

ةقداصملا مادختساب نمآلا SSL ليمع نيوكت ةقداصملا فTD لة نيوكت

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[تانوكتلا](#)

[صيخرتلا نم ققحتلا 1. ةوطخلا](#)

[FMC لة Cisco Secure Client Package لة ممت. 2. ةوطخلا](#)

[ايتا ةقوم ةداهش ءاش. 3. ةوطخلا](#)

[FMC لة ممت قاطن ءاش. 4. ةوطخلا](#)

[SSL Cisco Secure Client نيوكت. 5. ةوطخلا](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او ءاطخألا فاشكتسا](#)

ةمدقملا

مادختساب (AnyConnect نمضتي) نمآلا Cisco ليمع نيوكت ةيفيكن دنتمسلا اذه فصوي
Cisco FMC ةطساوب اهترادا ممتت يةلا Cisco FTD لة نيوكت ةقداصملا

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت:

- FirePOWER (FMC) ةرادا زكرم لالخن نم نمآلا SSL ليمع نيوكت
- FMC لالخن نم Firepower تانئاك نيوكت
- Firepower لة SSL تاداهش

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربل تارادصا لة دنتمسلا اذه في ةدراولا تامولعملا دنتمست:

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

ةصاخ ةي لم عم ةئيب يف ةدوجوم ل ةزهجال نم دنتسمل اذ يف ةدراول تامولعمل عاشنإ م تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذ يف ةمدختسمل ةزهجال عيمج تادب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف ، ليغشتلا ديقتك تكبش

ةيساسأ تامولعم

ةصاخلا ةكبشلا عاشنإل (SSL) ةنمأل ليصوتلا ذخأم ةقبط مادختسإ متي ، لاثملا اذ يف 10 Windows لي م و FTD ني (VPN) ةيرهظلا

ةيلحمل ةقداصم ل FMC ةطساوب هترادإ متت يذلا FTD لوكوتورب معددي ، 7.0.0 رادصلإ نم ةي طايح | ةقيرطك وأ ةيساسأ ةقداصم ةقيرطك اذ يف رعت نكميو . ني نمل آل Cisco ءالم عمل ةيلحمل ةقداصم ل نيوكب متي ، لاثملا اذ يف . ةيساسأ ل ةقيرطلا لشف ءلا يف ةيساسأ ةقداصم ك

طقف اجاتم FTD ل Cisco Secure Client Local Authentication اذ جم انربل رادصلإ نوكي نأ لبق Cisco Firepower Device Manager (FDM) ل

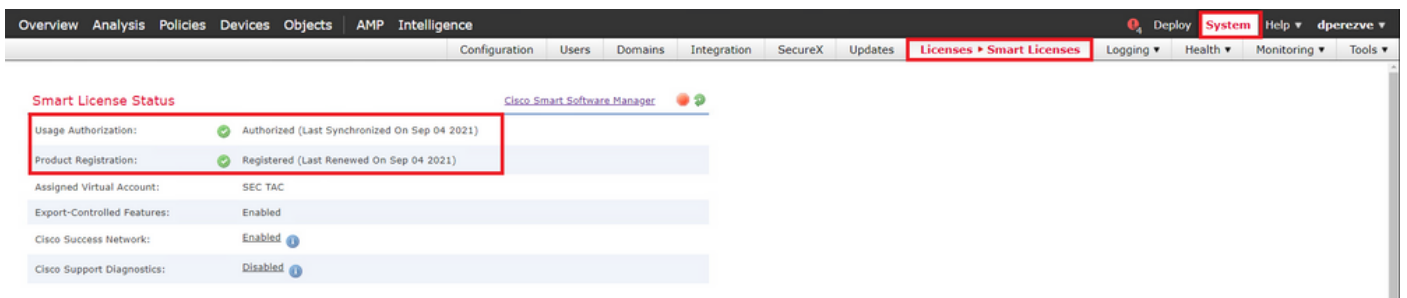
نيوكتل

تان نيوكتل

صخي رتل نم ققحتلا 1. ةوطخلا

صخي رتل لخدم عم ةقفاوتم نيوكب نأو ، FMC لي جست بجي ، Cisco Secure Client نيوكب لبق VPN أو APEX أو PLUS صخي رتل FTD ل نكي مل اذا Cisco Secure Client رشن كنكمي ال . ي كذلا طقف حلص

