Configura SSL Secure Client con autenticazione locale su FTD

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Secure Client (include Anyconnect) con autenticazione locale su FTD Cisco gestito da Cisco FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione SSL Secure Client tramite Firepower Management Center (FMC)
- Configurazione degli oggetti Firepower tramite FMC
- certificati SSL su Firepower

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower Threat Defense (FTD) versione 7.0.0 (build 94)
- Cisco FMC versione 7.0.0 (Build 94)
- Cisco Secure Mobility Client 4.10.01075

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nell'esempio, il protocollo SSL (Secure Sockets Layer) viene utilizzato per creare una rete VPN (Virtual Private Network) tra FTD e un client Windows 10.

A partire dalla versione 7.0.0, FTD gestito da FMC supporta l'autenticazione locale per Cisco Secure Client. Può essere definito come metodo di autenticazione primario o come fallback nel caso in cui si verifichi un errore del metodo primario. In questo esempio, l'autenticazione locale è configurata come autenticazione primaria.

Prima di questa versione software, l'autenticazione locale Cisco Secure Client su FTD era disponibile solo su Cisco Firepower Device Manager (FDM).

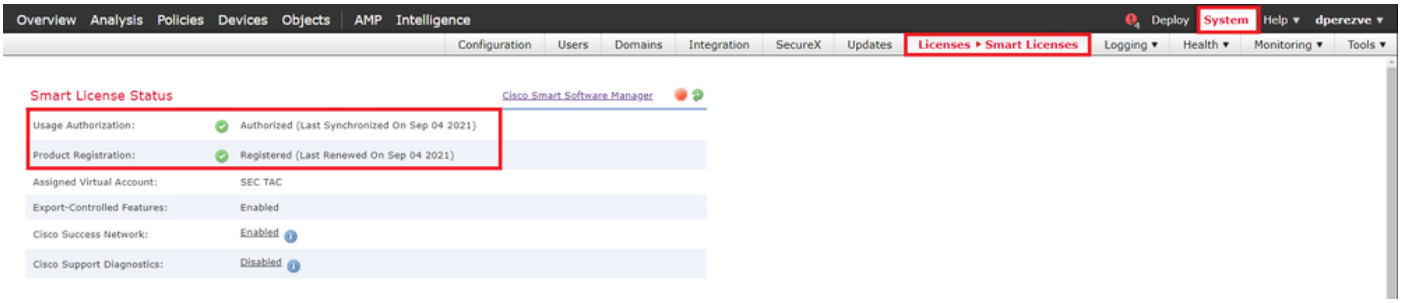
Configurazione

Configurazioni

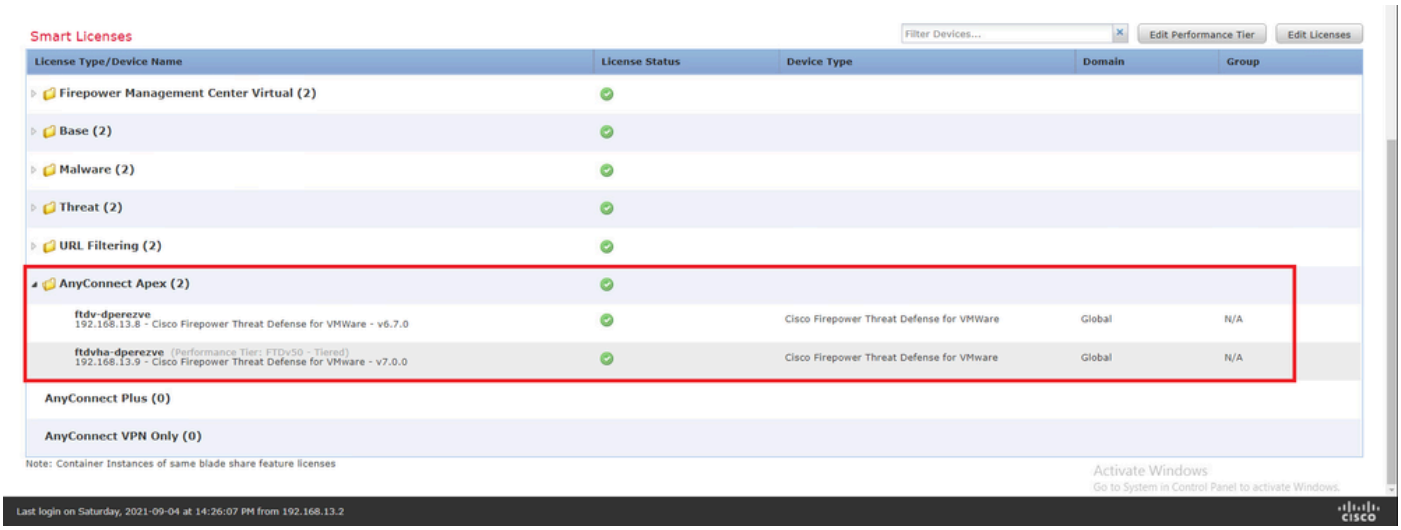
Passaggio 1. Verifica delle licenze

Prima di configurare Cisco Secure Client, è necessario registrare il FMC e renderlo conforme a Smart Licensing Portal. Non è possibile implementare Cisco Secure Client se FTD non ha una licenza Plus, Apex o VPN Only valida.

Selezionare Sistema > Licenze > Smart Licenses per verificare che FMC sia registrato e conforme al portale Smart Licensing:



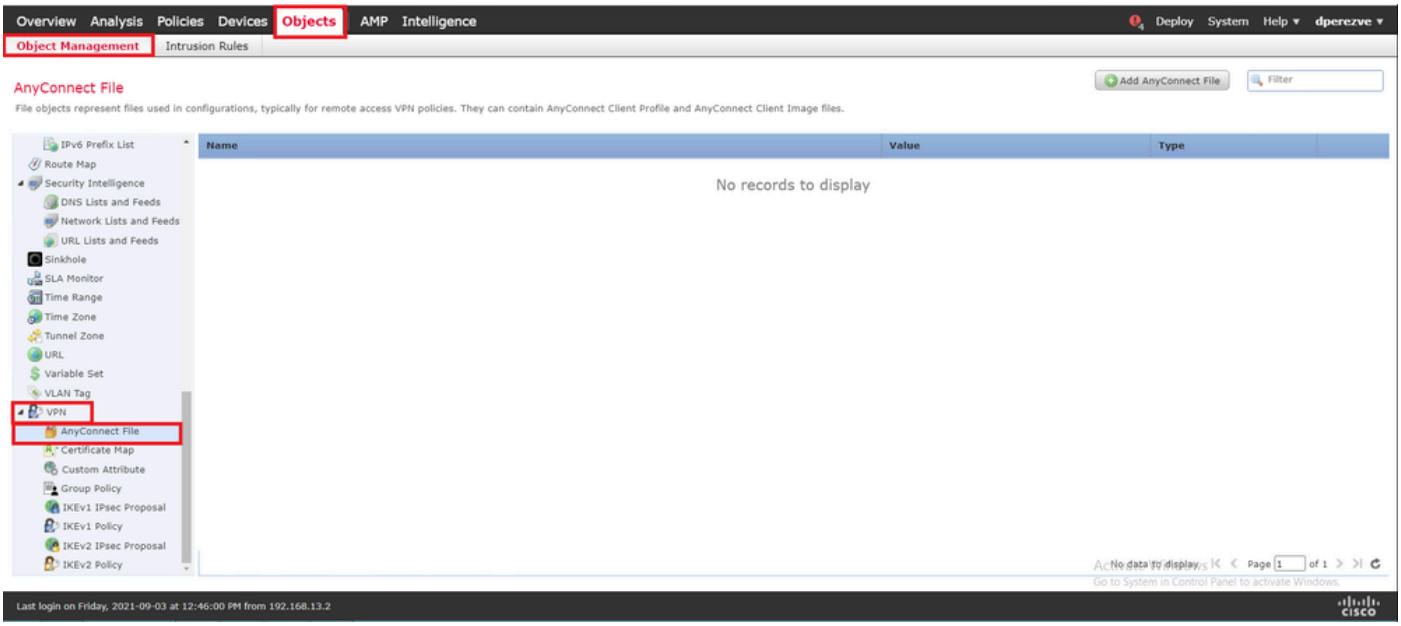
Scorrere verso il basso nella stessa pagina. Nella parte inferiore del grafico Licenze Smart, è possibile visualizzare i diversi tipi di licenze Cisco Secure Client (AnyConnect) disponibili e i dispositivi sottoscritti a ciascuno di essi. Assicurarsi che l'FTD in questione sia registrato in una delle seguenti categorie:



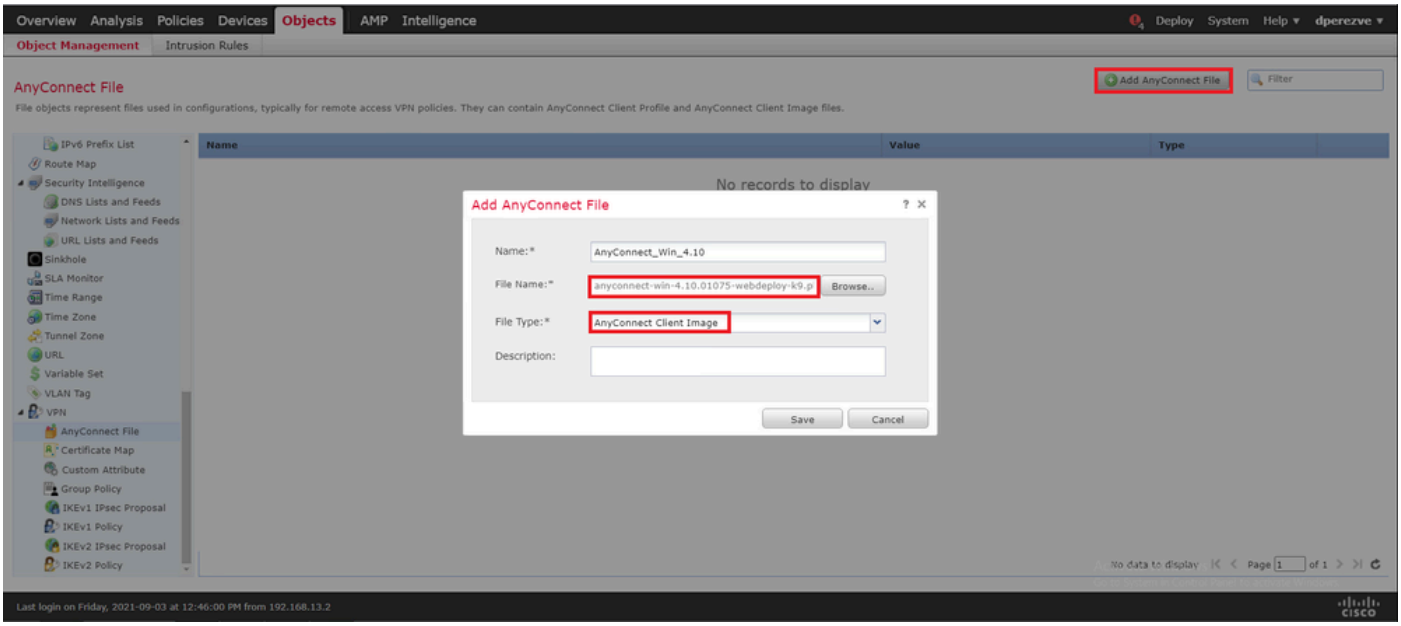
Passaggio 2. Carica Cisco Secure Client Package in FMC

Scaricare il pacchetto di distribuzione headend Cisco Secure Client (AnyConnect) per Windows dal sito [cisco.com:](cisco.com)

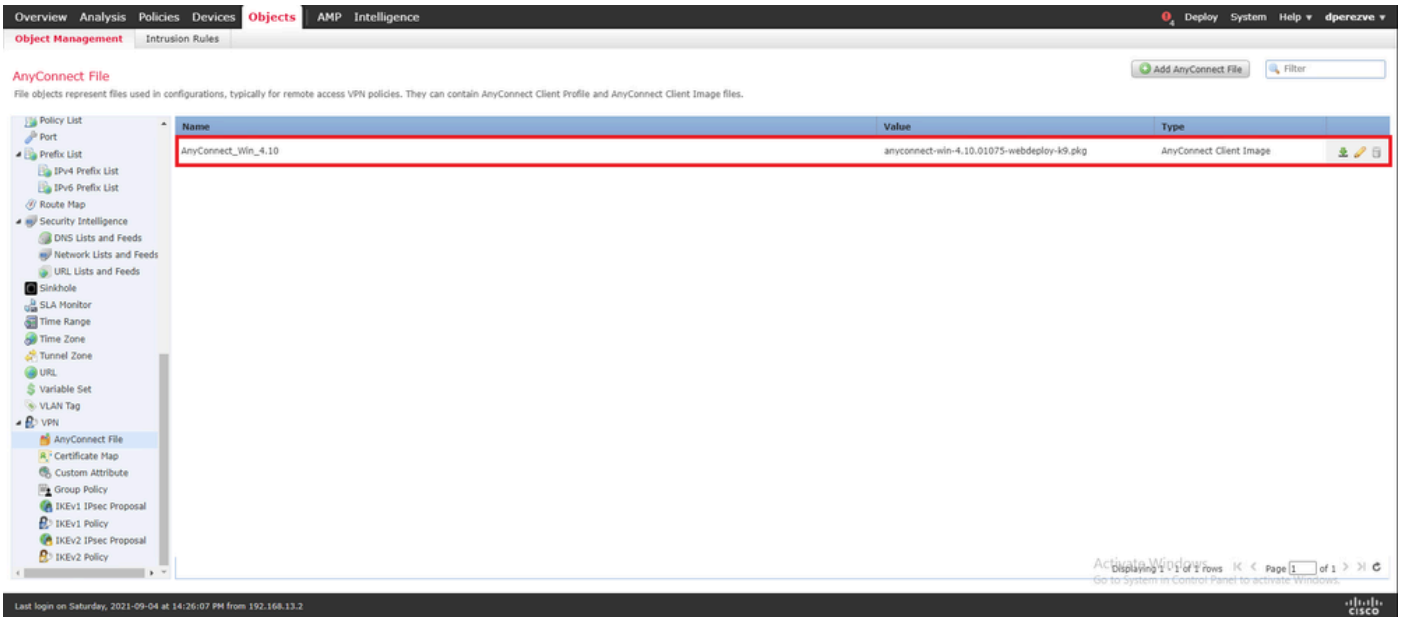
Per caricare l'immagine Cisco Secure Client, selezionare Oggetti > Gestione oggetti e scegliere Cisco Secure Client File nella categoria VPN del sommario:



Scegliere il pulsante Aggiungi file AnyConnect. Nella finestra Add AnyConnect Secure Client File, assegnare un nome all'oggetto, quindi scegliere Browse (Sfoglia) per selezionare il pacchetto Cisco Secure Client. Infine, scegliere AnyConnect Client Image come tipo di file dal menu a discesa:



Scegliere il pulsante Salva. L'oggetto deve essere aggiunto all'elenco degli oggetti:



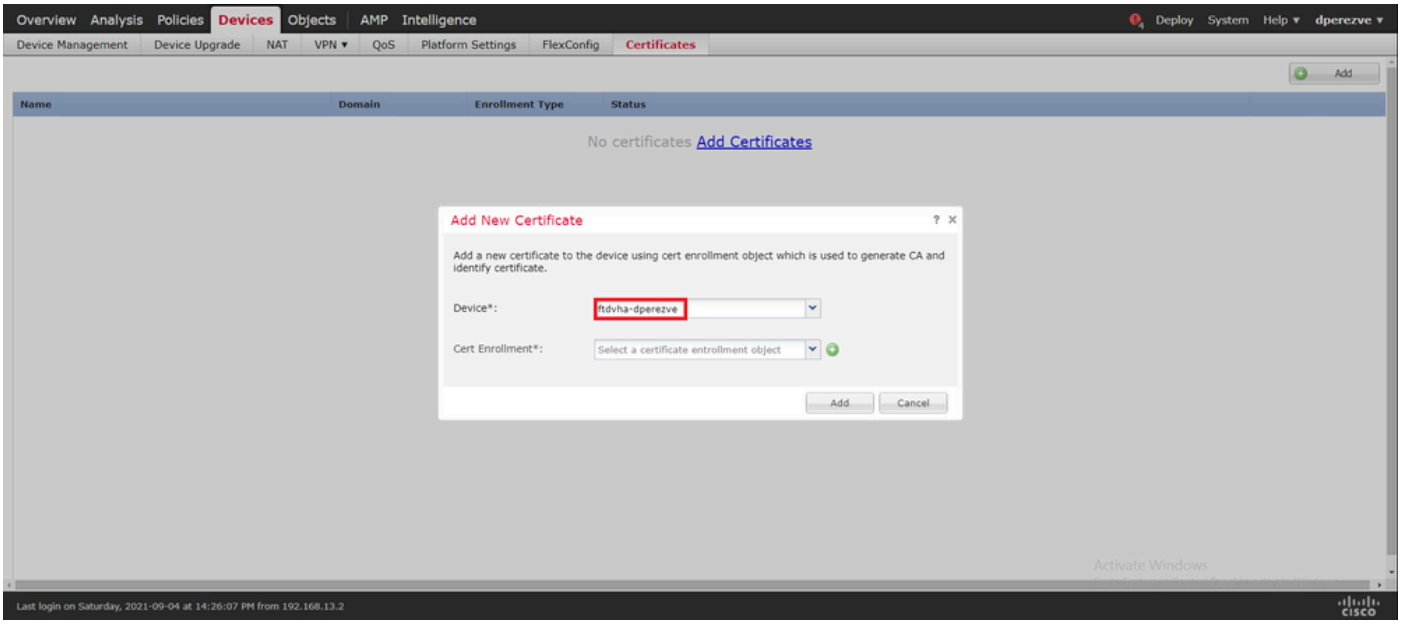
Passaggio 3. Genera un certificato autofirmato

