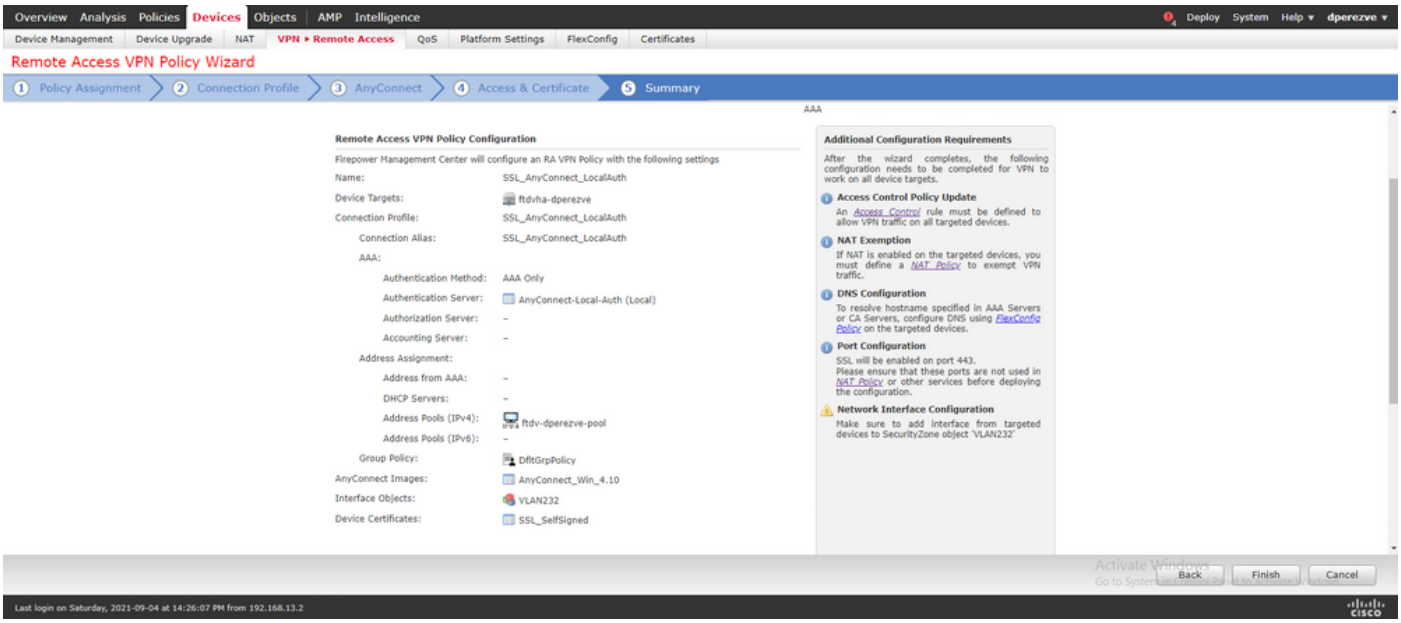
Nextを選択して、AnyConnectセクションに移動します。次に、ステップ2でアップロードしたCisco Secure Clientイメージを選択します。



