

Configura SSL Secure Client con autenticazione locale su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazioni](#)

[Passaggio 1. Verifica delle licenze](#)

[Passaggio 2. Carica Cisco Secure Client Package in FMC](#)

[Passaggio 3. Genera certificato autofirmato](#)

[Passaggio 4. Crea realm locale in FMC](#)

[Passaggio 5. Configura SSL Cisco Secure Client](#)

[Verifica](#)

[Risoluzione dei problemi](#)

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).

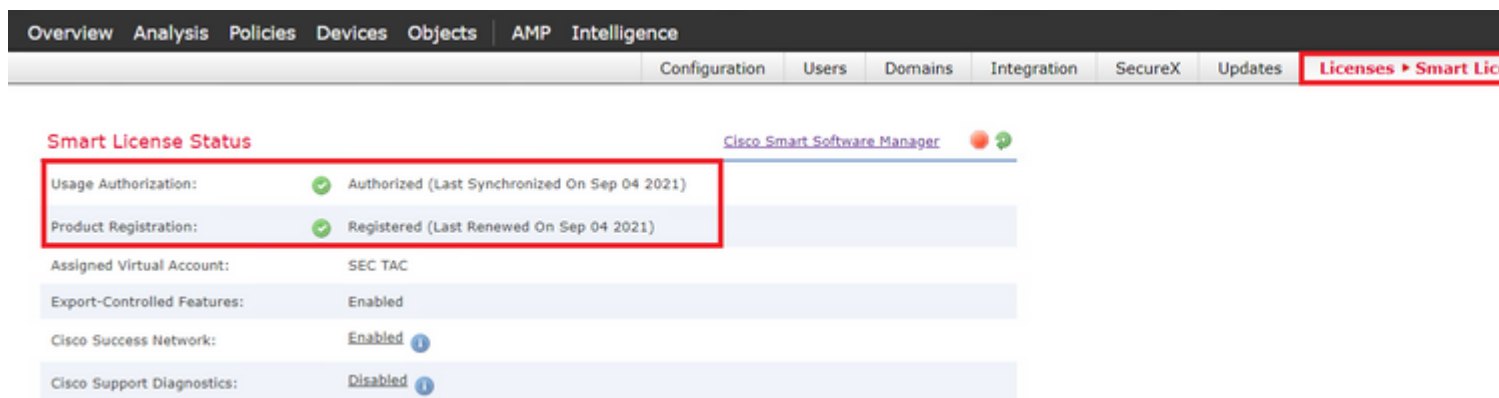
Configurazione

Configurazioni

Passaggio 1. Verifica delle licenze

Prima di configurare Cisco Secure Client, è necessario registrare il FMC e che sia 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 > Licenze Smart** per verificare che il FMC sia registrato e conforme a Smart Licensing Portal.



The screenshot shows the Cisco Smart License Status page. The navigation bar at the top includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main navigation bar includes Configuration, Users, Domains, Integration, SecureX, Updates, and Licenses > Smart Lic. The Smart License Status page displays the following information:

Smart License Status		Cisco Smart Software Manager
Usage Authorization:	Authorized (Last Synchronized On Sep 04 2021)	
Product Registration:	Registered (Last Renewed On Sep 04 2021)	
Assigned Virtual Account:	SEC TAC	
Export-Controlled Features:	Enabled	
Cisco Success Network:	Enabled	
Cisco Support Diagnostics:	Disabled	

Nella stessa pagina, in fondo al grafico **Smart Licenses** vengono visualizzati i diversi tipi di licenze Cisco Secure Client (AnyConnect) e i dispositivi sottoscritti. Verificare che l'FTD esistente sia registrato in una di queste categorie.

Smart Licenses













License Type/Device Name	License Status	Device Type
▶ Firepower Management Center Virtual (2)	✓	
▶ Base (2)	✓	
▶ Malware (2)	✓	
▶ Threat (2)	✓	
▶ URL Filtering (2)	✓	
▲ AnyConnect Apex (2)	✓	
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare
ftdvha-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMWare - v7.0.0	✓	Cisco Firepower Threat Defense for VMWare
AnyConnect Plus (0)		
AnyConnect VPN Only (0)		