ةرادإ يف مكحتلا ةدحو نأ نم ققحتلل ةي كذلا صخي رتل > صخي رتل > ماظنلا ل لقتنا ي كذلا صخي رتل لخدم عم ةقفاوتم ءل جسم (FMC) تاراطلا



كنكمي ةي كذلا صخي رتل ل ططخم لفسأ يف ، ءحفصلال سفن لفسأل ريرم تلاب مق ةزهجال او ةرفوتم ل (AnyConnect) نم آل Cisco لي مع صخي رتل نم ةفلتخمل ءاونأل ةدهاشم هذ نم ي نمض لي جستلا ديقت دوجوم ل FTD ءحص نم ققحتلا . اهنم لك يف ءكرتشملا تائفلا

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

Note: Container Instances of same blade share feature licenses

Activate Windows
Go to System in Control Panel to activate Windows.

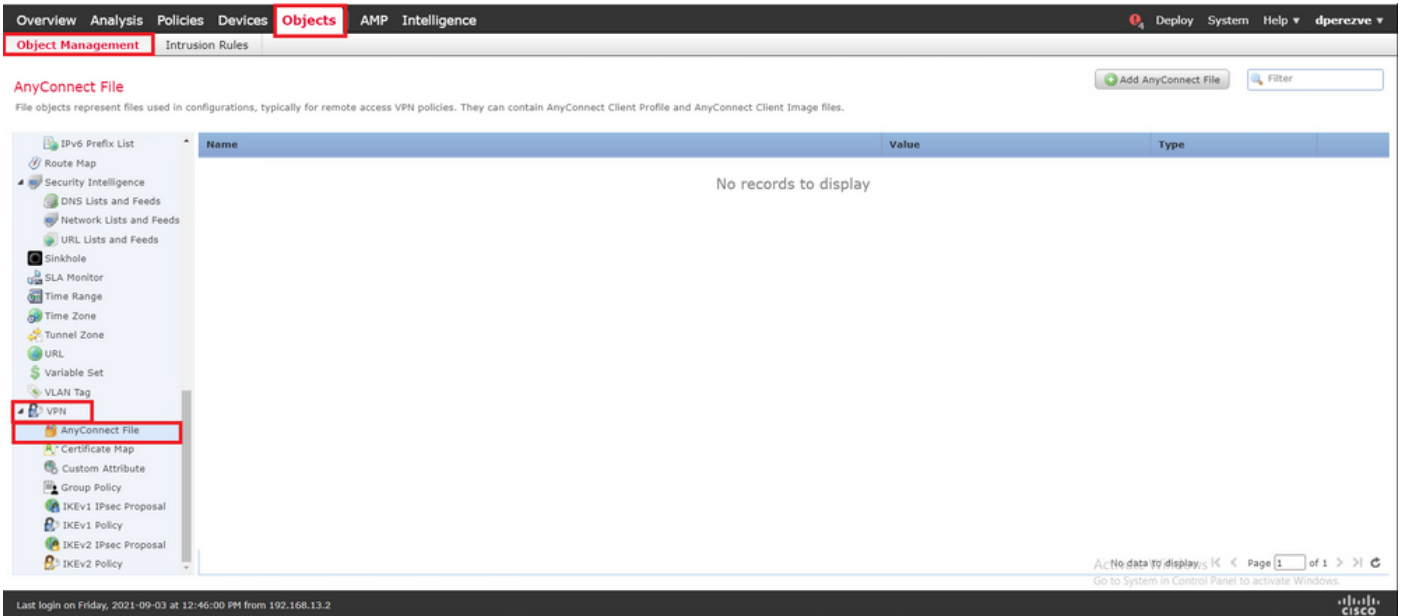
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