SSL Cisco Secure Client (AnyConnect) richiede l'utilizzo di un certificato valido nell'handshake SSL tra l'headend VPN e il client.

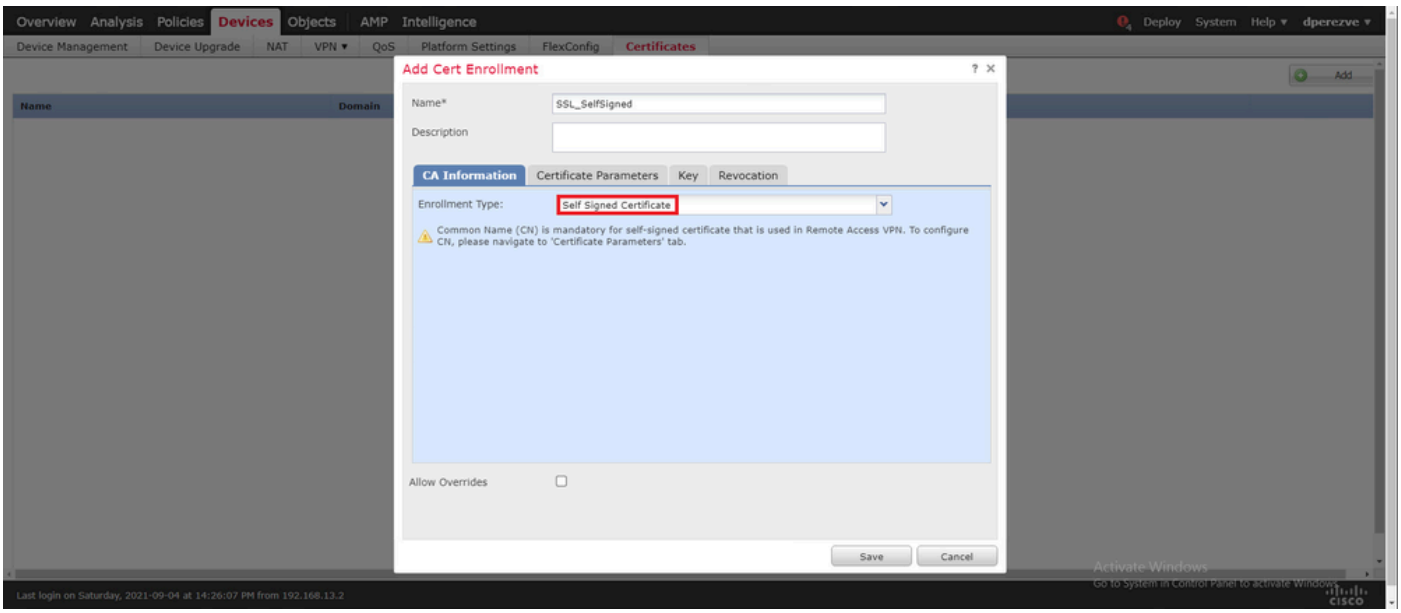
Nota: in questo esempio viene generato un certificato autofirmato. Oltre ai certificati autofirmati, è inoltre possibile caricare un certificato firmato da un'Autorità di certificazione (CA) interna o da una CA nota.

Per creare il certificato autofirmato, passare a Dispositivi > Certificati.

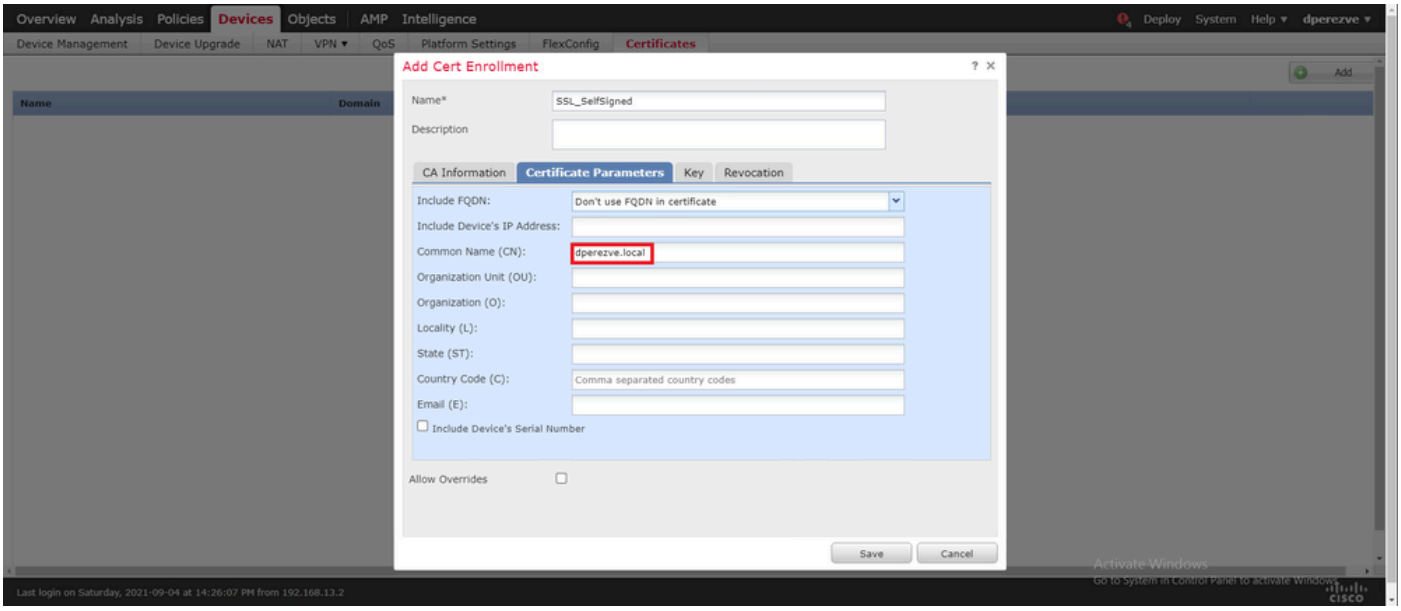
Scegliere il pulsante Aggiungi. Quindi scegliere l'FTD elencato nel menu a discesa Dispositivo nella finestra Aggiungi nuovo certificato.



Scegliere il pulsante Aggiungi registrazione certificato (verde + simbolo) per creare un nuovo oggetto di registrazione. Nella finestra Aggiungi registrazione certificato assegnare un nome all'oggetto e scegliere Certificato autofirmato dal menu a discesa Tipo di registrazione.