Note: Container Instances of same blade share feature licenses

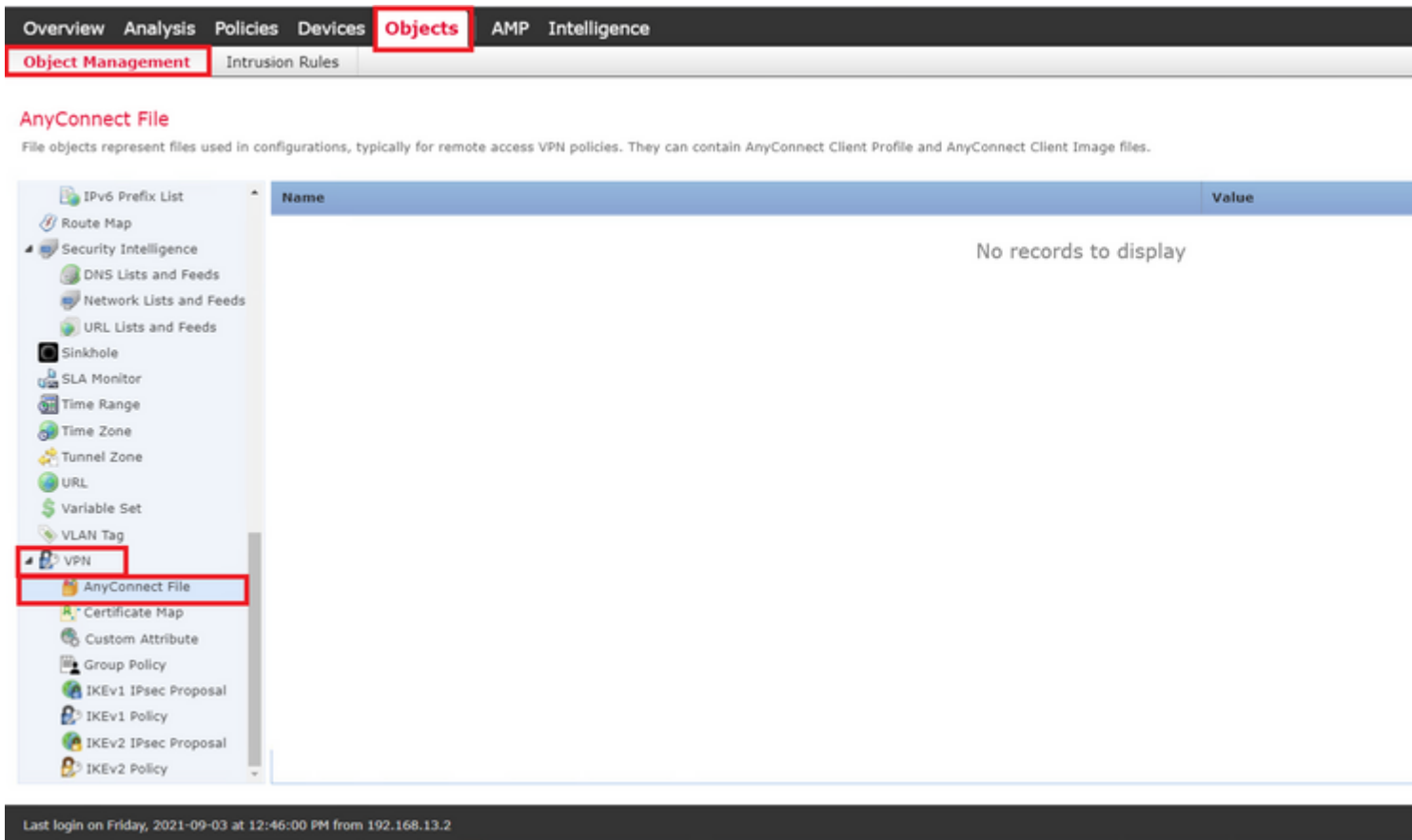
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Passaggio 2. Carica Cisco Secure Client Package in FMC