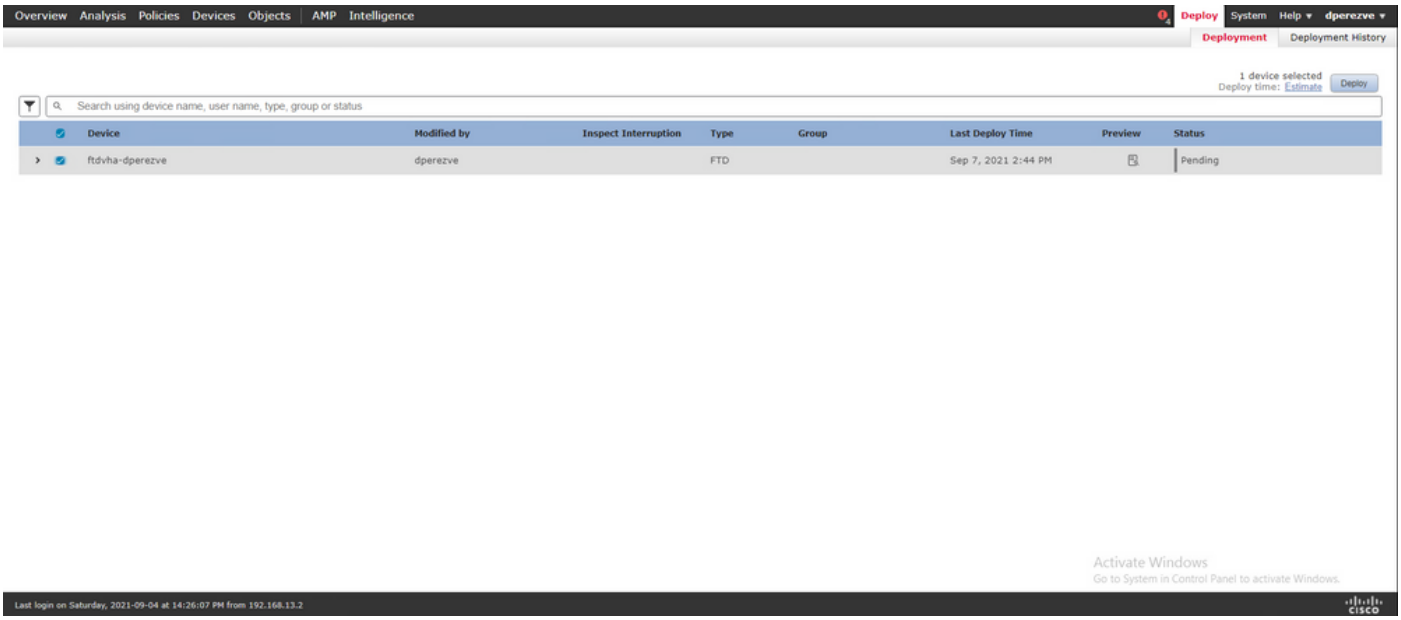
Nextを選択して、Access & Certificateセクションに移動します。Interface group/Security Zoneドロップダウンメニューで、Cisco Secure Client(AnyConnect)を有効にする必要があるインターフェイスを選択します。次に、Certificate Enrollmentドロップダウンメニューで、ステップ3で作成した証明書を選択します。