2. عوطخل Cisco Secure Client ليمحت

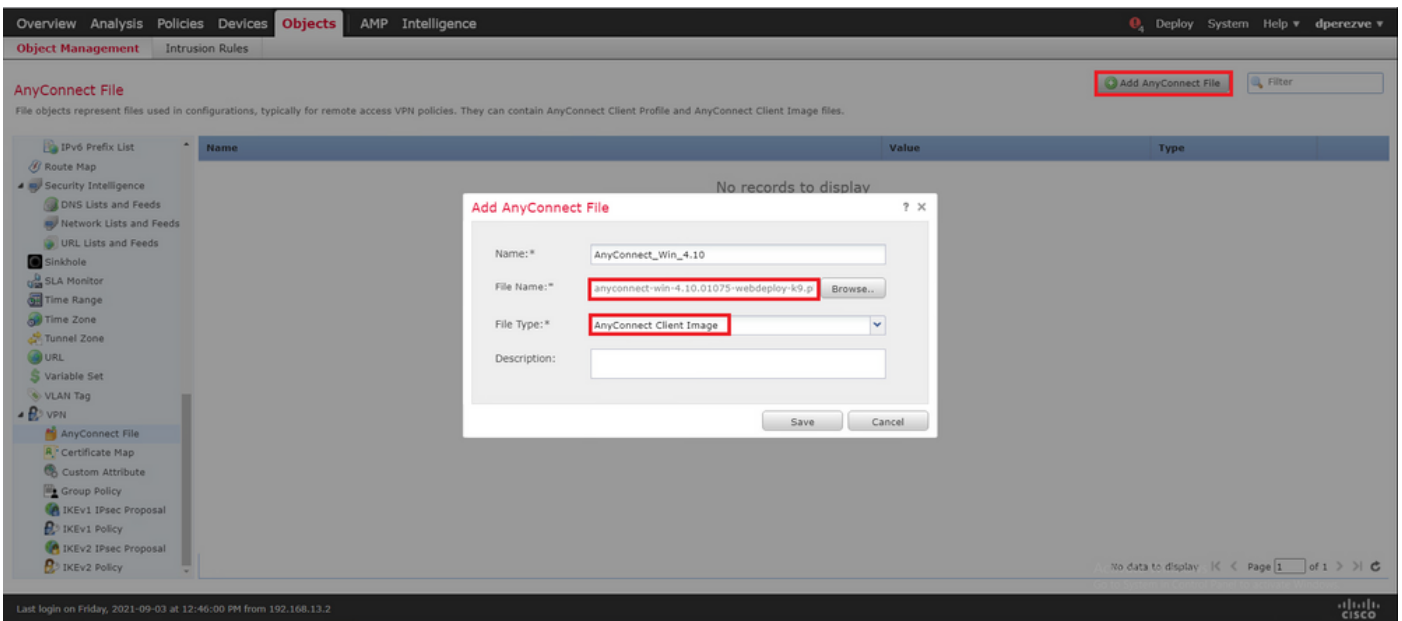
ل Cisco Secure Client (AnyConnect) ب ةصاخل ثللاو لابقتسال ةدحو رشن ةمحت ليزنتب مق cisco.com نم Windows.

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

للمع فلم رتخاو تانئال ةراد > تانئال ال ال لقتنا ، نم آل Cisco للمع ةروص ليمحتل
تايوتحمل لودج في VPN ةئف نمض نم آل Cisco.



مق ،نم آل AnyConnect ليمع فلم ةفاض اذفان يف . AnyConnect فلم ةفاض ازل رتخأ ةروص رتخأ اريخ أو نم آل Cisco ليمع ةمزح راي تخال . ضارعت سا رتخأ م ث ، نئ الك لل مسا ني عت ب ةلدس نم لا ةمئ اق لا يف فلم لا عونك AnyConnect ليمع .



ت انئ الك لا ةمئ اق لا ازل نئ الك لا ةفاض ا ب جي . ظفح رزل رتخأ

Name	Value	Type
AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	AnyConnect Client Image

