Configure SSL Secure Client with Local Authentication on FTD

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
<u>Configure</u>
Configurations
Step 1. Verify Licensing
Step 2. Upload Cisco Secure ClientPackage to FMC
Step 3. Generate a Self-Signed Certificate
Step 4. Create Local Realm on FMC
Step 5. Configure SSL Cisco Secure Client
Verify
Troubleshoot

Introduction

This document describes how to configure Cisco Secure Client (includes Anyconnect) with local authentication on Cisco FTD managed by Cisco FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SSL Secure Client configuration through Firepower Management Center (FMC)
- Firepower objects configuration through FMC
- SSL certificates on Firepower

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In this example, Secure Sockets Layer (SSL) is used to create Virtual Private Network (VPN) between FTD and a Windows 10 client.

From release 7.0.0, FTD managed by FMC supports local authentication for Cisco Secure Clients. This can be defined as either the primary authentication method, or as fallback in case the primary method fails. In this example, local authentication is configured as the primary authentication.

Before this software version Cisco Secure Client local authentication on FTD was only available on Cisco Firepower Device Manager (FDM).

Configure

Configurations

Step 1. Verify Licensing

Before you configure Cisco Secure Client, FMC must be registered and be compliant with Smart Licensing Portal. You cannot deploy Cisco Secure Client if FTD does not have a valid Plus, Apex, or VPN Only license.

Navigate to **System > Licenses > Smart Licenses** in order to ensure that the FMC is registered and compliant to Smart Licensing Portal:

Overview Analysis Policies	Devices Objects AMP Intellige	nce					<u>.</u>	🄍 De	ploy System	Help 🔻 dp	erezve 🔻
		Configuration	Users Domains	Integration	SecureX	Updates	Licenses + Smart Licenses	Logging •	Health v	Monitoring •	Tools •
											i
Smart License Status		Cisco Sma	rt Software Manager	9							
Usage Authorization:	Authorized (Last Synchronized On Sep 04	2021)									
Product Registration:	Registered (Last Renewed On Sep 04 202))									
Assigned Virtual Account:	SEC TAC										
Export-Controlled Features:	Enabled										
Cisco Success Network:	Enabled (1)										
Cisco Support Diagnostics:	Disabled 0										

Scroll-down on the same page. On the bottom of the **Smart Licenses** chart, you can see the different types of Cisco Secure Client (AnyConnect) licenses available and the devices subscribed to each one. Ensure that the FTD at hand is registered under any of these categories:

Smart Licenses		Filter Devices	× Edit	Performance Tier	dit License
License Type/Device Name	License Status	Device Type	Domain	Group	
🛛 📁 Firepower Management Center Virtual (2)	0				
⊳ 📁 Base (2)	0				
🛛 🚰 Malware (2)	٥				
🗁 💋 Threat (2)	0				
> 💋 URL Filtering (2)	0				
a 💋 AnyConnect Apex (2)	٥				
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	٥	Cisco Firepower Threat Defense for VMWare	Global	N/A	
ftdvha-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMware - v7.0.0	0	Cisco Firepower Threat Defense for VMware	Global	N/A	
AnyConnect Plus (0)					
AnyConnect VPN Only (0)					
iote: Container Instances of same blade share feature licenses			Activate Wir Go to System in	idows Control Panel to activate	Windows.
st login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2					,ı C

Step 2. Upload Cisco Secure Client Package to FMC

Download the Cisco Secure Client (AnyConnect) Headend Deployment Package for Windows from <u>cisco.com</u>:

Application Programming Interface [API] (Windows) anyconnect-win-4.10.01075-vpnapi.zip Advisories	21-May-2021	141.72 MB	<u>+</u> \;
AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	77.81 MB	<u>+</u> \;
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	<u>+</u> \;
AnyConnect Headend Deployment Package (Windows 10 ARM64) anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	44.76 MB	<u>+</u> \;
Profile Editor (Windows) tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 📑	21-May-2021	10.90 MB	<u>+</u> \:/
AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip Advisories	21-May-2021	0.05 MB	<u>+</u> \;