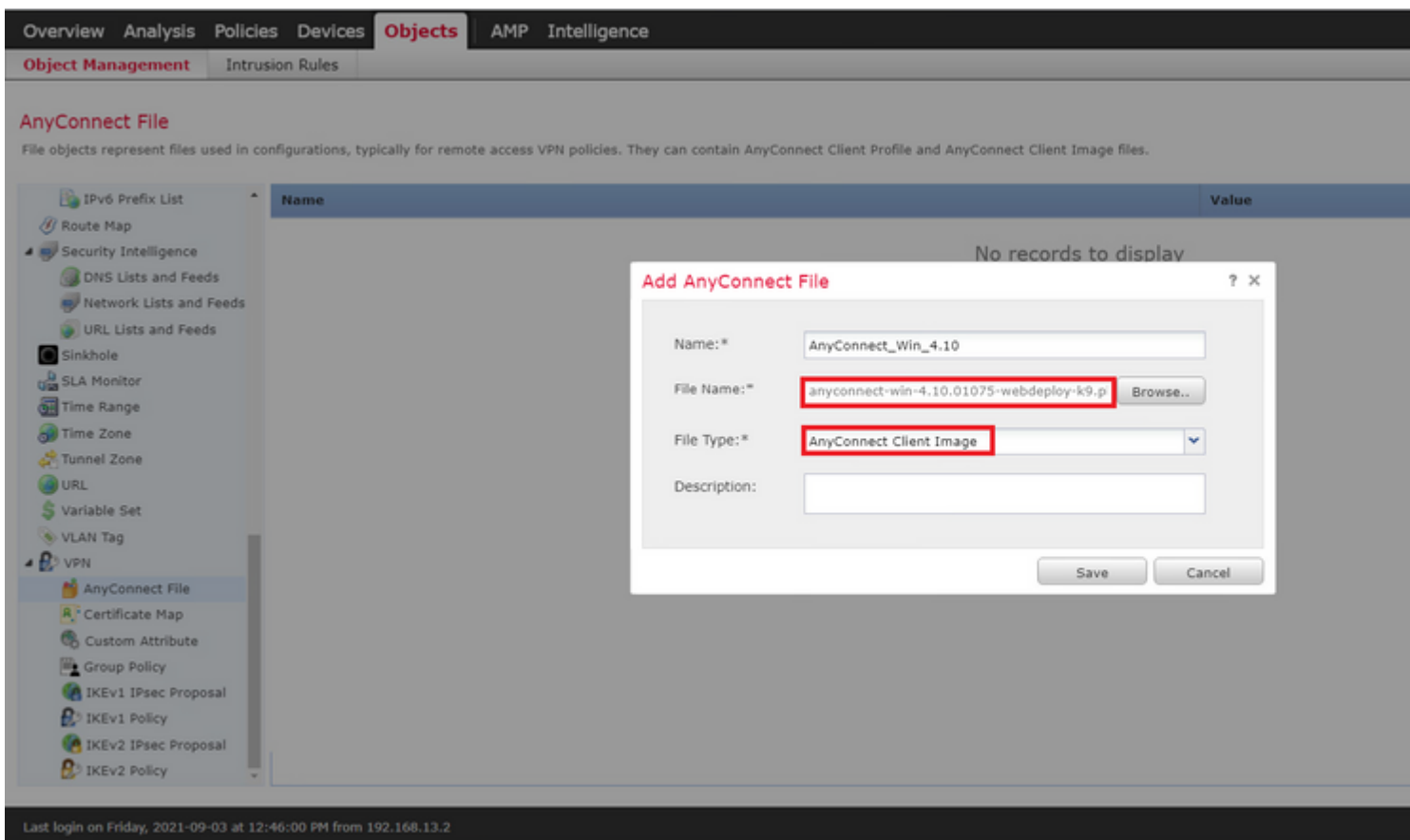
Scaricare il pacchetto di distribuzione headend Cisco Secure Client (AnyConnect) per Windows dal sito [cisco.com](https://www.cisco.com).

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

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



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



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

The screenshot shows the Cisco FTD GUI with the 'Objects' tab selected. The left sidebar contains a tree view of object categories, with 'AnyConnect File' highlighted under the 'VPN' category. The main area displays a table with the following data:

Name	Value
AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdep

At the bottom of the screen, a status bar indicates: 'Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2'.

Passaggio 3. Genera 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. Tuttavia, oltre ai certificati autofirmati, è possibile caricare anche un certificato firmato da un'autorità di certificazione (CA) interna o da una CA nota.

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

The screenshot shows the Cisco FTD GUI with the 'Devices' tab selected in the top navigation bar. Below it, the 'Certificates' sub-tab is also selected and highlighted with a red box.

Scegliere il pulsante **Aggiungi**. Quindi scegliere l'FTD presente nel menu a discesa **Device** nella finestra **Add New Certificate**.

Overview Analysis Policies **Devices** Objects AMP Intelligence


Device Management Device Upgrade NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

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*: 

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

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**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain
------	--------


Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

 Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides

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

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

The screenshot shows the 'Add Cert Enrollment' dialog box in the FMC interface. The 'Certificate Parameters' tab is selected, and the 'Common Name (CN)' field is highlighted with a red box, containing the text 'dperezve.local'. Other fields include 'Name*' (SSL_SelfSigned), 'Description', 'Include FQDN' (Don't use FQDN in certificate), 'Include Device's IP Address', 'Organization Unit (OU)', 'Organization (O)', 'Locality (L)', 'State (ST)', 'Country Code (C)', and 'Email (E)'. There is also an unchecked checkbox for 'Include Device's Serial Number' and an 'Allow Overrides' checkbox.

Scegliere i pulsanti **Salva** e **Aggiungi**. Dopo alcuni secondi, il nuovo certificato deve essere aggiunto all'elenco dei certificati.