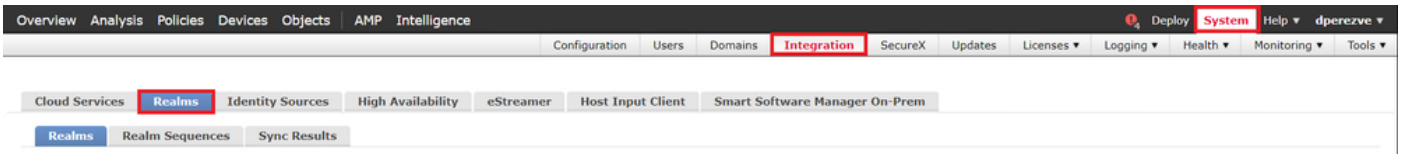
Infine, per i certificati autofirmati, è obbligatorio disporre di un nome comune (CN). Passare alla scheda Parametri certificato per definire un CN:



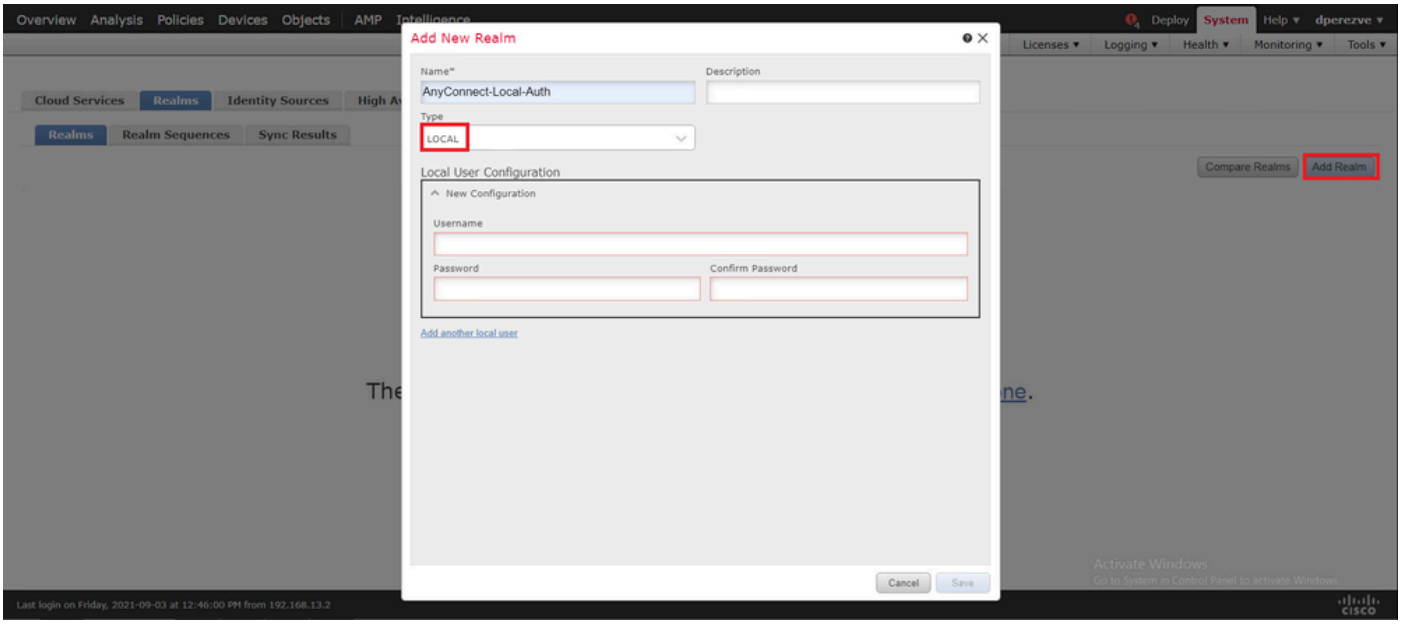
Fare clic sui pulsanti Salva e Aggiungi. Dopo un paio di secondi, il nuovo certificato deve essere aggiunto all'elenco dei certificati:

Passaggio 4. Crea realm locale in FMC

Il database degli utenti locale e le rispettive password vengono archiviati in un realm locale. Per creare il realm locale, passare a Sistema > Integrazione > Realm:

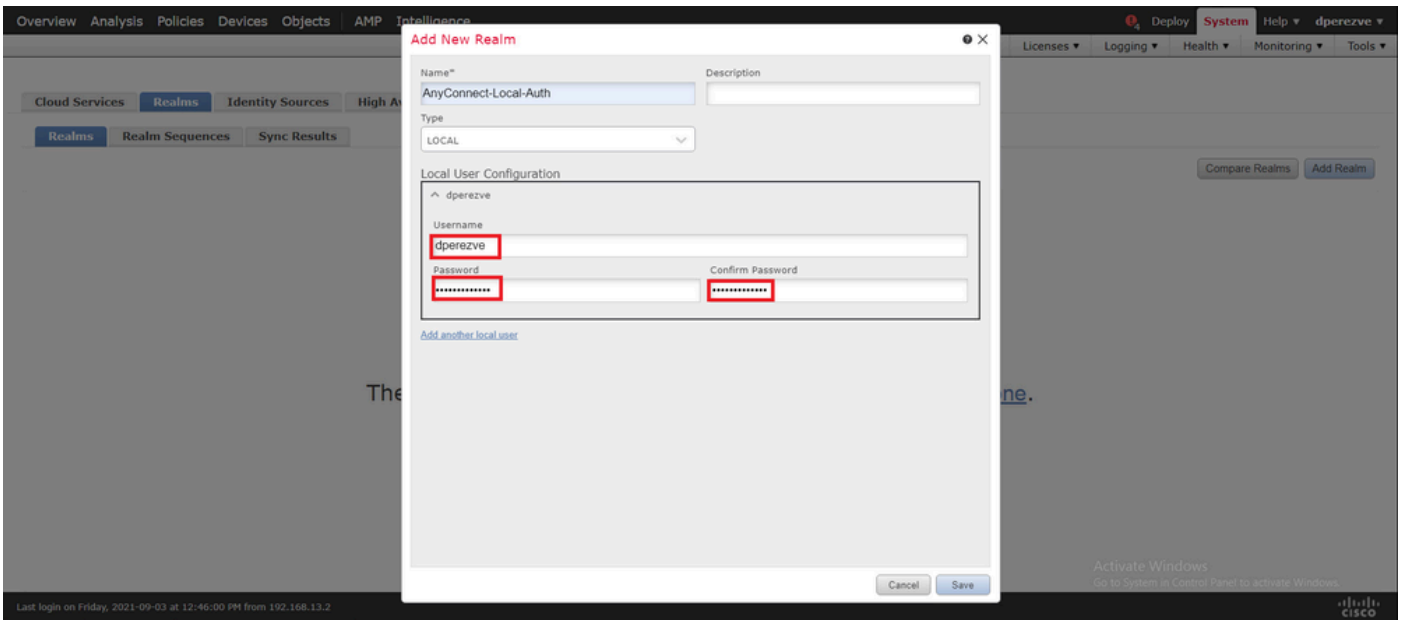


Scegliere il pulsante Aggiungi realm. Nella finestra Add New Realm, assegnare un nome e scegliere LOCAL dal menu a discesa Type:

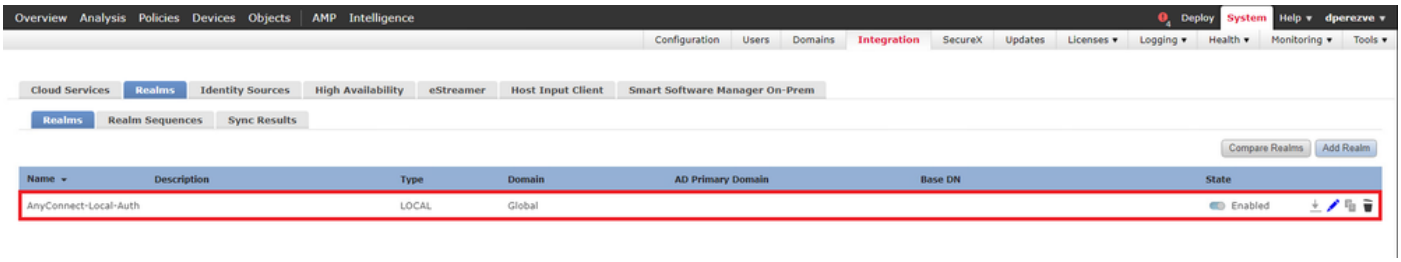


Nella sezione Configurazione utente locale vengono creati account utente e password.

Nota: le password devono contenere almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale.

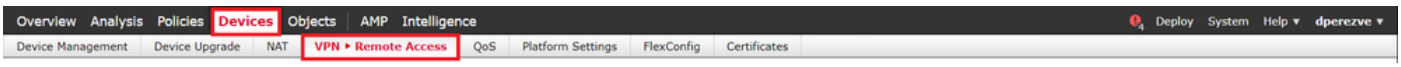


Salvare le modifiche, quindi fare clic su Aggiungi realm per aggiungere un nuovo realm all'elenco dei realm esistenti.

