

Configure SSL Secure Client with Local Authentication on FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configurations](#)

[Step 1. Verify Licensing](#)

[Step 2. Upload Cisco Secure Client Package to FMC](#)

[Step 3. Generate 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, the FMC must be registered, and be compliant to 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 validate the FMC is registered and compliant to 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. Below this, there are tabs for Configuration, Users, Domains, Integration, SecureX, Updates, and Licenses > Smart Licenses. The main content area is titled "Smart License Status" and includes a link to "Cisco Smart Software Manager". The status is summarized in a table:

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 ⓘ

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. Validate the FTD at hand is registered under any of these categories.

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

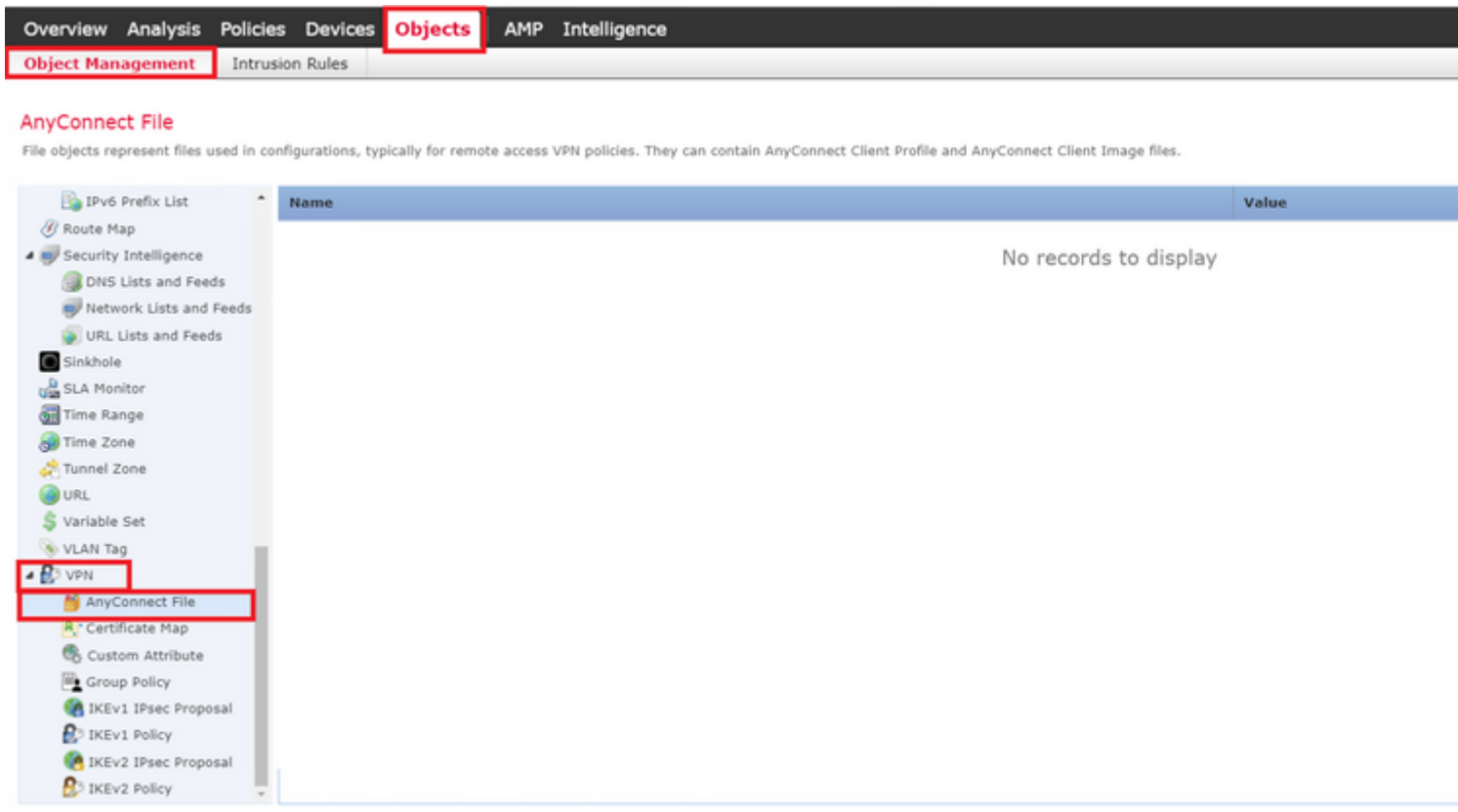
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Step 2. Upload Cisco Secure Client Package to FMC

Download the Cisco Secure Client (AnyConnect) Headend Deployment Package for Windows from [cisco.com](https://www.cisco.com).