ايتاذ ةعقوم ةداهش عاشنإ. 3 ةوطخلا

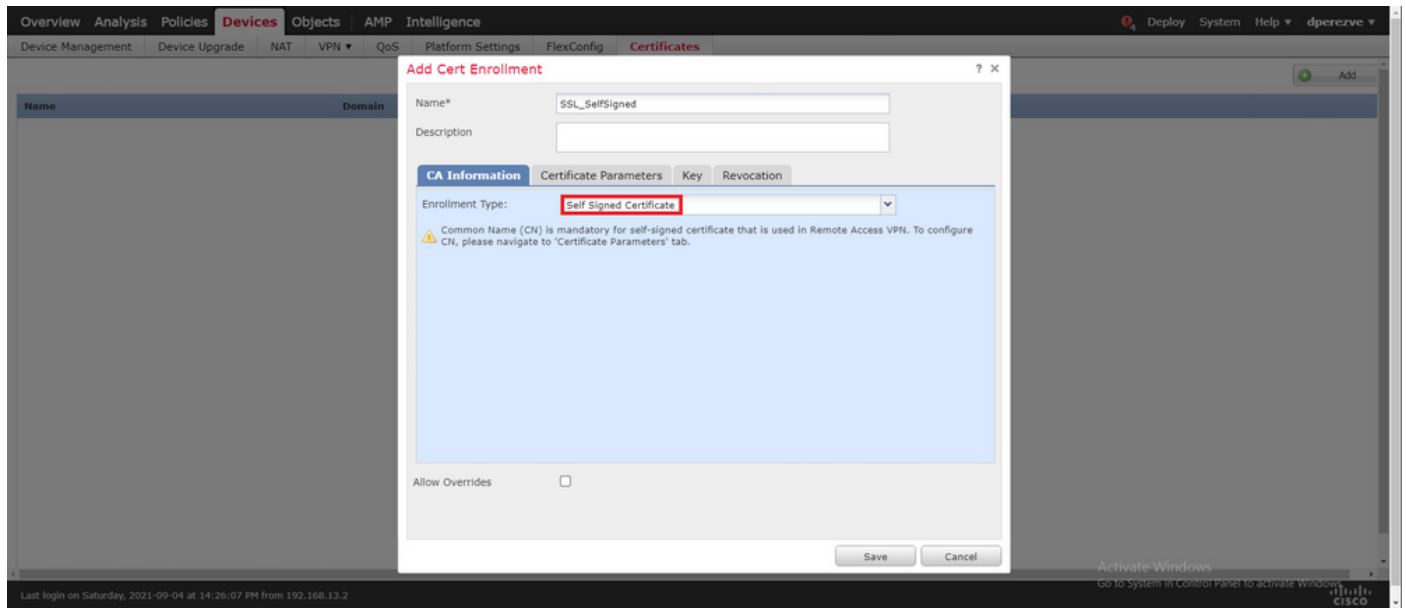
يف اهم ادخستسإ متيل ةحل اص ةدحاو ةداهش دوجو (AnyConnect) SSL Cisco Secure Client ب لطي ليمعلاو VPN ةكبش ب ةصاخلا ثبل او لابق تسالا ةدحو ني ب SSL ةحفاصم

بناج ىلإ ف ، كلذ عمو . ضرغلا اذهل ايتاذ ةعقوم ةداهش عاشنإ متي ، لاثملا اذه يف : ةظحالم وأ ةيلخاد ةداهش ةئيه نم اما ةعقوم ةداهش ليمحت نكمملا نم ، ايتاذ ةعقوملا تاداهشلا اضيأ فورعم قدصم عجرم نم

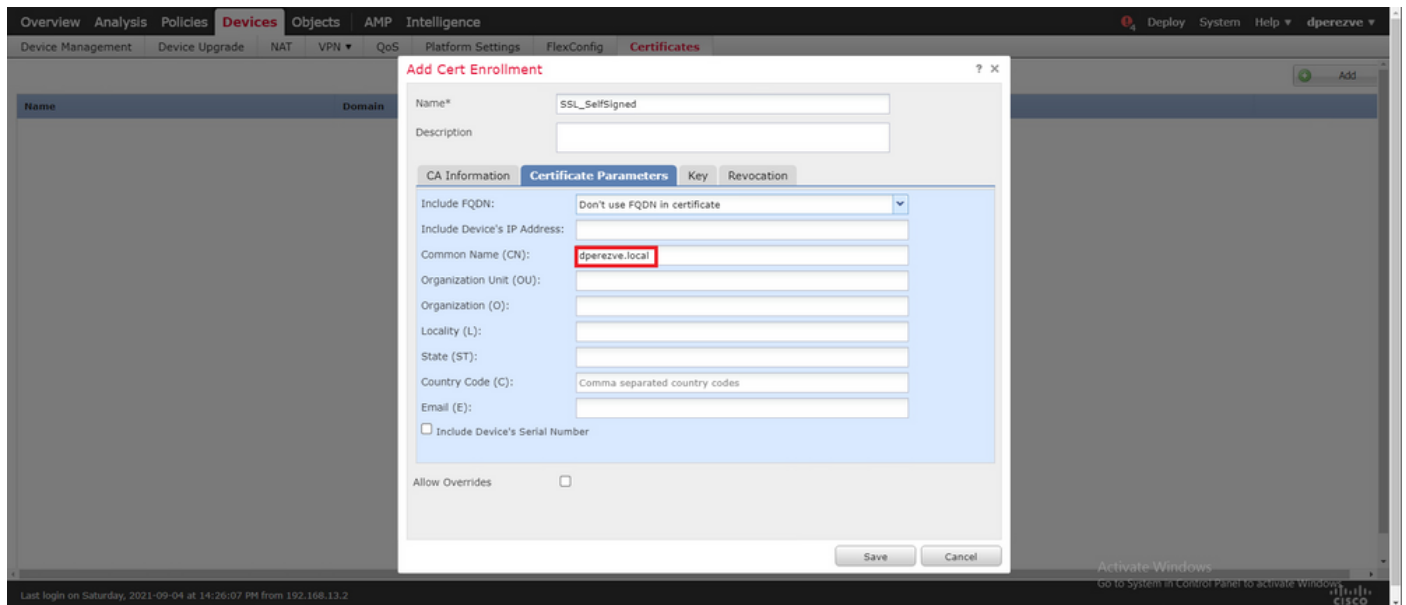
تاداهشلا > ةزهجالا ىلإ لقتنا ، ايتاذ ةعقوملا ةداهشلا عاشنإل