最後に、Nextを選択して、Cisco Secure Clientの設定の概要を表示します。

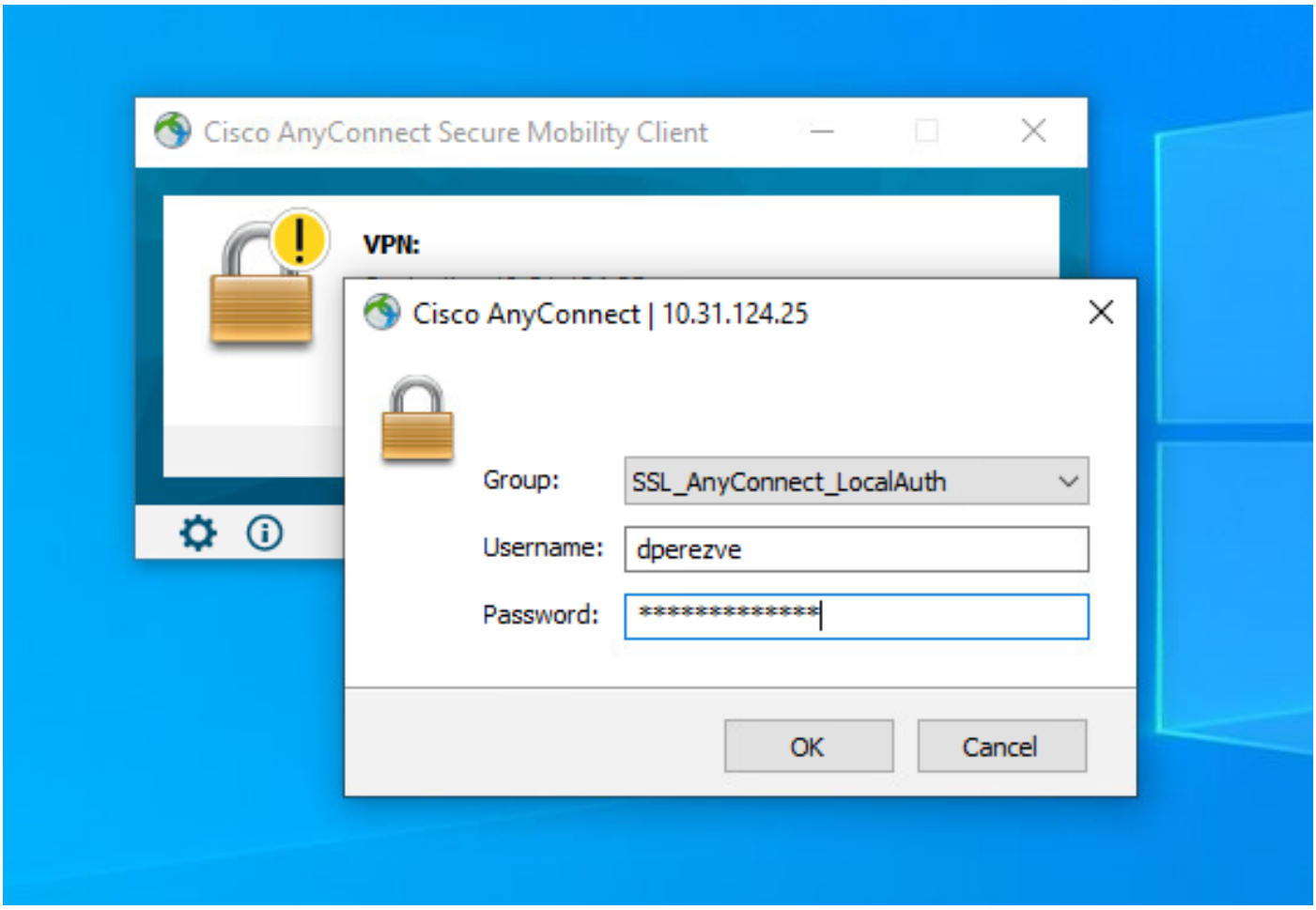


すべての設定が正しい場合は、Finishを選択して、FTDに対する変更を展開します。

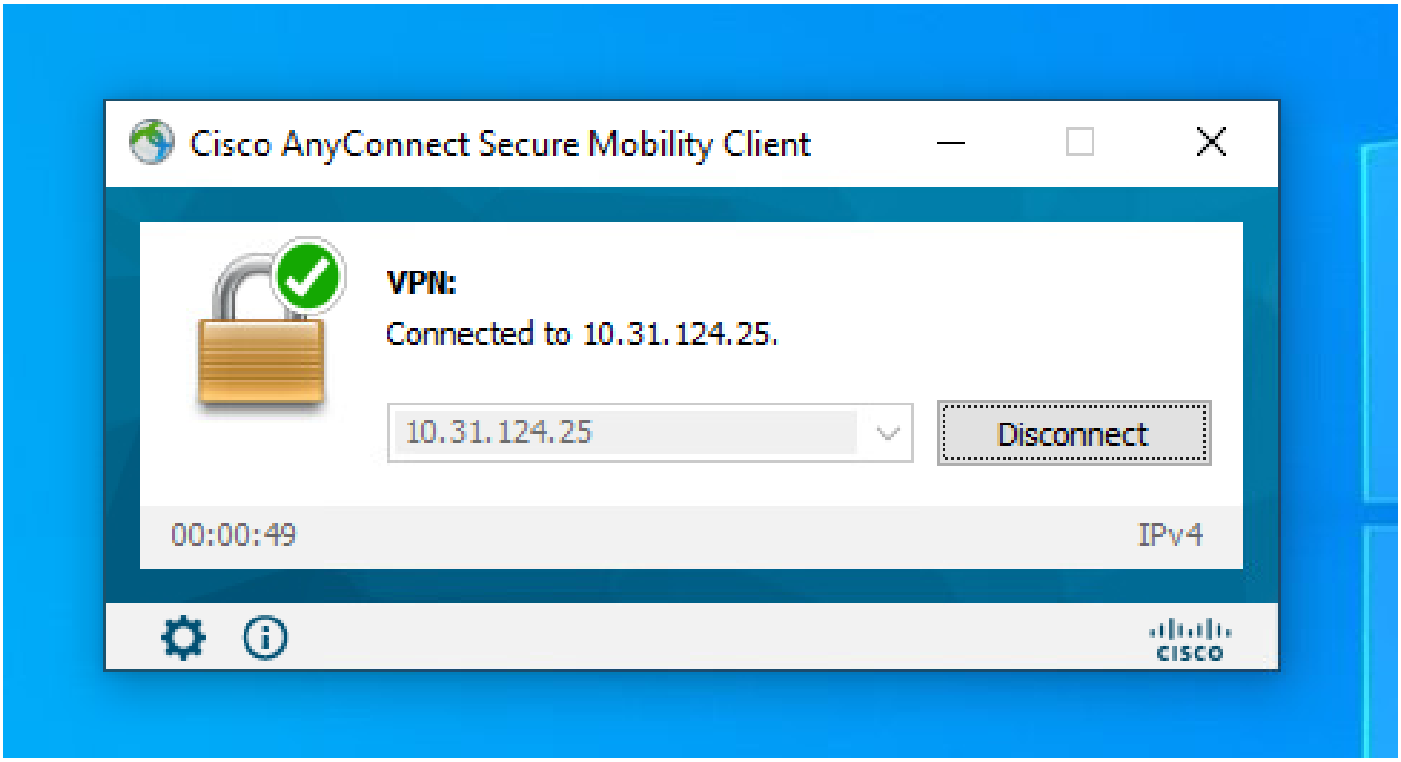


確認

導入が成功したら、WindowsクライアントからFTDへのCisco AnyConnectセキュアモビリティ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じ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に接続状態が表示されます。



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ィ

ブなCisco Secure Clientセッションを表示できます。

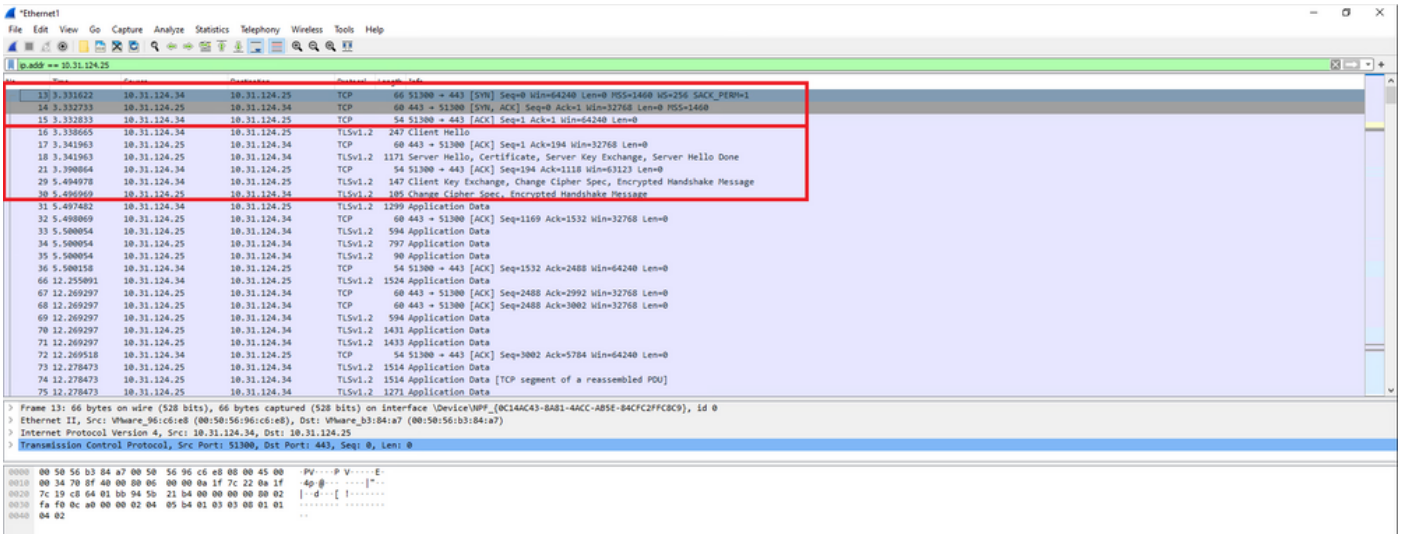
```
firepower# show vpn-sessiondb anyconnect

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 : 0000000000000800006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

トラブルシュート

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

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

Cisco Secure Clientのデバッグに加えて、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、WindowsクライアントとFTDの間の通常の3つのハンドシェイクが完了し、続いて暗号の同意に使用されるSSLハンドシェイクが完了した正常な接続の例です。



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。