To upload the Cisco Secure Client image, navigate to **Objects > Object Management** and choose **Cisco Secure Client File** under the **VPN** category in the table of contents:

Overview Analysis Polic	ies Devices	Objects	AMP Intelligence				$oldsymbol{\theta}_4$ Deploy Syste	m Help ▼	dperezve *
Object Management Intr	usion Rules								
AnyConnect File File objects represent files used in a	configurations, typ	sically for remo	te access VPN policies. They can contain A	AnyConnect Client Profile and	AnyConnect Client Image files.		Add AnyConnect File	🔍 Filter	
🛐 IPv6 Prefix List 📍	Name					Value	Туре		
🛞 Route Map	_								
4 🤿 Security Intelligence					No records to display				
DNS Lists and Feeds									
Network Lists and Feeds									
URL Lists and Feeds									
Sinkhole									
SLA Monitor									
Time Range									
🔊 Time Zone									
Cunnel Zone									
S Variable Set									
VLAN Tag									
A DVPN									
AnyConnect File									
R, Certificate Map									
Custom Attribute									
Group Policy									
(A) IKEv1 IPsec Proposal									
E IKEv1 Policy									
IKEv2 IPsec Proposal	1								
🚯 IKEv2 Policy	-						AcNo data to display/s K <		
							Go to System in Control Panel	to activate Win	
Last login on Friday, 2021-09-03 at 1	12:46:00 PM from 1	92.168.13.2							uluilu cisco

Click Add AnyConnect File. In the Add AnyConnect Secure Client File window, assign a name for the object, then choose Browse.. to pick the Cisco Secure Client package. Finally, select AnyConnect Client Image as the file type in the drop-down menu:

Overview Analysis Policies Devices Objects AMP Intellige	1969		
	ince		et aperezve +
Object Management Intrusion Rules			
AnyConnect File File objects represent files used in configurations, typically for remote access VPN policies	. They can contain AnyConnect Client Profile and AnyConnect Client Image files.		Add AnyConnect File
IPv6 Prefix List * Name		Value	Туре
@ Route Map			
A Security Intelligence	No records to display		
DNS Lists and Feeds	Add AnyConnect File	? ×	
Network Lists and Feeds			
URL Lists and Feeds	Name II		
Sinkhole	Name:* AnyConnect_Win_4.10		
Gian SLA Monitor	File Name:" anyconnect-win-4.10.01075-webdeploy-k9.p Browse		
Time Range			
🗿 Time Zone	File Type: * AnyConnect Client Image	~	
A Tunnel Zone		5	
O URL	Description:		
S Variable Set		-	
A B VPN			
AnyConnect File	Save	Cancel	
R [°] Certificate Map			
Custom Attribute			
Group Policy			
() IKEV1 IPsec Proposal			
B IKEV1 Policy			
(§ IKEv2 IPsec Proposal			
B IKEv2 Policy			A cities No data to display S IK is Page 1 of 1 > > I C
			Go to System in Control Panel Yo activate Windows
			··II··II·· cisco

Click Save. The object must be added to objects list:

Overview Analysis Policies Devices Objects AMP Intelligence		. Deploy System Help ▼	dperezve v
Object Management Intrusion Rules			
AnyConnect File File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.		Add AnyConnect File	
Mane	Value	Туре	
Port AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	AnyConnect Client Image	2/8
Prefix List AnyConnect_Win_4.10 Dr4 Prefix List	anyconnectranity. 10.01073-webdeptoy-k5.pkg	AnyConnect Crent Image	x / 0
Compared Prefer List			
@ Route Map			
■ Security Intelligence			
DNS Lists and Feeds			
Pletwork Lists and Feeds			
URL Lists and Feeds			
Sinkhole			
da SLA Monitor			
a Time Range			
a Time Zone			
Turnel Zone Will			
© Und. S. Variable Set			
VILLAN TAG			
- B. VPN			
AnyConnect File			
R ² Certificate Map			
® Custom Attribute			
E Group Policy			
(g) IKEV1 IPsec Proposal			
B IKEVI Policy			
🛞 IKEV2 IPsec Proposal			
C IXEV2 Policy	Ac	Bisplaying 10104 Fows K < Page 1	of 1 > > C
	Go	to System in Control Panel to activate Wind	lows.
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192:166.13.2			.ili.ili. cisco