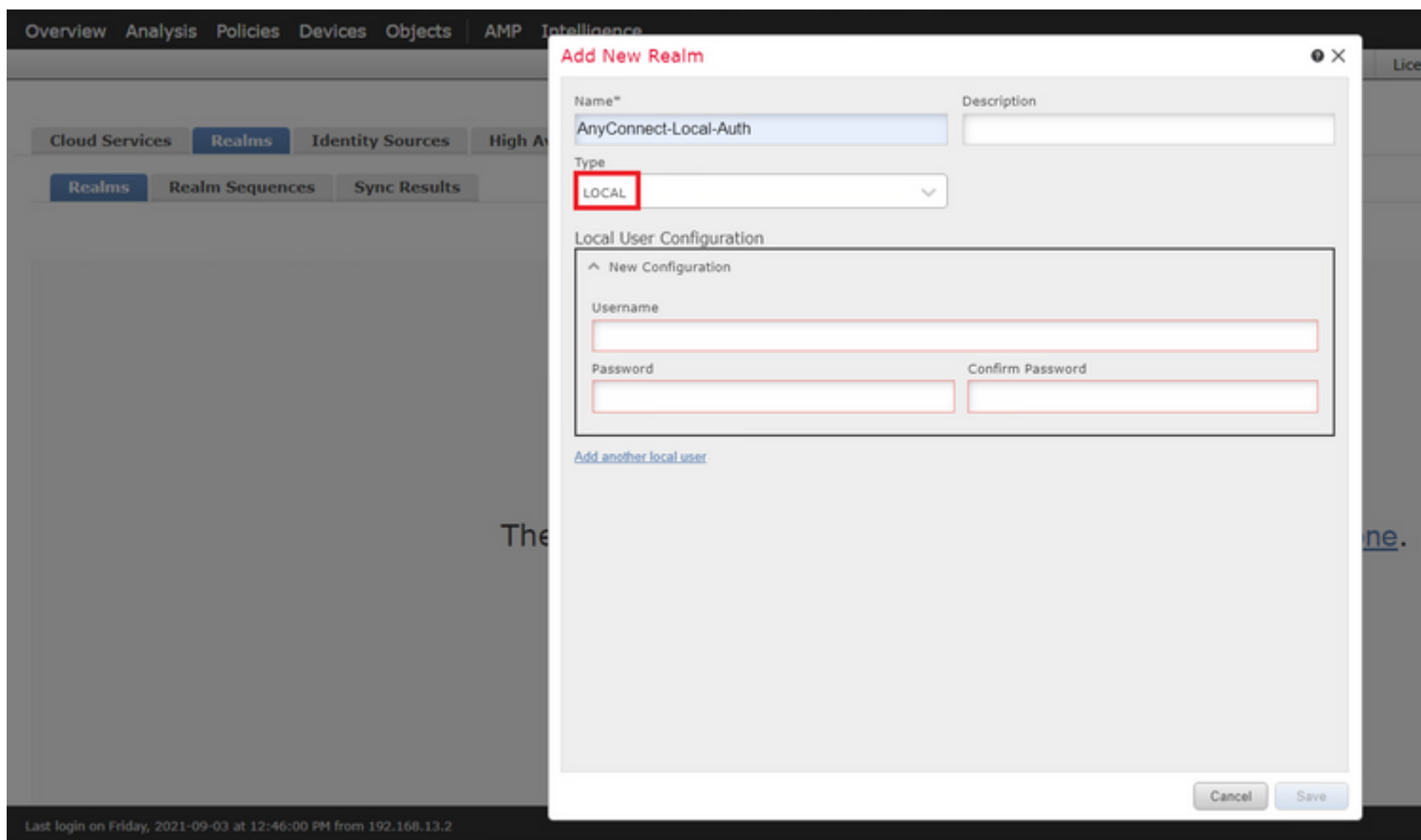
The screenshot shows the 'Certificates' list in the FMC interface. A new certificate entry is visible, highlighted with a red box. The entry is named 'ftdvha-dperezve' and has a sub-entry 'SSL_SelfSigned' with a 'Global' domain and 'Self-Signed' enrollment type. The table has columns for Name, Domain, Enrollment Type, and Status.

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, selezionare **Sistema > Integrazione > Realm**.