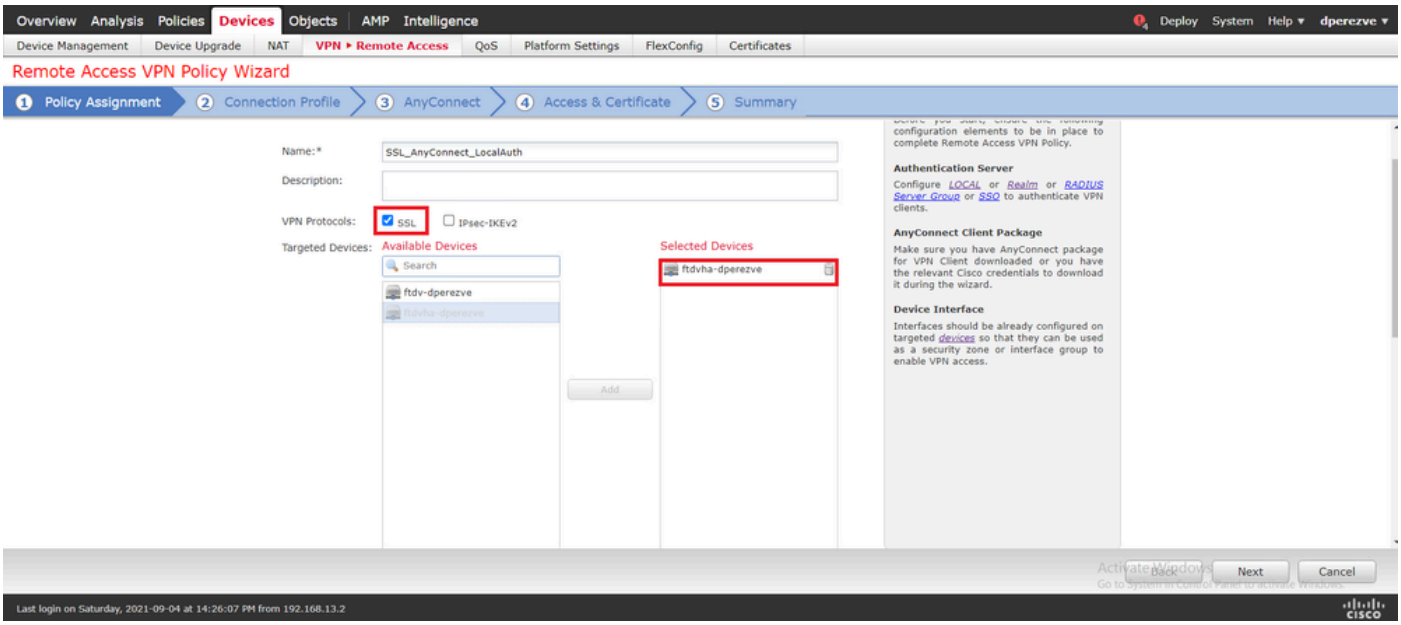


Passaggio 5. Configura SSL Cisco Secure Client

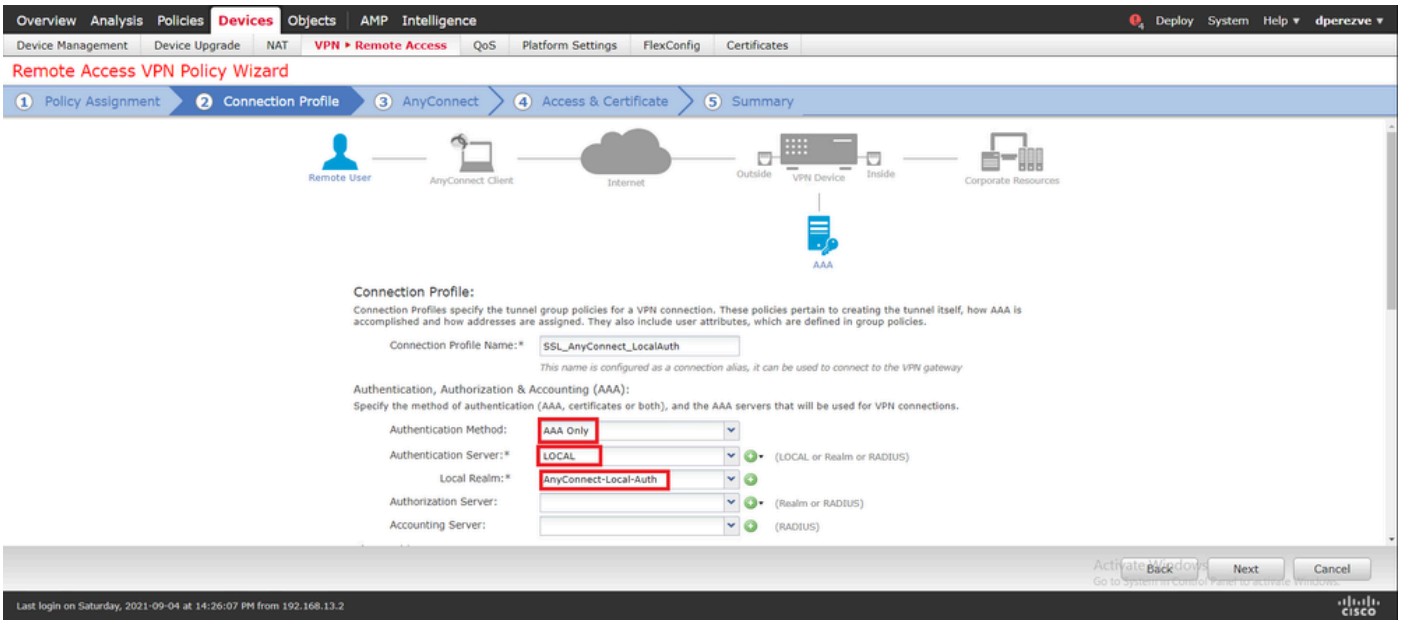
Per configurare SSL Cisco Secure Client, selezionare Dispositivi > VPN > Accesso remoto:



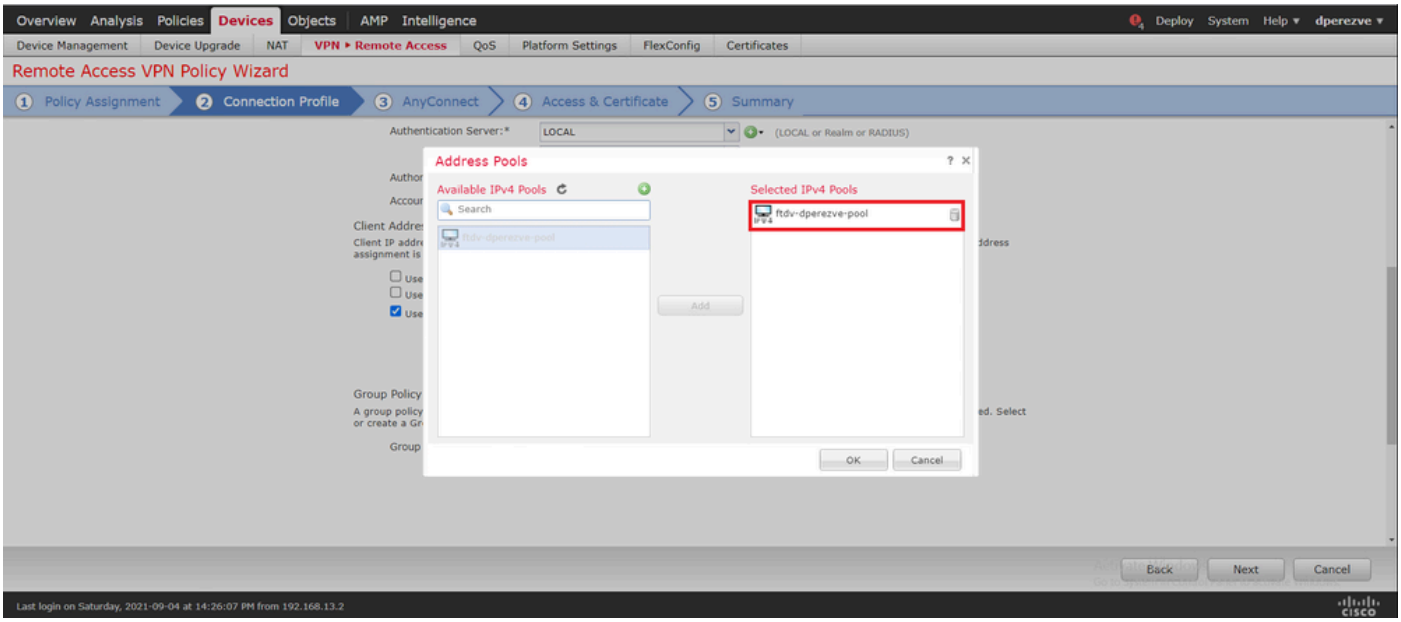
Per creare un nuovo criterio VPN, fare clic sul pulsante Add (Aggiungi). Definite un nome per il profilo di connessione, selezionate la casella di controllo SSL e scegliete l'FTD elencato come dispositivo di destinazione. È necessario configurare tutto nella sezione Assegnazione criteri della Creazione guidata criteri VPN di Accesso remoto:



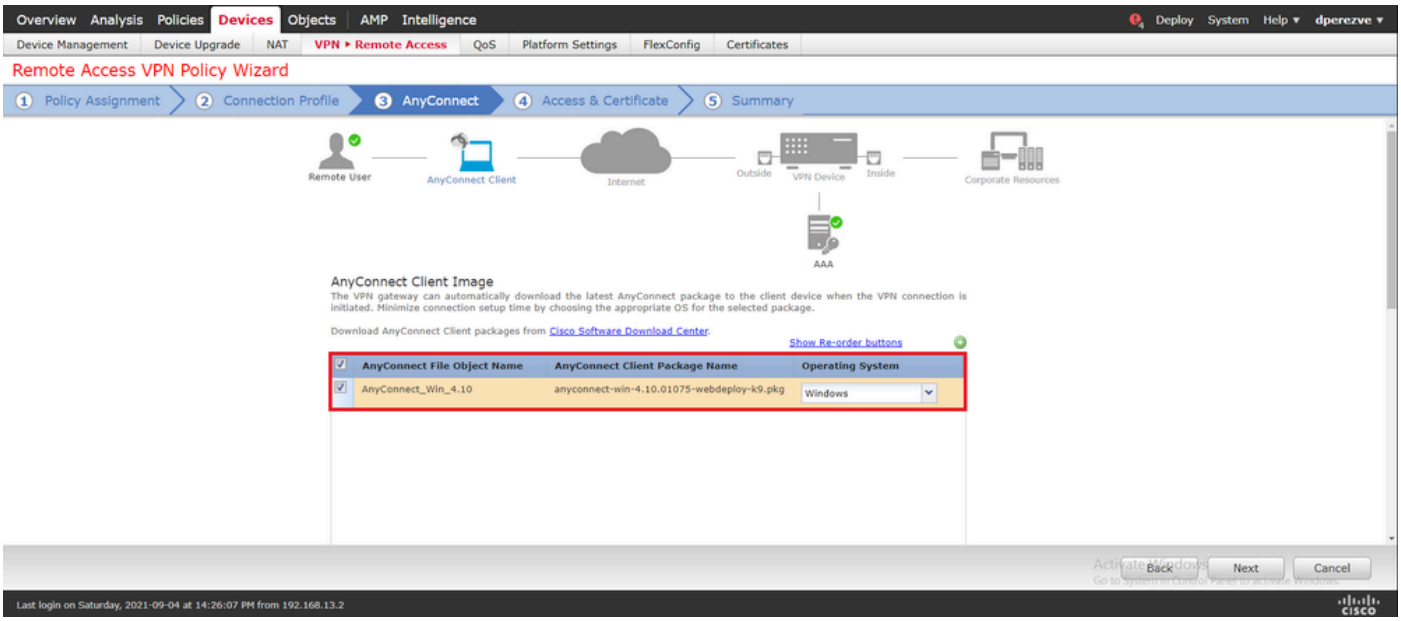
Per passare alla configurazione del profilo di connessione, scegliere Successivo. Assegnare un nome al profilo di connessione e scegliere Solo AAA come metodo di autenticazione. Quindi, nel menu a discesa Authentication Server, scegliere LOCAL, e infine, scegliere il realm locale creato al punto 4 nel menu a discesa Local Realm:



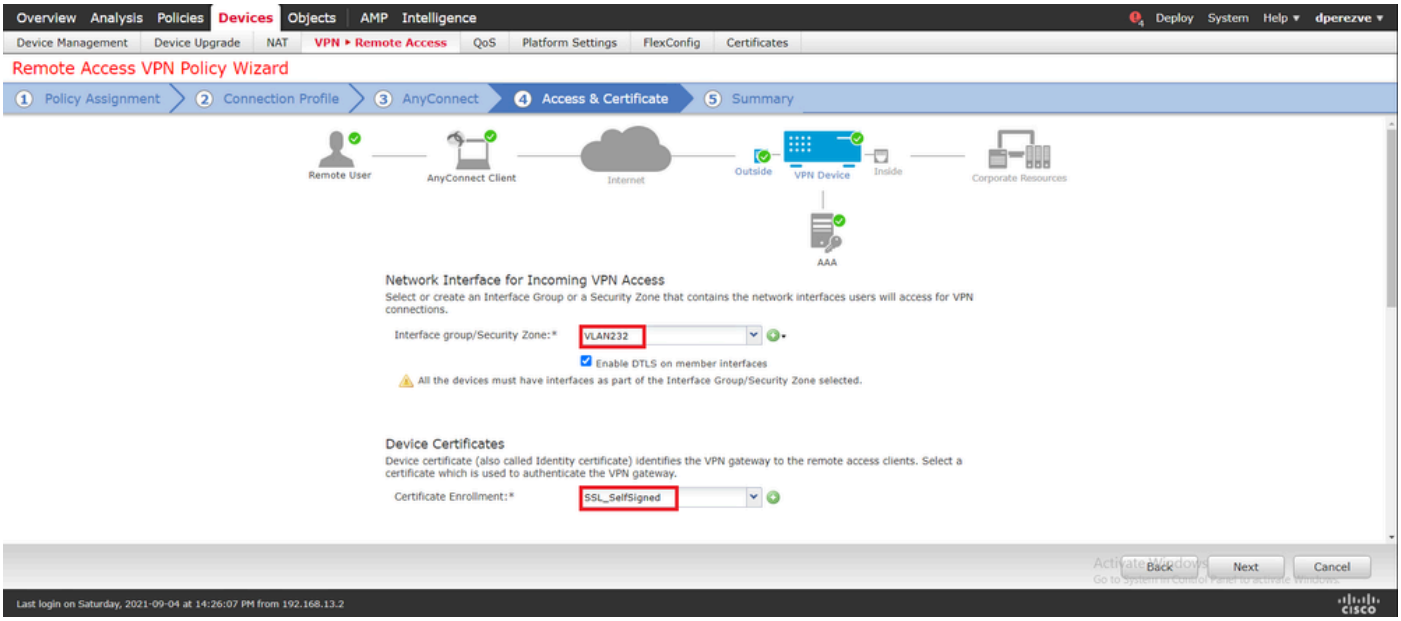
Scorrere la pagina verso il basso, quindi fare clic sull'icona a forma di matita nella sezione Pool di indirizzi IPv4 per definire il pool IP utilizzato dai Cisco Secure Client:



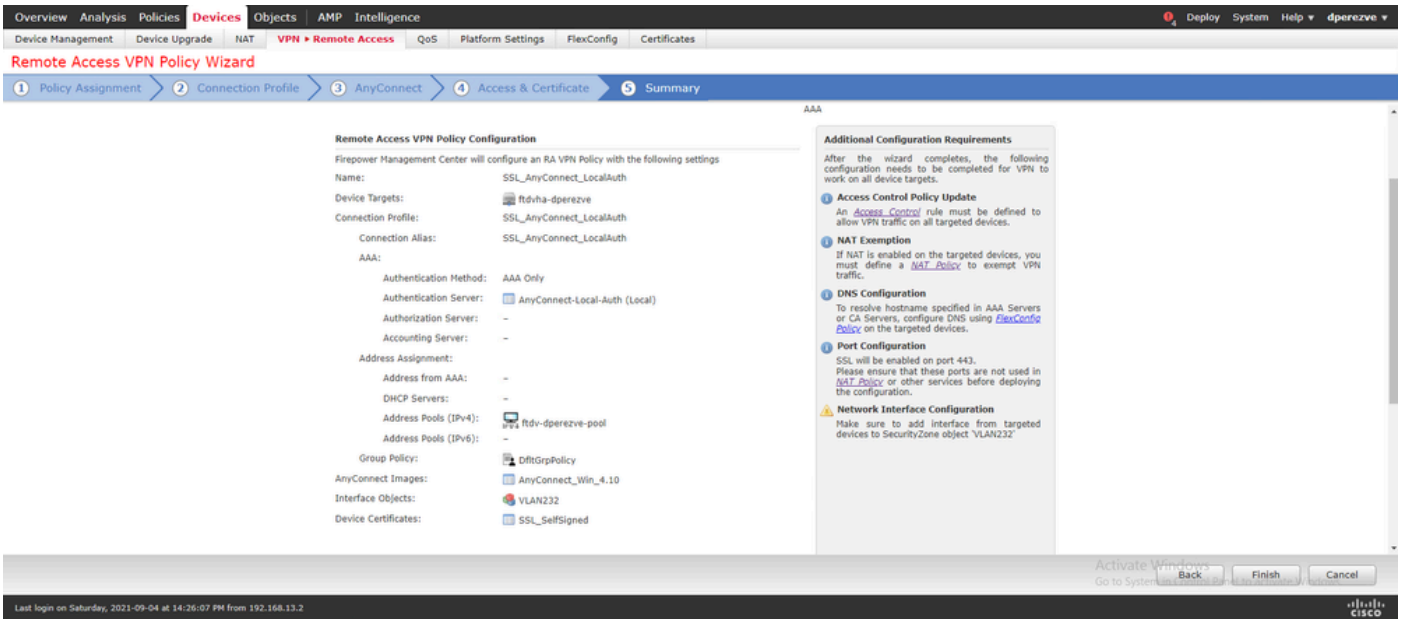
Per passare alla sezione AnyConnect, fare clic su Next (Avanti). A questo punto, selezionare l'immagine Cisco Secure Client caricata nel passaggio 2:



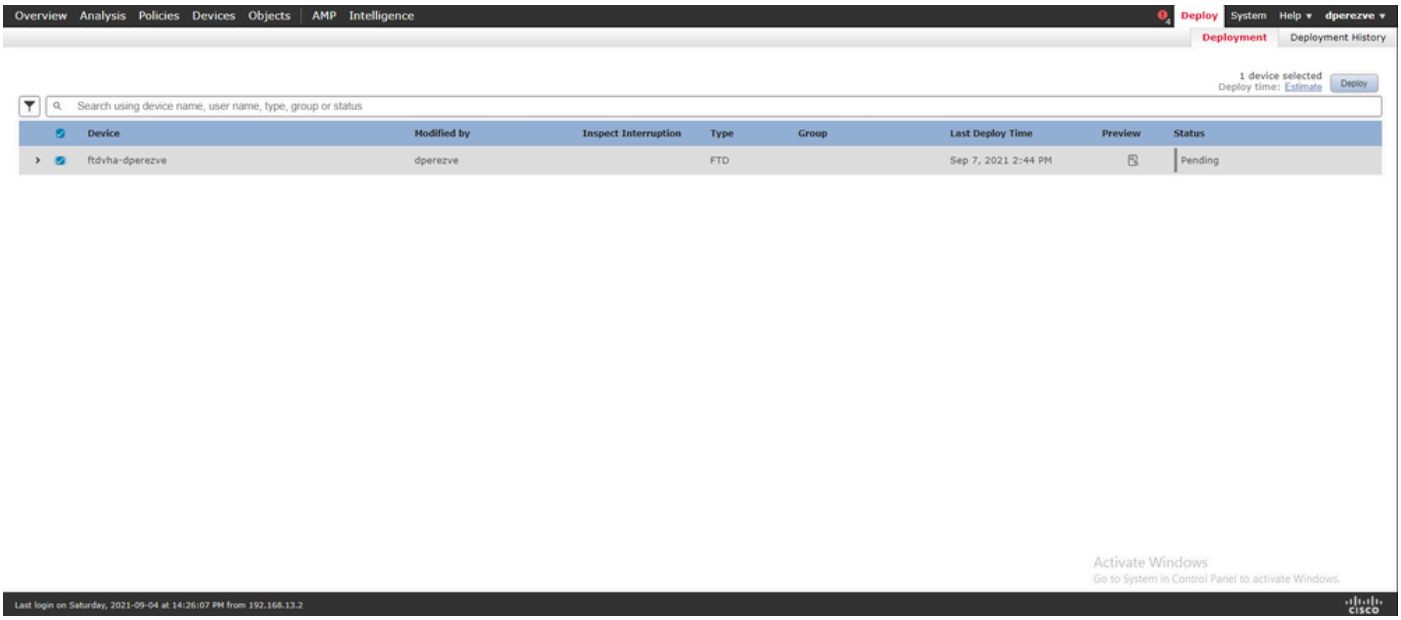
Per passare alla sezione Accesso e certificato, fare clic su Avanti. Nel menu a discesa Interface group/Security Zone (Gruppo di interfacce/Area di sicurezza), selezionare l'interfaccia su cui Cisco Secure Client (AnyConnect) deve essere abilitato. Quindi, nel menu a discesa Registrazione certificato, scegliere il certificato creato nel Passaggio 3:



Infine, fare clic su Avanti per visualizzare un riepilogo della configurazione di Cisco Secure Client:

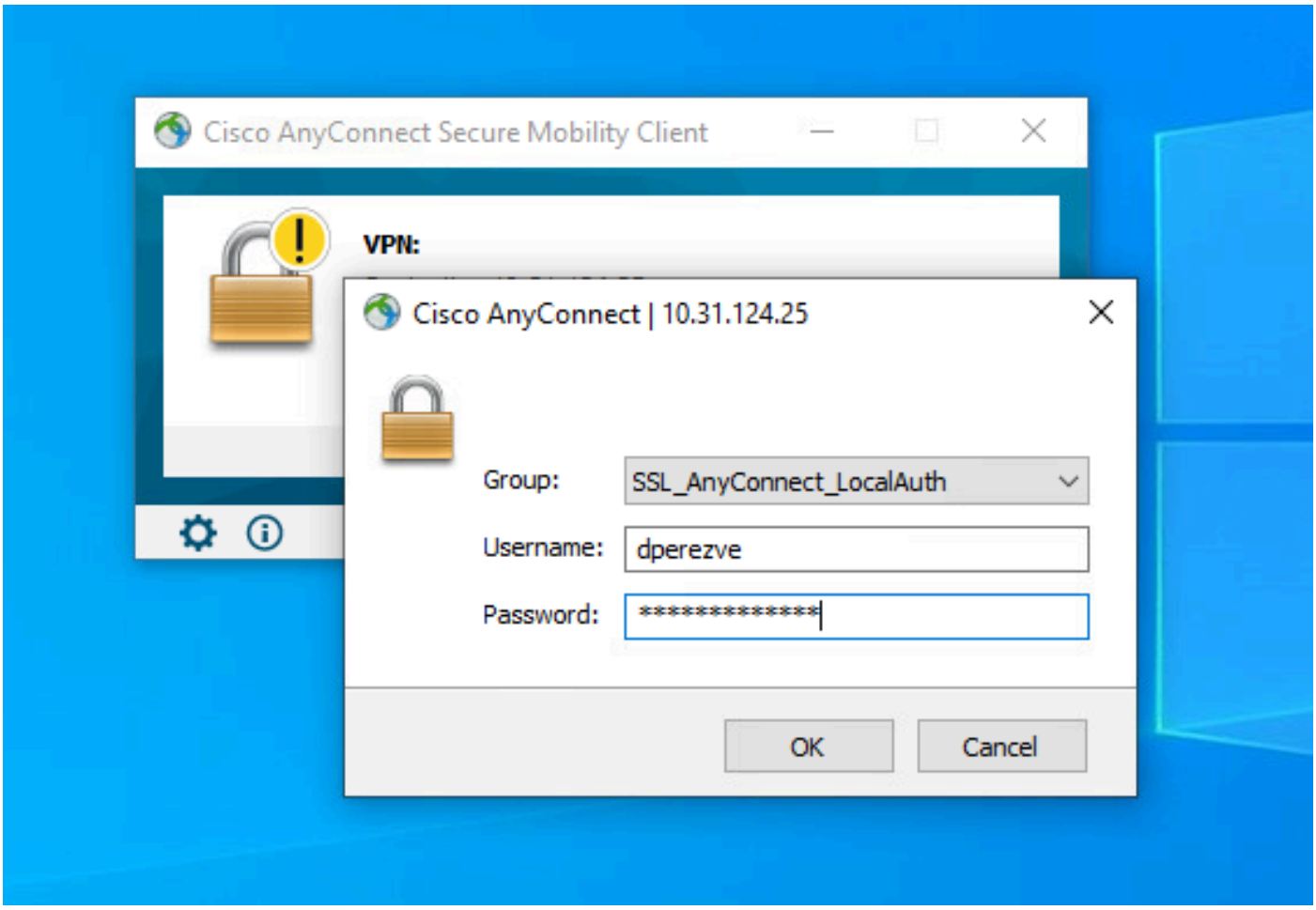


Se tutte le impostazioni sono corrette, fare clic su Fine e distribuire le modifiche a FTD.