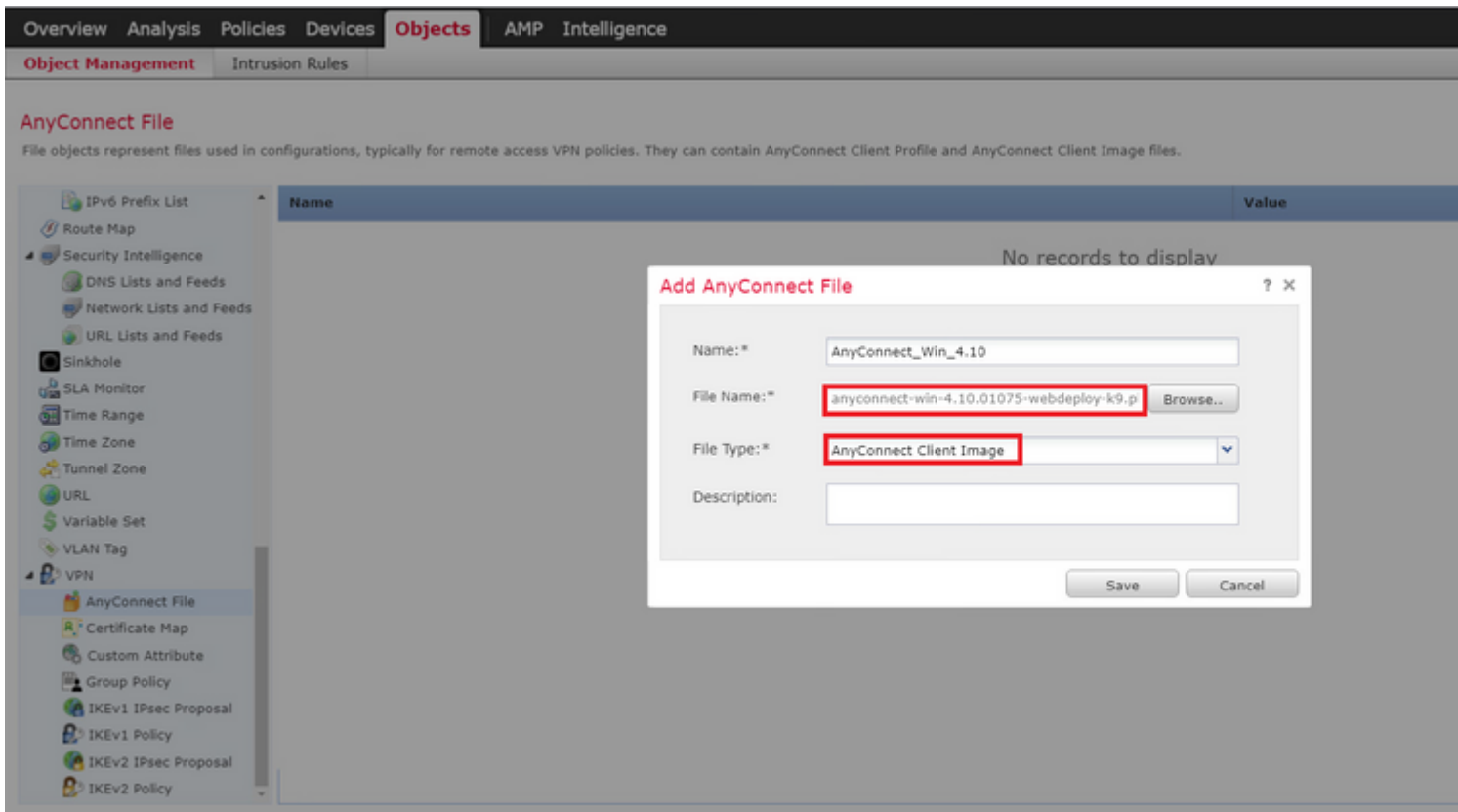
Application Programming Interface [API] (Windows)  anyconnect-win-4.10.01075-vpnapi.zip Advisories 	21-May-2021	141.72 MB
AnyConnect Headend Deployment Package (Windows)  anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	77.81 MB
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - 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

In order 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.



Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2

Choose the **Add AnyConnect File** button. In the **Add AnyConnect Secure Client File** window assign a name for the object, then choose **Browse..** in order to pick the Cisco Secure Client package and finally choose **AnyConnect Client Image** as the file type in the drop-down menu.



Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2

Choose **Save** button. The object must be added to objects list.

Overview Analysis Policies Devices **Objects** AMP Intelligence

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.