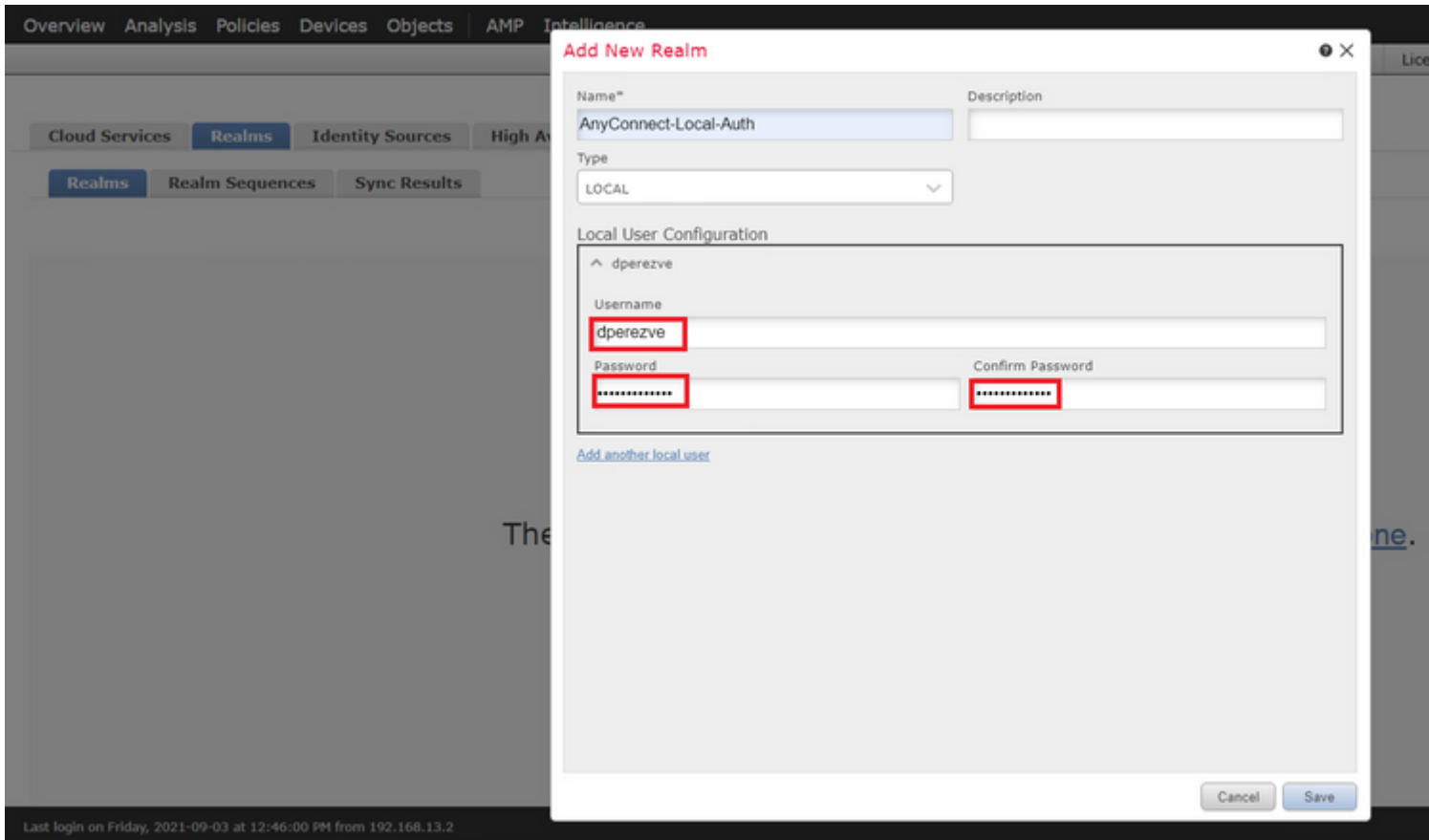
The screenshot shows the 'Integration' menu in the FMC interface. The 'Realms' option is highlighted with a red box. Other options in the menu include 'Configuration', 'Users', 'Domains', 'SecureX', 'Updates', and 'License'. Below the menu, there are buttons for 'Cloud Services', 'Realms', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Manager On-Prem'. The 'Realms' button is also highlighted with a red box.

Scegliere il pulsante **Aggiungi realm**. Nella finestra **Aggiungi nuovo realm**, assegnare un nome e scegliere l'opzione **LOCAL** nel menu a discesa **Type**.