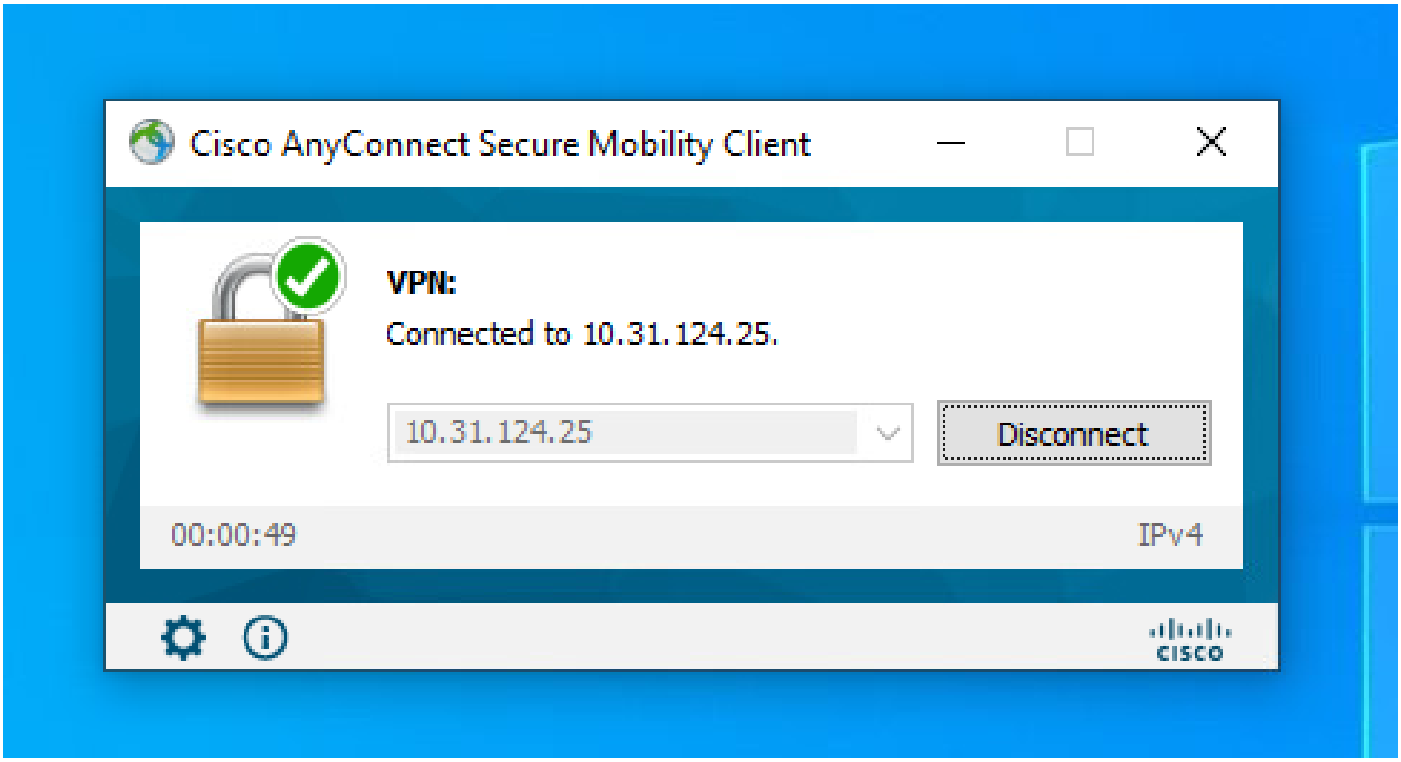


Verifica

Dopo aver completato la distribuzione, avviare una connessione Cisco AnyConnect Secure Mobility Client dal client Windows al file FTD. Il nome utente e la password utilizzati nella richiesta di autenticazione devono essere gli stessi di quelli creati al punto 4:



Dopo aver approvato le credenziali con FTD, l'app Cisco AnyConnect Secure Mobility Client deve visualizzare lo stato connesso:



Da FTD, è possibile eseguire il comando show vpn-sessiondb anyconnect per visualizzare le

sessioni Cisco Secure Client attualmente attive sul firewall:

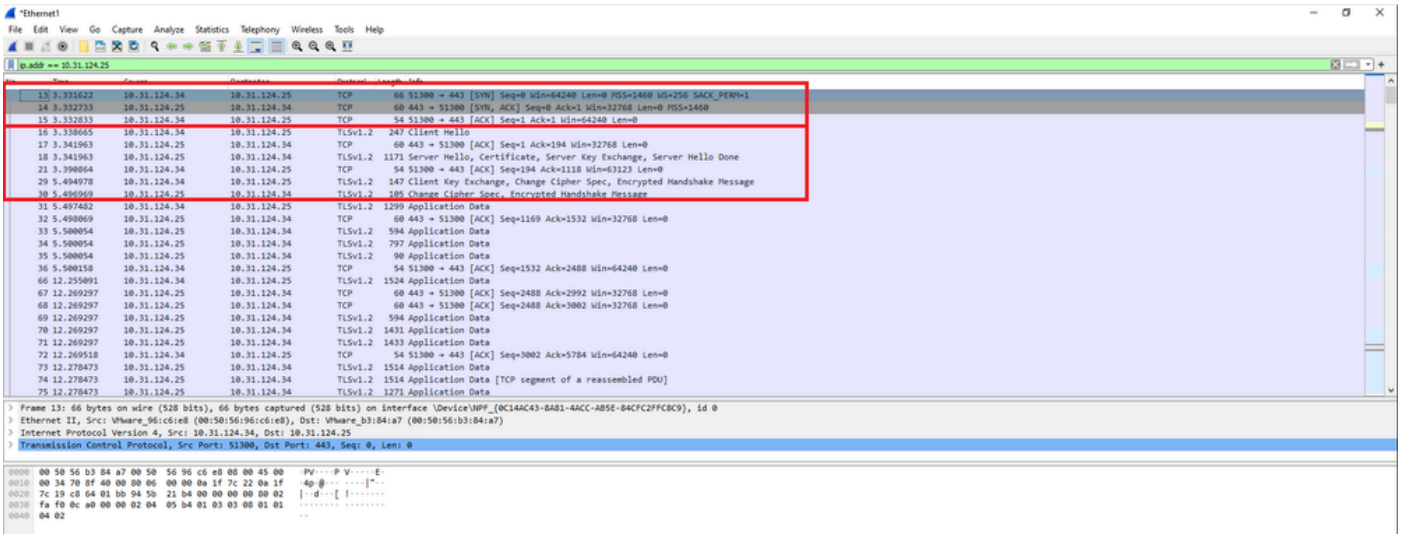
```
firepower# show vpn-sessiondb anyconnect

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
```

Risoluzione dei problemi

Eseguire il comando debug webvpn anyconnect 255 su FTD per verificare il flusso della connessione SSL su FTD:

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

Oltre ai debug Cisco Secure Client, il flusso di connessione può essere osservato anche con le acquisizioni di pacchetti TCP. Questo è un esempio di connessione riuscita, viene completato un normale handshake di tre caratteri tra il client Windows e FTD, seguito da un handshake SSL utilizzato per accettare i cifrari.



Dopo gli handshake del protocollo, FTD deve convalidare le credenziali con le informazioni archiviate nel realm locale.

Raccogliere il bundle DART e contattare Cisco TAC per ulteriori ricerche.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).