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

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

Step 3. Generate Self-Signed Certificate

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

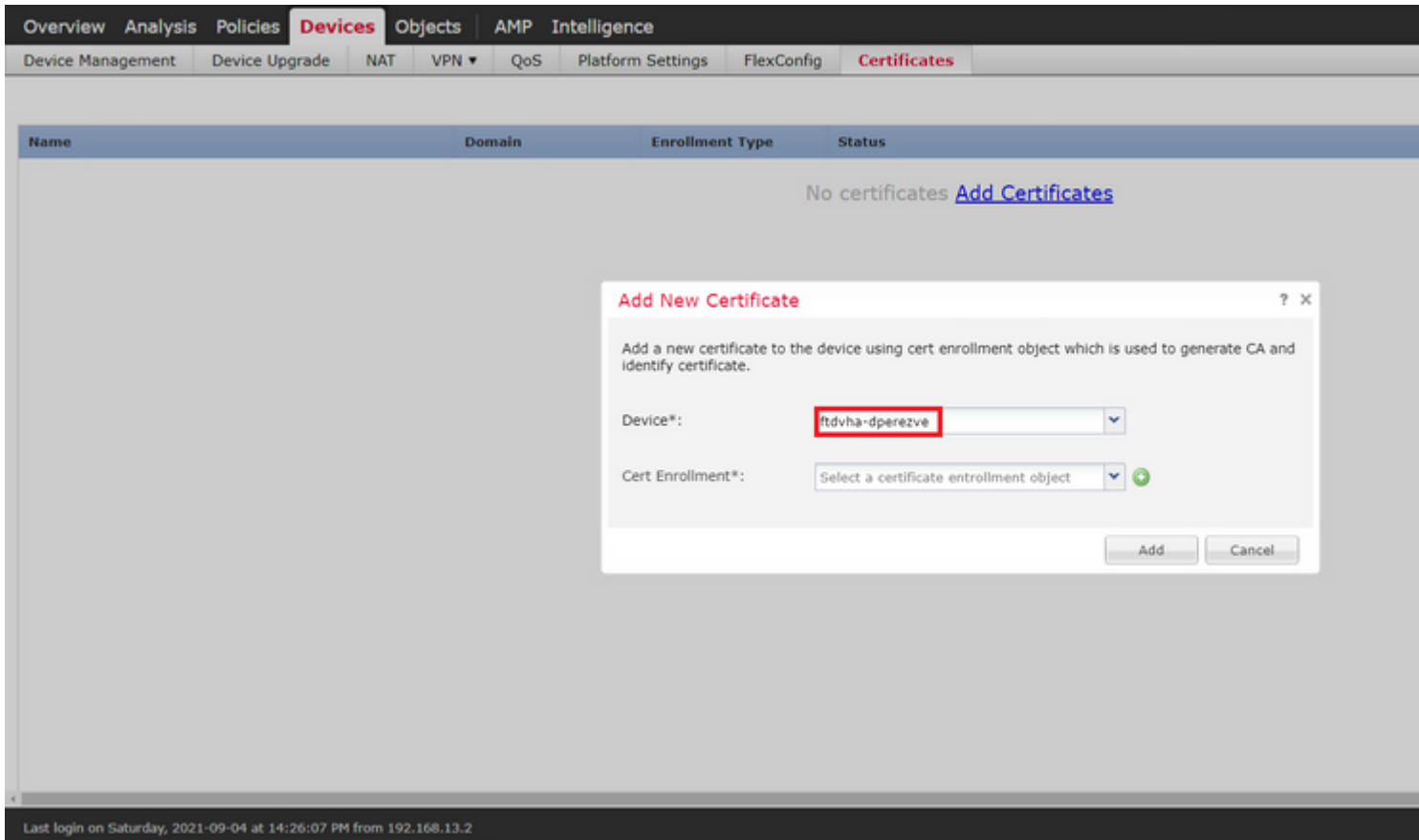
Note: In this example, a self-signed certificate is generated for this purpose. However, besides self-signed certificates, it is possible to upload a certificate signed by either an internal Certificate Authority (CA) or a well-known CA too.

In order to create the self-signed certificate navigate to **Devices > Certificates**.

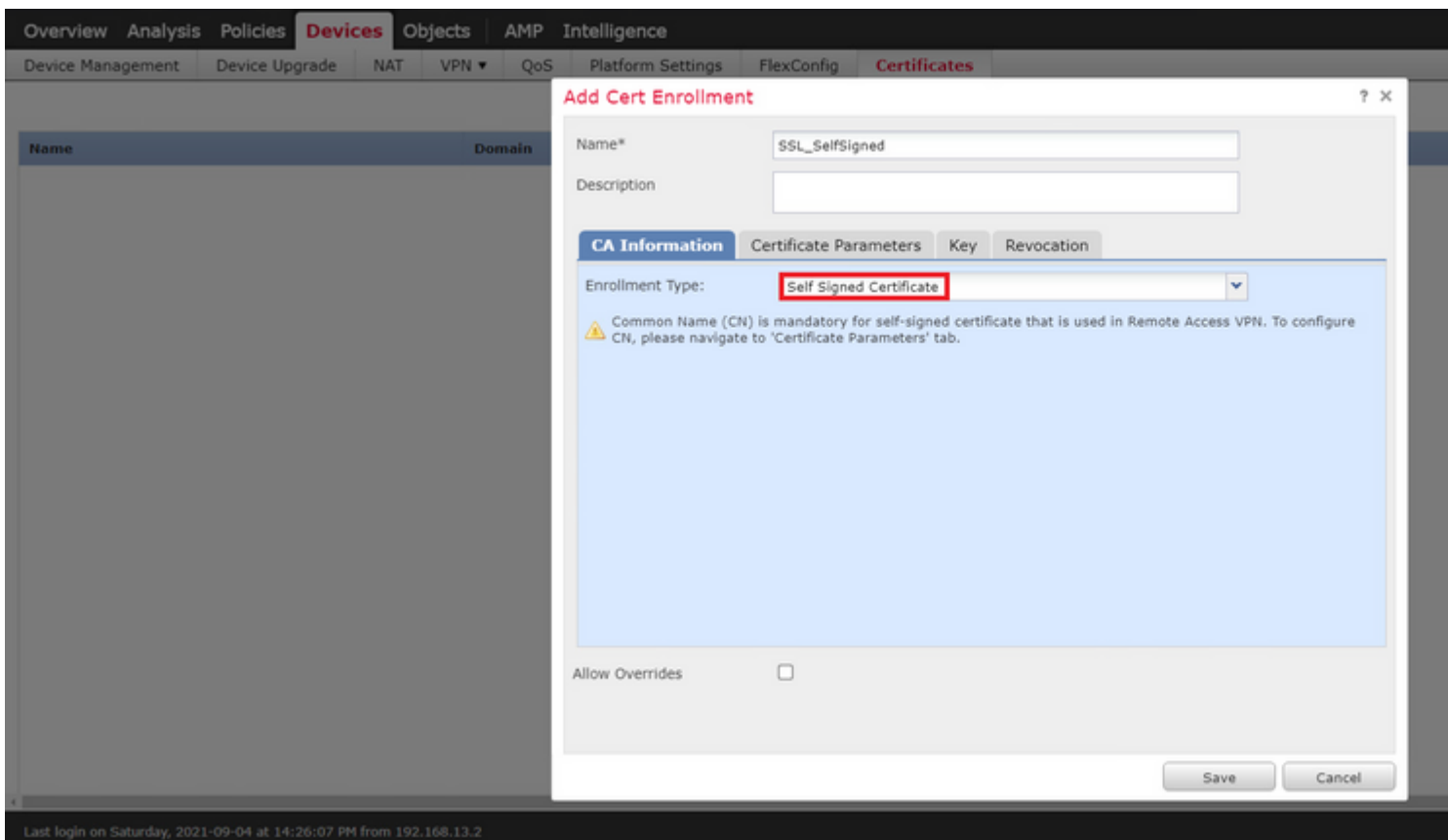
Overview Analysis Policies **Devices** Objects AMP Intelligence