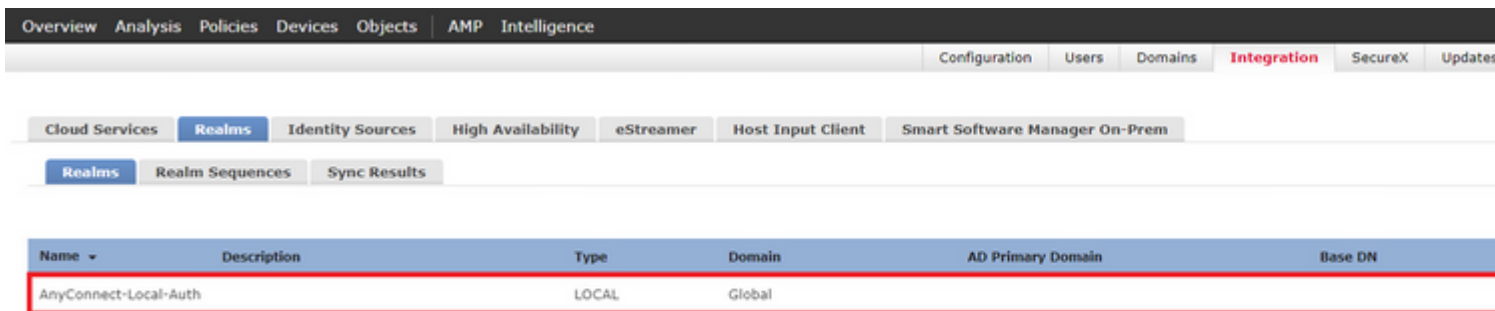


Nella sezione Configurazione utente locale vengono creati account utente e password.

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



Salvare le modifiche e 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, scegliere il pulsante **Aggiungi**. Definite un nome per il profilo di connessione, selezionate la casella di controllo SSL e scegliete l'FTD disponibile come dispositivo di destinazione. È necessario configurare tutto nella sezione **Assegnazione criteri** della **Creazione guidata criteri VPN di Accesso remoto**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT **VPN ► Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

Name: * SSL_AnyConnect_LocalAuth

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

Search

ftdv-dperezve

ftdvha-dperezve

Add

Selected Devices

ftdvha-dperezve

Authentication Server
Configure [LOCAL](#) or [Realm Server Group](#) or [SSO](#) to authenticate clients.

AnyConnect Client Package
Make sure you have AnyConnect for VPN Client downloaded on the relevant Cisco credentials during the wizard.

Device Interface
Interfaces should be already configured and targeted [devices](#) so that they can be used as a security zone or interface to enable VPN access.

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

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**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT **VPN ► Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

Remote User — AnyConnect Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

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: * SSL_AnyConnect_LocalAuth
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: AAA Only

Authentication Server: * LOCAL (LOCAL or Realm or RADIUS)

Local Realm: * AnyConnect-Local-Auth

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

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

Scorrere la pagina verso il basso, quindi scegliere l'icona a forma di matita nella sezione **Pool di indirizzi IPv4** per definire il pool IP utilizzato dai Cisco Secure Client.

The screenshot displays the Cisco Secure VPN Policy Wizard interface. The main navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. Below this, there are sub-tabs for Device Management, Device Upgrade, NAT, VPN > Remote Access, QoS, Platform Settings, FlexConfig, and Certificates. The wizard is currently in the 'Access & Certificate' step (step 4 of 5). The 'Authentication Server' is set to 'LOCAL'. A modal dialog titled 'Address Pools' is open, showing a list of 'Available IPv4 Pools' with one pool, 'ftdv-dperezve-pool', selected. This pool is also listed in the 'Selected IPv4 Pools' section. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Per passare alla sezione **AnyConnect**, scegliere **Successivo**. A questo punto, scegliere l'immagine Cisco Secure Client caricata nel passaggio 2.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT **VPN ▶ Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
The VPN gateway can automatically download the latest AnyConnect 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 AnyConnect Client packages from [Cisco Software Download Center](#). [Show Re-order buttons](#)

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	Windows

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

Per passare alla sezione **Accesso e certificato**, scegliere **Avanti**. Nel menu a discesa **Gruppo di interfacce/Area di sicurezza**, scegliere 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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT **VPN ▶ Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

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:*

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

Infine, scegliere **Avanti** per visualizzare un riepilogo della configurazione di Cisco Secure Client.

The screenshot shows the 'Remote Access VPN Policy Wizard' in the Cisco Secure Client interface. The navigation bar includes: Overview, Analysis, Policies, **Devices**, Objects, AMP, Intelligence. Below this, there are tabs for Device Management, Device Upgrade, NAT, **VPN** (with a sub-tab for Remote Access), QoS, Platform Settings, FlexConfig, and Certificates. The wizard progress is shown as: 1 Policy Assignment, 2 Connection Profile, 3 AnyConnect, 4 Access & Certificate, 5 Summary.