Step 3. Generate a Self-Signed Certificate

Objects

SSL Cisco Secure Client (AnyConnect) requires one valid certificate to be used in the SSL handshake between VPN headend and client.

Note: In this example, a self-signed certificate is generated for this purpose. In addition, aside from self-signed certificates, it is possible to upload a certificate signed by either an internal Certificate Authority (CA) or a well-known CA too.

Help v dperez

To create the self-signed certificate, navigate to **Devices > Certificates**.

Click Add. Then choose the FTD listed in the Device drop-down menu in the Add New Certificate

window.

Overview Analysis Policies Devices Objects AMP Inte	lligence	🍳 Deploy System Help 🔻 dperezve 🔻
Device Management Device Upgrade NAT VPN ¥ QoS F	latform Settings FlexConfig Certificates	
		bh S
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*: ftdvha-dperezve 👻	
	Cert Enrollment*: Select a certificate entrollment object	
	Add Cancel	
		Activate Windows
4		Contra divisional a discontra la Constala Constala constala di substanza di segunaria di segunaria di segunaria
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		۰۱ ۱۰۱ ۱۰ داsco

Click the Add Cert Enrollment button (green + symbol) to create a new enrollment object. Now, in the Add Cert Enrollment window, assign a name for the object and select Self Signed Certificate from the Enrollment Type drop-down menu.

Overview Analysis Policies Devices Objects AMP	Intelligence	
Device Management Device Upgrade NAT VPN ¥ Qot	Platform Settings FlexConfig Certificates	
	Add Cert Enrollment	? ×
Name Domain	Name* SSL_SelfSigned	
	Description	
	CA Information Certificate Parameters Key Revocation	
	Enrollment Type: Self Signed Certificate	
	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.	re
	Allow Overrides	
	Save Cano	cel Activate Windows
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		Go to system in Control Panel to activate Windows

Finally, for self-signed certificates, it is mandatory to have a Common Name (CN). Navigate to the **Certificate Parameters** tab to define a CN:

Overview Analysis Policies Devices Objects	AMP Intelligence			●, Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN •		exConfig Certificates		
	Add Cert Enrollment		? ×	Add I
Name Don	ain Name*	SSL_SelfSigned		
	Description			
	CA Information Cert	ificate Parameters Key Revocation		
	Include FQDN:	Don't use FQDN in certificate	~	
	Include Device's IP Addres	s:		
	Common Name (CN):	dperezve.local		
	Organization Unit (OU):			
	Organization (O):			
	Locality (L):			
	State (ST):			
	Country Code (C):	Comma separated country codes		
	Email (E):			
	Include Device's Serial N	lumber		
		-		
	Allow Overrides			
		6		
			Save Cancel	Activate Windows
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				Go to System in Control Panel to activate Windows

Click the **Save** and **Add** buttons. After a couple of seconds, the new certificate must be added to the certificate list:

Overview Analysis	Policies Dev	ices 0	bjects	AMP	Intelligence			0 ₄ Deploy System Help	• dperezve •
Device Management	Device Upgrade	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates		
									Add
Name			Don	nain	Enrollment	Type 5	itatus		
4 🗐 ftdvha-dperezve								<u> ۵</u>	
SSL_SelfSigned			Glob	bal	Self-Signed		🤤 CA 🔍 ID	ی 🕭	Φ 🖩

Step 4. Create Local Realm on FMC

The local user database and the respective passwords are stored in a local realm. To create the local realm, navigate to **System > Integration > Realms**:



Choose the Add Realm button. In the Add New Realm window, assign a name and choose LOCAL option in the Type drop-down menu:

Overview Analysis Policies Devices Objects AMP In	ntelligence				Help 🔻 dp	
	Add New Realm	e .	× Licenses •	Logging Health	Monitoring 💌	Tools 🔻
Cloud Services Realms Identity Sources High Av Realms Realm Sequences Sync Results	Add New Realm Name" AnyConnect-Local-Auth Type Local Local User Configuration Vsemame Password Local user	Confirm Password	× Ucenses •		Monitoring •	
		Cancel Save		Activate Windows Go to System in Control Panel to	activate Window	
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2						altalta

User accounts and passwords are created in the Local User Configuration section.

Note: Passwords must have at least one upper case letter, one lower case letter, one number and one special character.

Overview Analysis Policies Devices Objects AMP	ntelligence				🔍 Deploy	System Help v	dperezve v
	Add New Realm		θ×	Licenses 🔻	Logging • H	fealth Monitoring	 Tools
Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results	Add New Realm Name* AnyConnect-Local-Auth Type LoCAL V Local User Configuration Operezve Username Operezve Paseword Add another local user	Confirm Password	• ×	Licenses •	Logging • •	tealth Monitoring Compare Realms	
		Cancel	Save				
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2							

Save changes, then click Add Realm to add a new realm to the existing realms list.

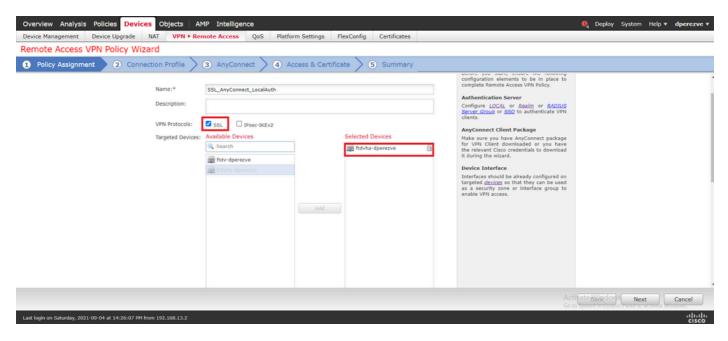
verview Analys	sis Policies Devices Objects	AMP Intelligence									🔒 Depi	y Syster	n Help 🔻	dperezve 1
				Configuration	Users	Domains	Integration	SecureX	Updates	Licenses •	Logging •	Health 🔻	Monitoring	 Tools
Cloud Services	Realms Identity Sources	High Availability eStreame	Host Input Client	Smart Software Mar	nager On	-Prem								
Realms R	tealm Sequences Sync Results													
												Compar	e Realms	Add Realm
Name +	Description	Туре	Domain	AD Primary	Domain		B	ase DN				State		
AnyConnect-Local	Auth	LOCAL	Global									Enable	id 🛓	/ 5 🕯

Step 5. Configure SSL Cisco Secure Client

To configure SSL Cisco Secure Client, navigate to **Devices > VPN > Remote Access**:



Click **Add** in order to create a new VPN policy. Define a name for the connection profile, select SSL checkbox, and choose the FTD listed as the targeted device. Everything must be configured in the **Policy Assignent** section in the **Remote Access VPN Policy Wizard**:



Click **Next** in order to move to the **Connection Profile** configuration. Define a name for the connection profile and choose **AAA Only** as the authentication method. Then, in the **Authentication Server** drop-down menu, choose **LOCAL**, and finally, choose the local realm created in Step 4 in the **Local Realm** drop-down menu:

Overview Analysis Policies Devices Objects AMP Intelligence	🧕 Deploy System He	lp v dperezve v
Device Management Device Upgrade NAT VPN + Remote Access QoS Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard		
Policy Assignment O Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary		
Remote User AnyConnect Client Outside Corporate Resources		
Connection Profile:		
Connection refiles 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 VPW 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 V (LOCAL or Realm or RADIUS)		
Local Realm:* AnyConnect-Local-Auth 🗸 🖉		
Authorization Server: Calumor RADIUS)		
Accounting Server:		
	Activate Back dows Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		uluitu cisco