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

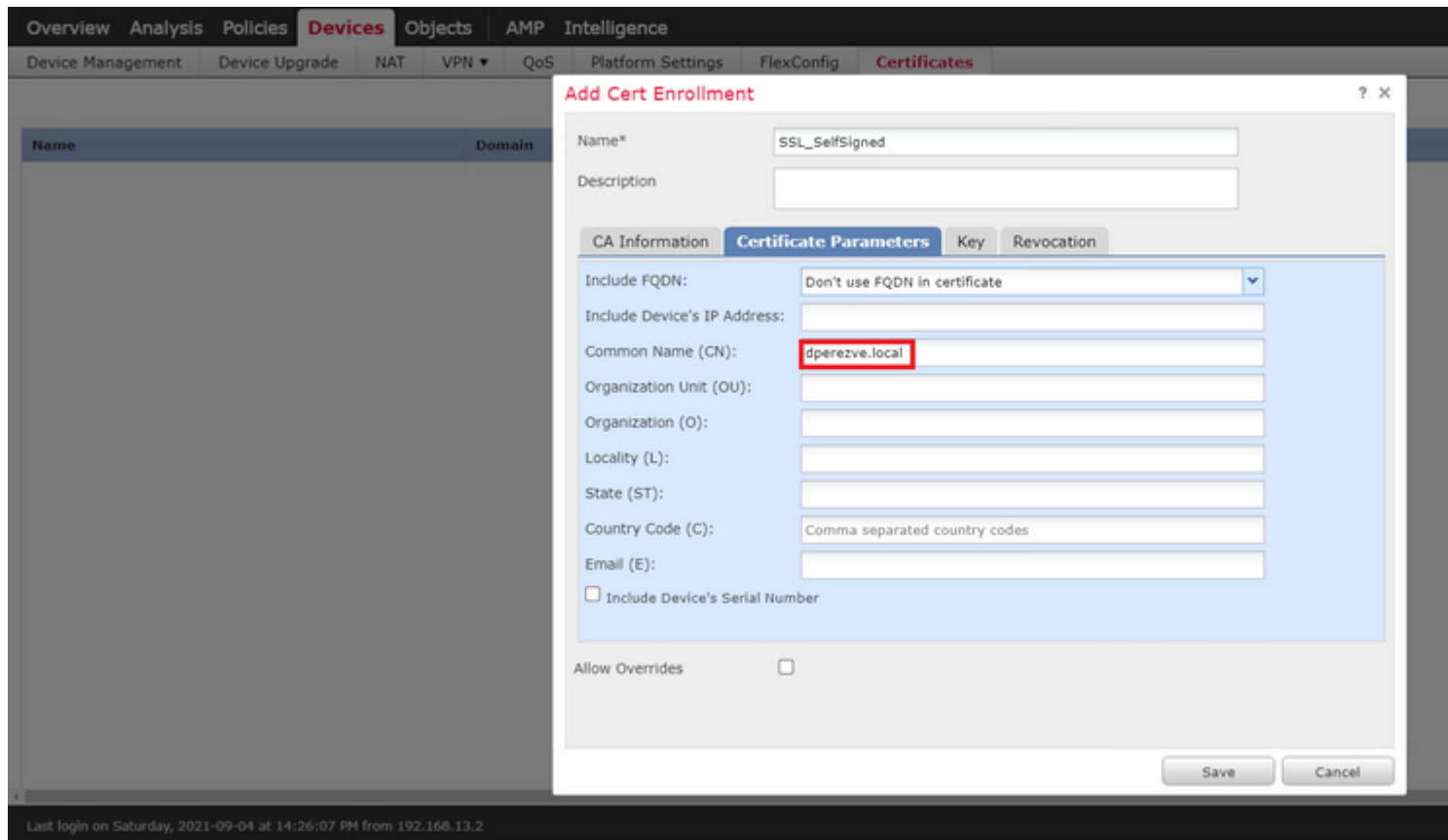
Choose the **Add** button. Then choose the FTD at hand in the **Device** drop-down menu in the **Add New Certificate** window.