ةفاضإ ةذفان يف زاهجالا ةلدسنملا ةمئاقلا يف ايلاح دوجوملا FTD رتخأ مث . ةفاضإ رزلا رتخأ ةديج ةداهش

ةذفان يف ،نآلا مق .ديج ليجست نئاك عاشنإل (زمر + رضأ) لوصولا ليجست ةفاضل رزرتأ ةمئاقلا يف ايتاذ ةعقوم ةداهش رتخاو نئاكلل مسا نييعتب ،رصنعلل لوخد ليجست ةفاضل ليجستلا عون ةلدسنملا



(CN) كرتشم مسا كانه نوكي نأ ايمازل نوكي ،ايتاذ ةعقوملا تاداهشلل ةبسنلاب ،اريخأ CN. ديحتل تاداهشلا تاملعم بيوبت ةمالع ىلا لقتنا



تاداهشلا ةمئاق ىلا ةديجلا ةداهشلا ةفاضل بجي ،ناوث عضب دعب .ةفاضل وظفح رارزأ رتخأ



FMC ىلع يلحم قاطن عاشنإ 4. ةوطخل

يلحم قاطن يف ةلباقملا رورملا تاملكو يلحملا مدختسملا تانايب ةدعاق نيخت متي

Name	Description	Type	Domain	AD Primary Domain	Base DN	State
AnyConnect-Local-Auth		LOCAL	Global			Enabled

5. SSL Cisco Secure Client نيوكت

دع ب نع لوصول VPN > زهجالا لى لقتنا، SSL Cisco Secure Client نيوكت

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
Device Management	Device Upgrade	NAT	VPN Remote Access	QoS	Platform Settings	FlexConfig

فیرت فل مل مسا دي دحتب مق. ةسايس VPN دي دج ت قلخ in order to رز فيضي ترتخأ لك نيوكت بجي. فدهتسم زاهك دوجومال FTD رتخأ م، SSL رايتخا ةناخ دح م، لاصتالا دع ب نع لوصول VPN جهن جلاعم في جهنل نييعت مسق في عيش

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
Device Management	Device Upgrade	NAT	VPN Remote Access	QoS	Platform Settings	FlexConfig