Scroll down on the same page, then click the pencil icon in the **IPv4 Address Pool** section in order to define the IP pool used by Cisco Secure Clients:

Overview Analysis Policies Devices Objects AMP Inte	lligence	🧕 Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN > Remote Act	ess QoS Platform Settings FlexConfig Certificates	
Remote Access VPN Policy Wizard		
Policy Assignment 2 Connection Profile 3 Any	Connect > ④ Access & Certificate > ⑤ Summary	
Auther	tication Server:* LOCAL V (LOCAL or Realm or RADIUS)	· · · · · · · · · · · · · · · · · · ·
Author Client Addree Client Baddre assignment is Use Use Use	Address Pools ? × Available IPv4 Pools C Selected IPv4 Pools Search Search Add A	
Group Policy A group policy or create a G Group	ed. Select	
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192,168.13.2		Back Next Cancel

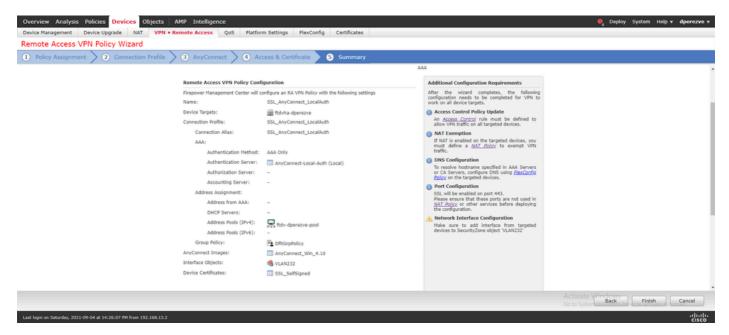
Click **Next** in order to move to the **AnyConnect** section. Now, select the Cisco Secure Client image uploaded in Step 2:

Overview Analysis Policies Devices Objects AMP Intelligence	🌒 Deploy System Help 🔻	dperezve *
Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard		
Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary		
Remote User AnyConnect Client Outside User Corporate Resources		Â
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.		I
Download AnyConnect Client packages from <u>Cisco Software Download Center</u> . Show Re-order buttons		
AnyConnect File Object Name AnyConnect Client Package Name Operating System		
AnyConnect_Win_4.10 anyconnect-win-4.10.01075-webdeploy-k9.pkg Windows		
	Activate Back don's Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		uluilu cisco

Click **Next** in order to move to the **Access & Certificate** section. In the **Interface group/Security Zone** drop-down menu, choose the interface where Cisco Secure Client (AnyConnect) needs to be enabled. Then, in the **Certificate Enrollment** drop-down menu, choose the certificate created in Step 3:

Overview Analysis Policies Devices Objects AMP Intelligence	🔍 Deploy System F	tele a deservo a
	💘 Deploy System r	ieip • aperezve •
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 Outside Outside Corporate Resources		ĺ
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:* VLAN232		
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:* SSL_SelfSigned 🗸 🖉		
	Activate Backdov's Next Go to System Control Part to act	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		-ili-ili- cisco

Finally, click Next to see a summary of the Cisco Secure Client configuration:



If all the settings are correct, click Finish and deploy the changes to FTD.

view Analysis Policies Devices	Objects AMP Intelligence					0₄ Deploy System Help v dpe
						Deployment Deploymen
						t device extended
						1 device selected Deploy time: Estimate
 Search using device name, user na 						
Device	Modified by	Inspect Interruption	Type Group	Last Deploy Time	Preview	Status
ftdvha-dperezve	dperezve		FTD	Sep 7, 2021 2:44 PM	8.	Pending
					Activate V	Vindows 1 in Control Panel to activate Windows.