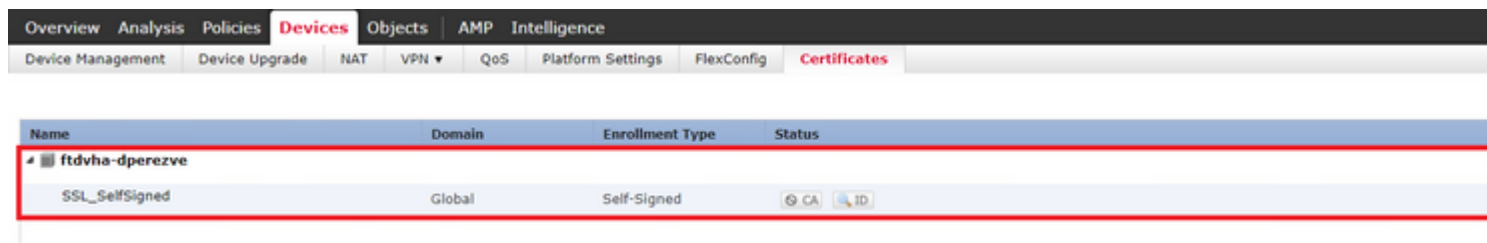
Choose the **Add Cert Enrollment** button (green + symbol) to create a new enrollment object. Now, in the **Add Cert Enrollment** window, assign a name for the object and choose **Self Signed Certificate** in the **Enrollment Type** drop-down menu.



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

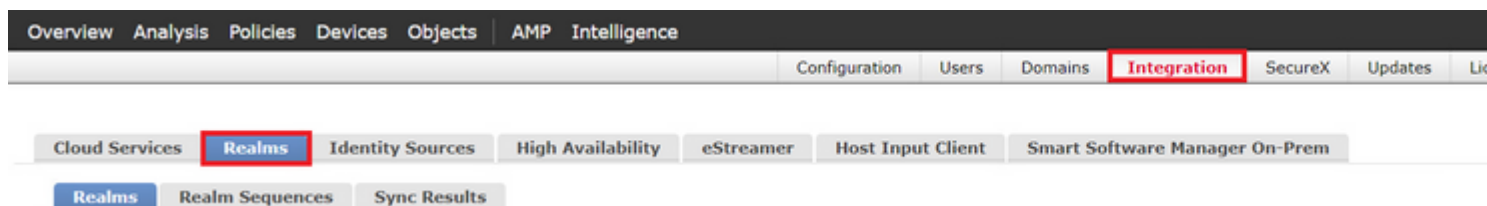


Choose **Save** and **Add** buttons. After a couple of seconds, the new certificate must be added to the certificate list.