Remote Access VPN Policy Wizard

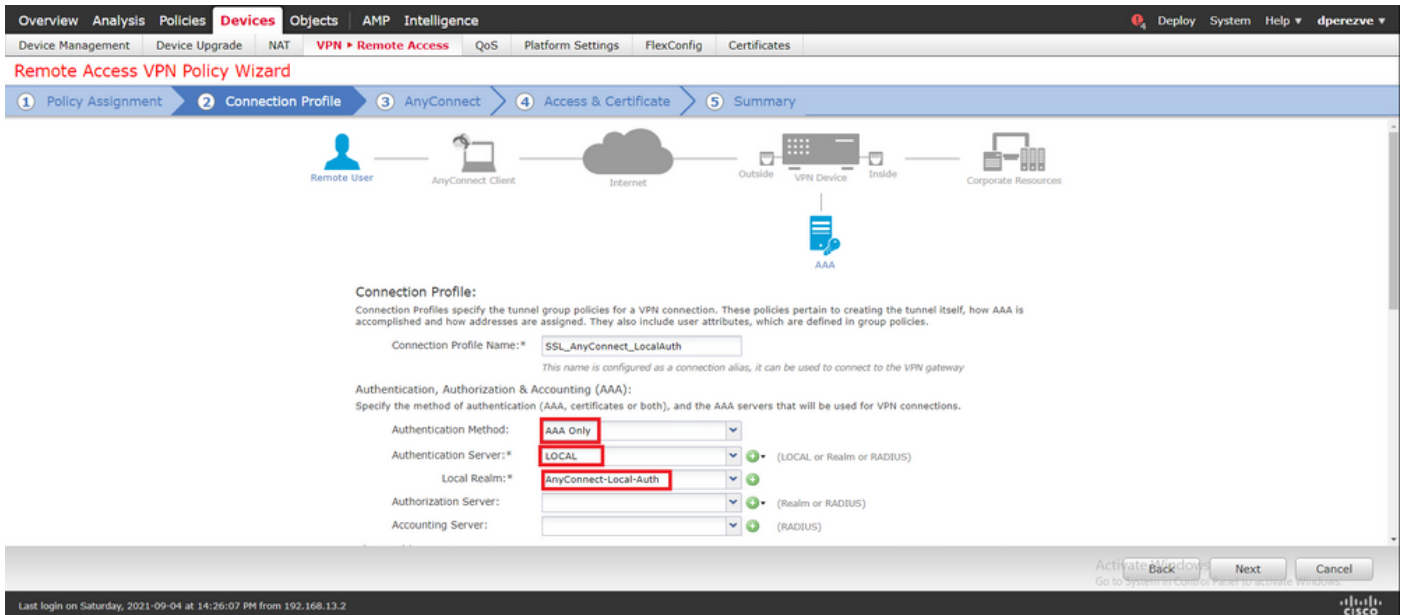
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Name: * SSL_AnyConnect_LocalAuth
 Description:
 VPN Protocols: SSL IPsec-IKEv2
 Targeted Devices: Available Devices: ftdv-dperezve, ftdvha-dperezve
 Selected Devices: ftdvha-dperezve

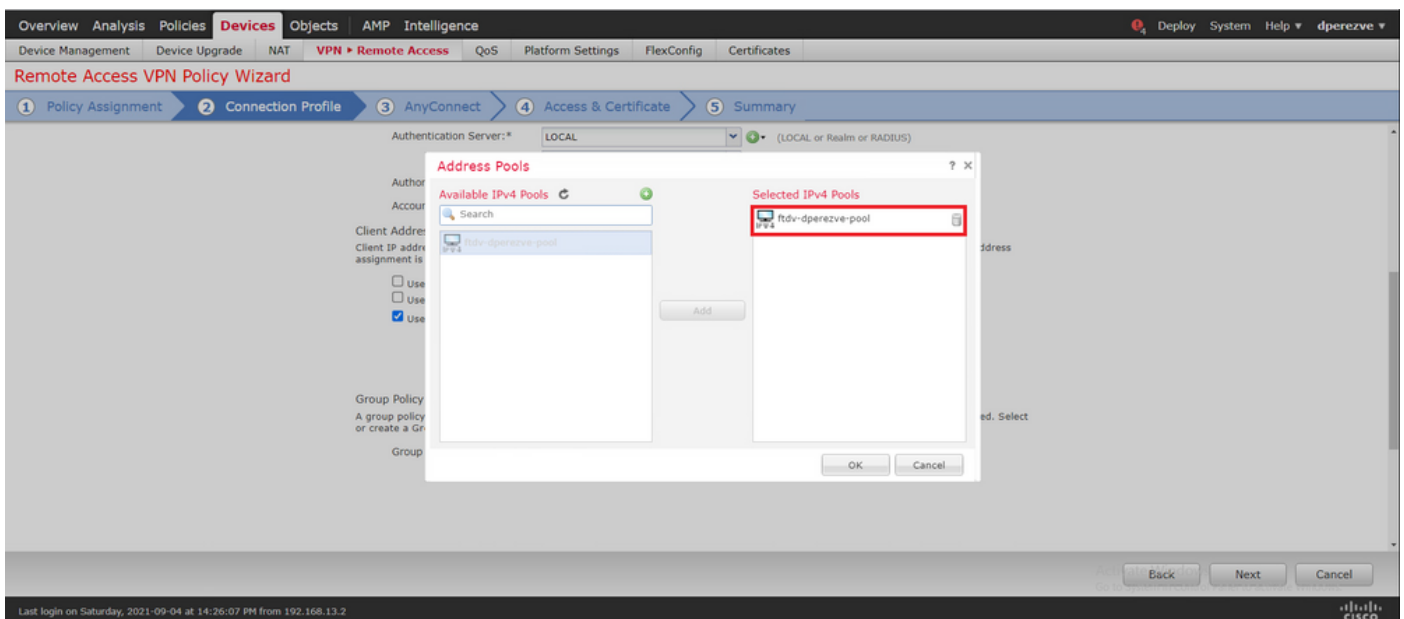
Authentication Server: Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.
 AnyConnect Client Package: Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.
 Device Interface: Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Next Cancel