Remote Access VPN Policy Configuration

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

- Name: SSL_AnyConnect_LocalAuth
- Device Targets: ftdvha-dperezve
- Connection Profile: SSL_AnyConnect_LocalAuth
- Connection Alias: SSL_AnyConnect_LocalAuth
- AAA:
 - Authentication Method: AAA Only
 - Authentication Server: AnyConnect-Local-Auth (Local)
 - Authorization Server: -
 - Accounting Server: -
- Address Assignment:
 - Address from AAA: -
 - DHCP Servers: -
 - Address Pools (IPv4): ftdv-dperezve-pool
 - Address Pools (IPv6): -
- Group Policy: DfltGrpPolicy
- AnyConnect Images: AnyConnect_Win_4.10
- Interface Objects: VLAN232
- Device Certificates: SSL_SelfSigned

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'VLAN232'

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

Se tutte le impostazioni sono corrette, scegliere **Fine** e distribuire le modifiche a FTD.

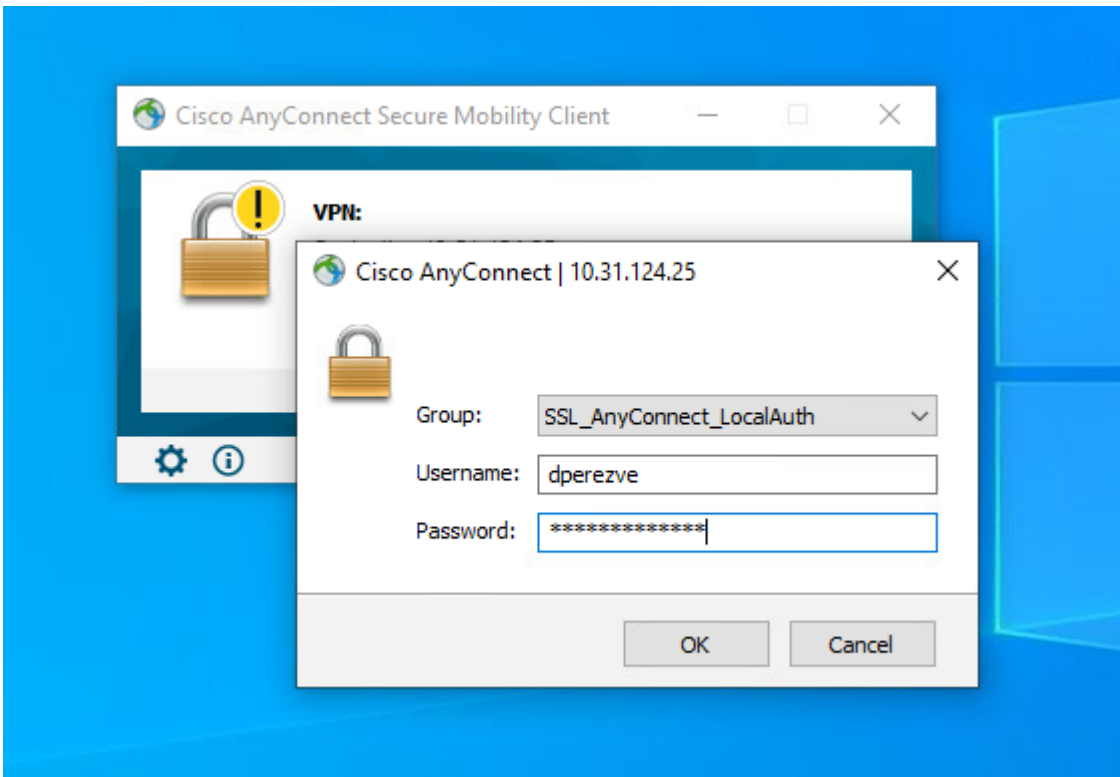
The screenshot shows the Cisco Secure Client interface with the navigation bar: Overview, Analysis, Policies, **Devices**, Objects, AMP, Intelligence. Below the navigation bar is a search bar with the text 'Search using device name, user name, type, group or status'.

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time
<input checked="" type="checkbox"/> ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 P