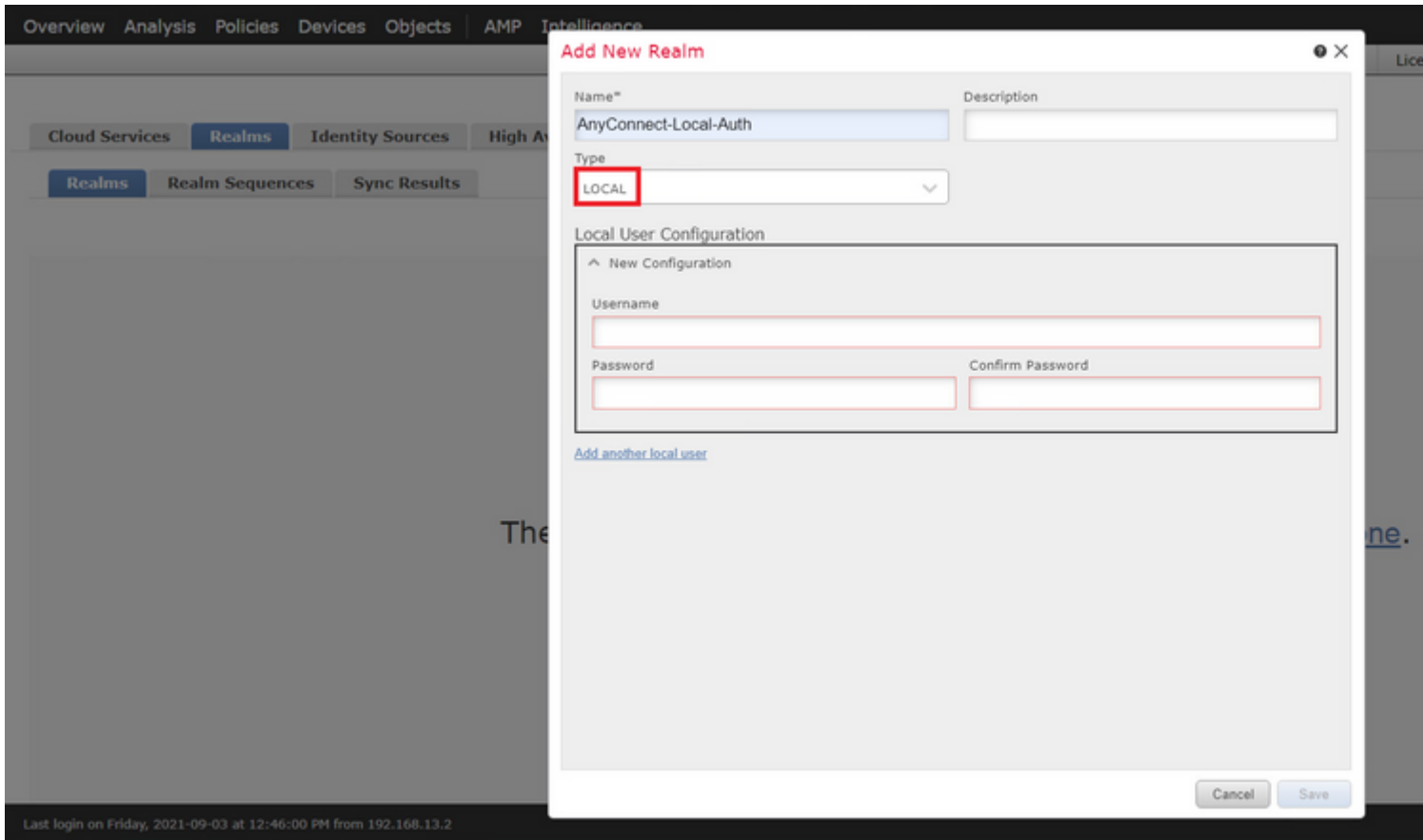


Step 4. Create Local Realm on FMC

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

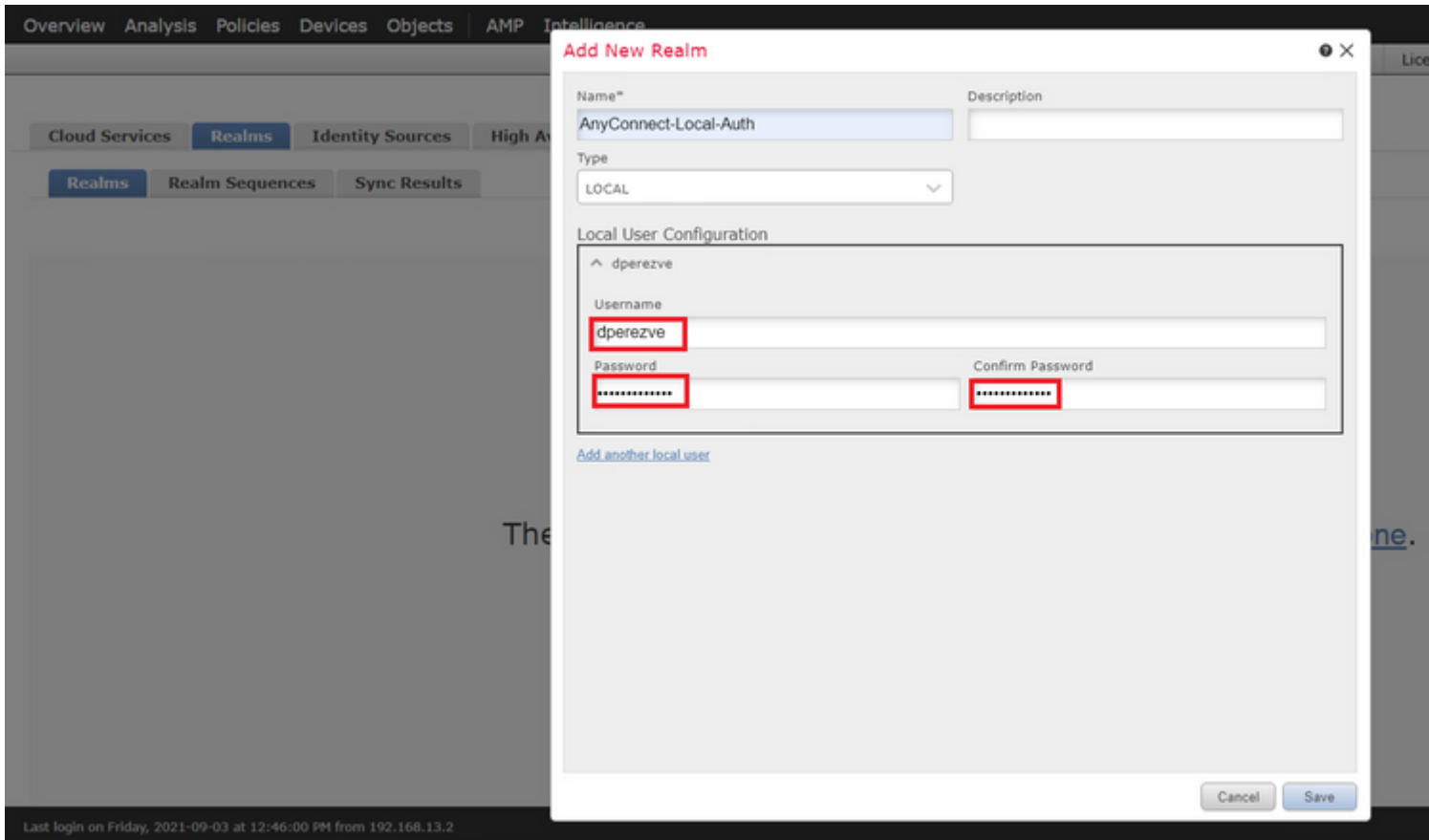


Choose the **Add Realm** button. In the **Add New Realm** window, assign a name and choose **LOCAL** option in the **Type** drop-down menu.