Verify

ay, 2021-09-04 at 14:26:07 PM fr

After deployment has been successful, initiate a Cisco AnyConnect Secure Mobility Client connection from Windows client to FTD. The username and password used in the authentication prompt must be the same as created in Step 4:

uluilu cisco

	VPN:
	S Cisco AnyConnect 10.31.124.25 ×
	Group: SSL_AnyConnect_LocalAuth ~
¢ i	Username: dperezve
	Password: *********

After credentials are approved by FTD, Cisco AnyConnect Secure Mobility Client app must display connected state:

🕥 Cisco AnyC	Connect Secure Mobility Client		—		×
	VPN: Connected to 10.31.124.25. 10.31.124.25	~	D	isconnect	
00:00:49				I	IPv4
Q ()					alialia cisco

From FTD, you can run **show vpn-sessiondb anyconnect** command in order to display the Cisco Secure Client sessions currently active on the 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
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Premium
          : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Encryption
          : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
           : 15756
                                    Bytes Rx : 14606
Bytes Tx
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time : 21:42:33 UTC Tue Sep 7 2021
            : 0h:00m:30s
Duration
           : 0h:00m:00s
Inactivity
VLAN Mapping : N/A
                                    VLAN
                                                 : none
Audt Sess ID : 0000000000080006137dcc9
                                   Tunnel Zone : 0
Security Grp : none
```

Troubleshoot

Run debug webvpn anyconnect 255 command on FTD in order to see SSL connection flow on FTD:

Besides Cisco Secure Client debugs, connection flow can observed with TCP packet captures as well. This is an example of a successful connection, a regular three handshake between Windows client and FTD is completed, followed by a SSL handshake used to agree ciphers.

	5	0	Annual London Tab	×
13 3.331622	10.31.124.34	10.31.124.25	TCP 66 51300 + 443 [SYN] Seq=0 Hin=64240 Len=0 PSS=1460 HS=256 SACK P[RH=1	
14 3.332733	10.31.124.25	10.31.124.34	TCP 60 443 + 51300 [511] 2000 ALTO COMP A DECEMBER 105205 300 ACC 1 100 5251 460	
15 3,332833	10,31,124,34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
16 3.338665	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 kin=32768 Len=0	
18 3.341963	10.31.124.25	10.31.124.34	TLSv1.2 1171 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
21 3.390864	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seg=194 Ack=1118 Win=63123 Len=0	
29 5.494978	10.31.124.34	10.31.124.25	TLSv1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
30 5.496969	10.31.124.25	10.31.124.34	TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message	
31 5.497482	10.31.124.34	10.31.124.25	TLSv1.2 1299 Application Data	
32 5.498869	10.31.124.25	10.31.124.34	TCP 60 443 + 51300 [ACK] Seq=1169 Ack=1532 Win=32768 Len=0	
33 5,500054	10.31.124.25	10.31.124.34	TLSv1.2 594 Application Data	
34 5.500054	10.31.124.25	10.31.124.34	TLSv1.2 797 Application Data	
35 5.500054	10.31.124.25	10.31.124.34	TLSv1.2 90 Application Data	
36 5.500158	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq=1532 Ack=2488 Win=64240 Len=0	
66 12.255091	10.31.124.34	10.31.124.25	TLSv1.2 1524 Application Data	
67 12.269297	10.31.124.25	10.31.124.34	TCP 60 443 * 51300 [ACK] Seq=2488 Ack=2992 Win=32768 Len=0	
68 12.269297	10.31.124.25	10.31.124.34	TCP 60 443 → 51300 [ACK] Seq=2488 Ack=3002 Win=32768 Len+0	
69 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 594 Application Data	
70 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 1431 Application Data	
71 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 1433 Application Data	
72 12.269518	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq=3002 Ack=5784 Win=64240 Len=0	
73 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1514 Application Data	
74 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1514 Application Data [TCP segment of a reassembled PDU]	
75 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1271 Application Data	

After protocol handshakes, FTD must validate the credentials with the information stored in local realm.

Collect the DART bundle and contact Cisco TAC for further research.