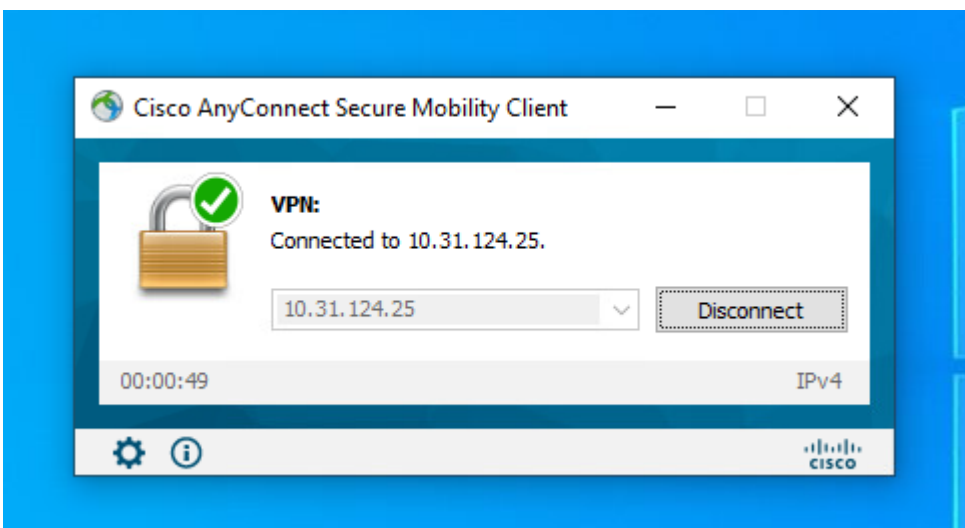
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

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 uguali a quelli creati al passaggio 4.



Dopo l'approvazione delle credenziali da parte dell'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

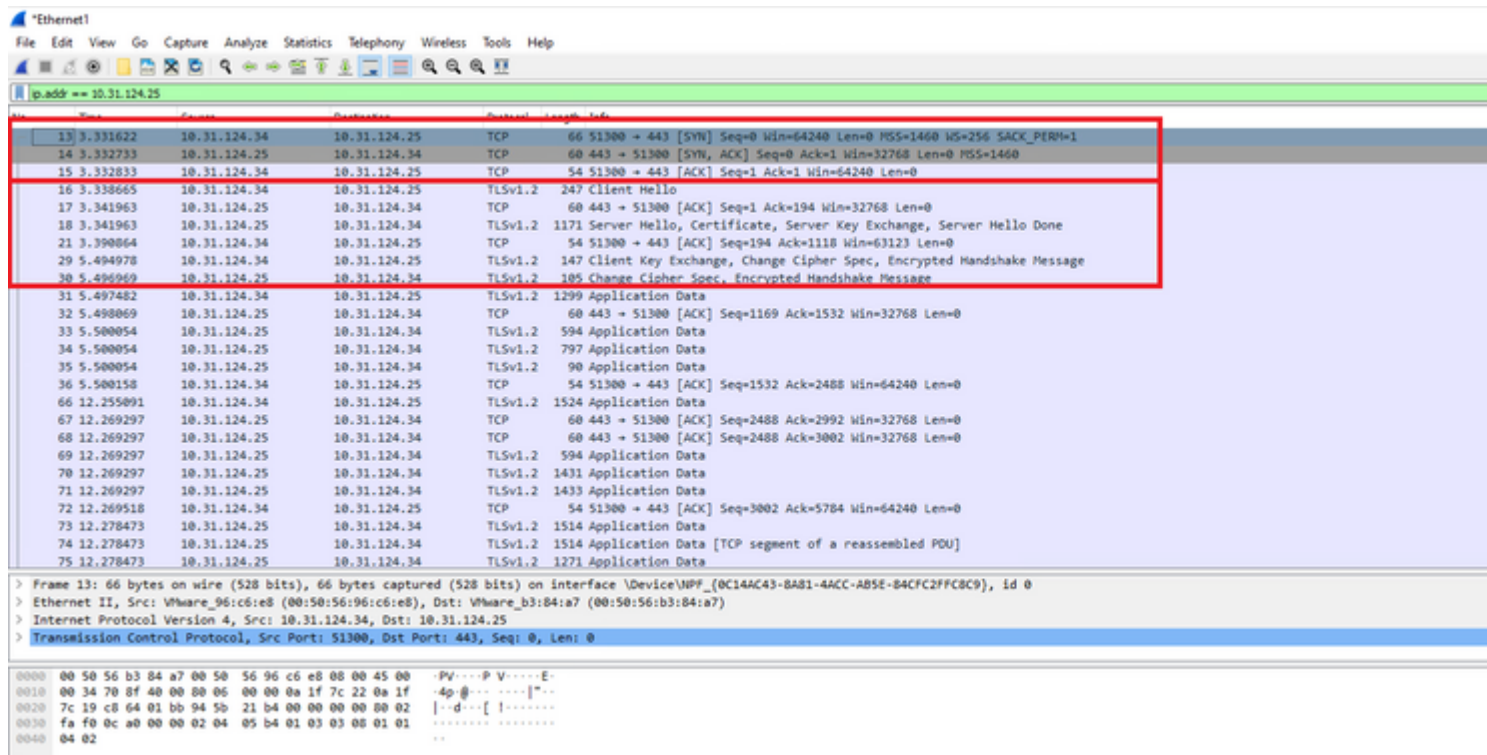
```

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).