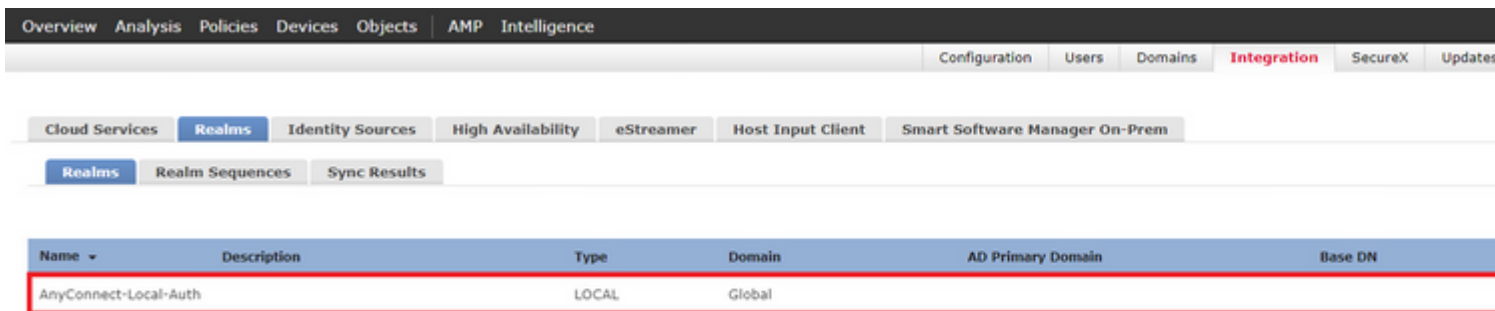


User accounts and passwords are created in the Local User Configuration section.

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



Save changes and new realm must be added to existing realms list.



Step 5. Configure SSL Cisco Secure Client

In order to configure SSL Cisco Secure Client, navigate to **Devices > VPN > Remote Access**.



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

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: *

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

- 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 on 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

Choose **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

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

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: *
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 or Realm or RADIUS)

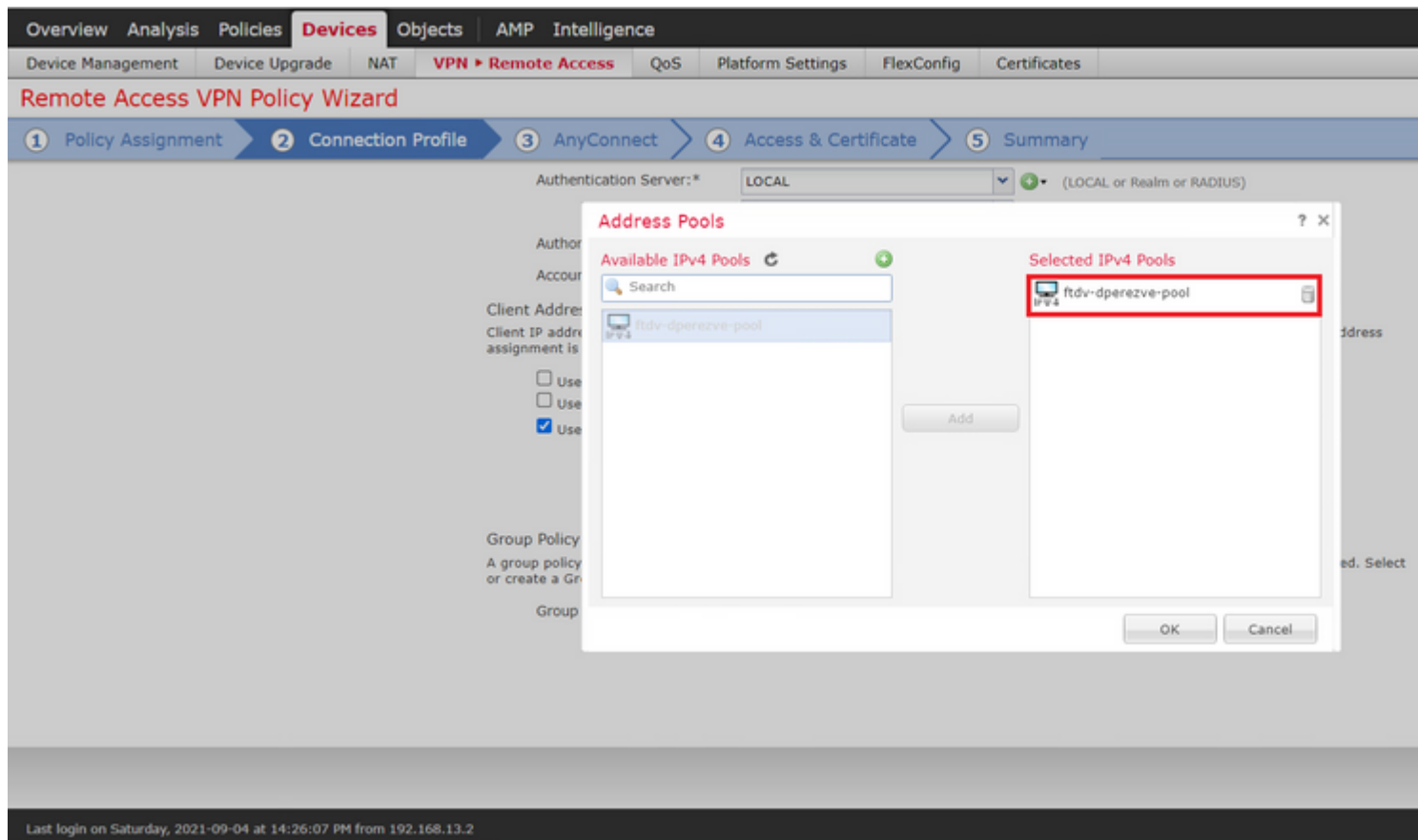
Local Realm: * (AnyConnect-Local-Auth)

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

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



Choose **Next** in order to move to the **AnyConnect** section. Now, choose the Cisco Secure Client image uploaded in Step 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

Choose **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

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

Finally, choose **Next** in order to see a summary of the Cisco Secure Client configuration.

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

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

Overview Analysis Policies Devices Objects AMP Intelligence

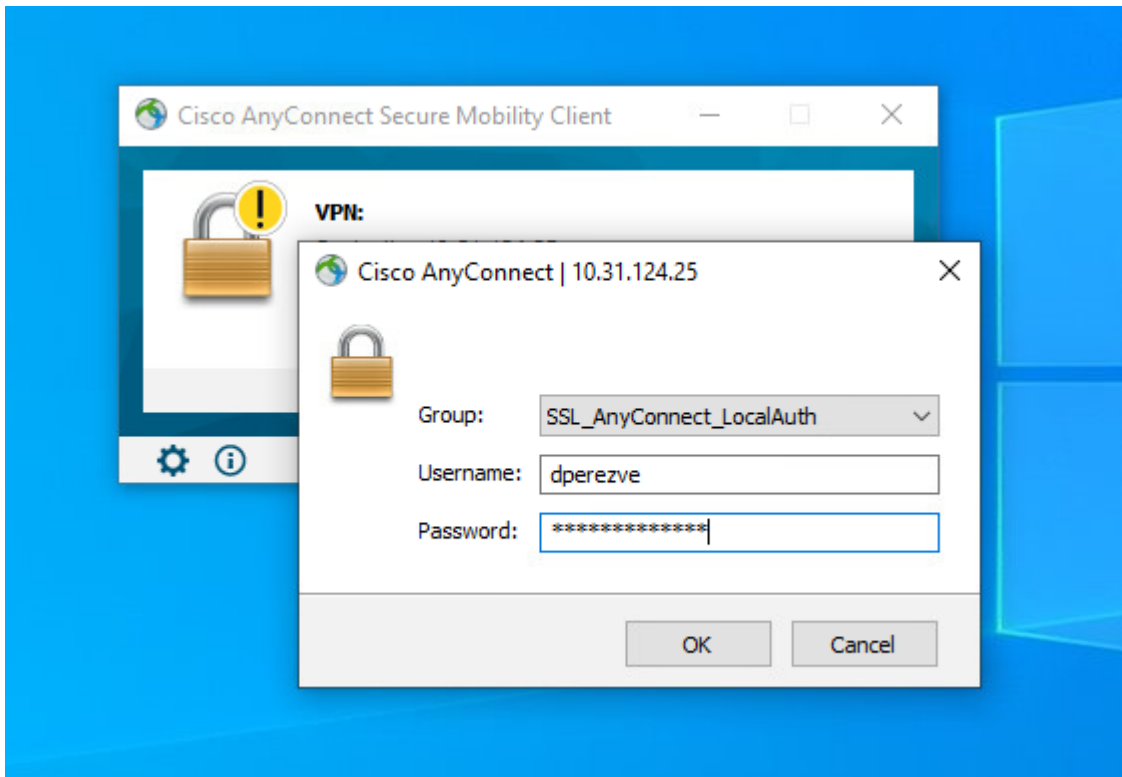
Search using device name, user name, type, group or status

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

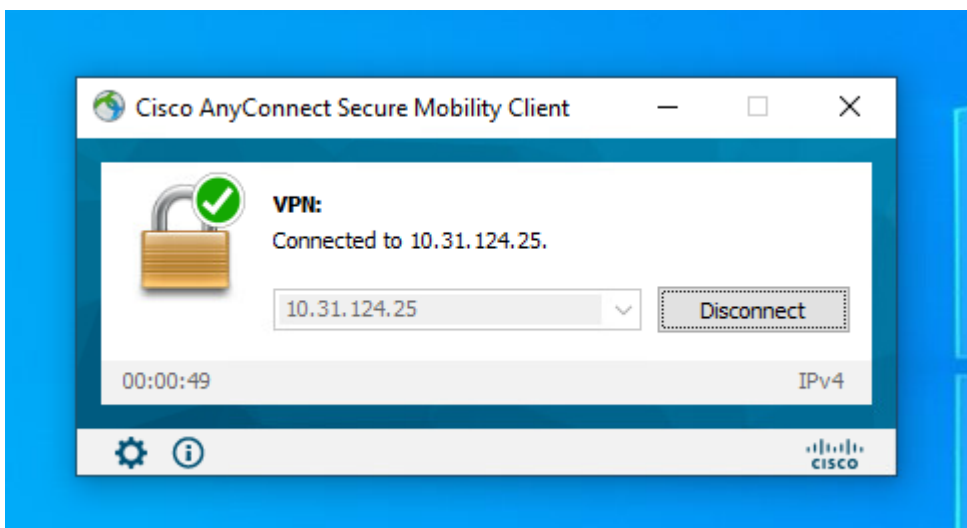
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Verify

Once 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.



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



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
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

```

Troubleshoot

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

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

Besides Cisco Secure Client debugs, connection flow can be 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.

The screenshot shows a Wireshark capture of network traffic on the Ethernet interface. The filter is set to 'ip.addr == 10.31.124.25'. A red box highlights the initial three-way handshake and the start of the SSL/TLS handshake:

- 13: 3.331622 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
- 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 Win=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] Seq=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 TLSv1.2 185 Change Cipher Spec, Encrypted Handshake Message

Below the highlighted packets, the details pane shows the structure of the captured frames, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. At the bottom, the raw packet bytes are displayed in hexadecimal and ASCII.

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

Collect DART bundle and contact Cisco TAC for further research.