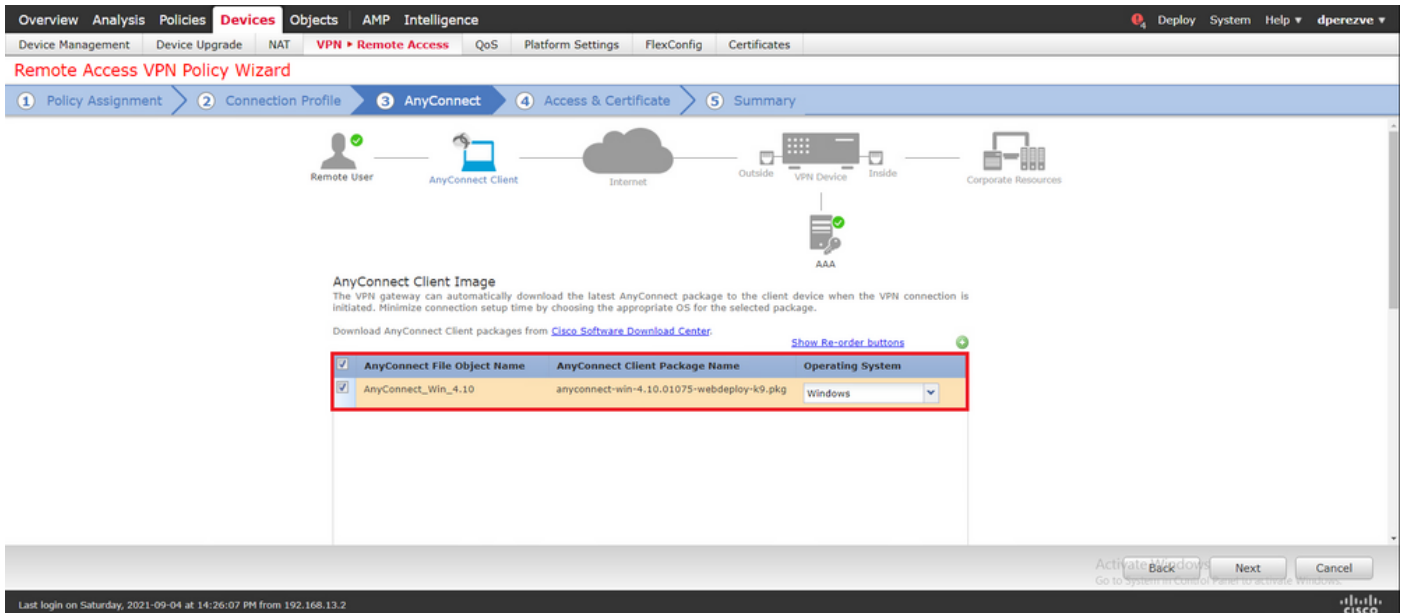
في صوتل مسا في رعتب مق. لاصتالا في رعت فل م نيوكت لى لقل لل لياتال رتخأ، ةقداصم ل مدخال ةلدسنم ل ةمئاقلا في، م. ةقداصم ةقيرطك طقف AAA رتخاو لي صوتل ل ةلدسنم ل ةمئاقلا في 4 ةوطخال في هؤاشن م يذلا يلحمل لاطنل رتخأ، اريخأ و، يلحمل رتخأ يلحمل لاطنل.



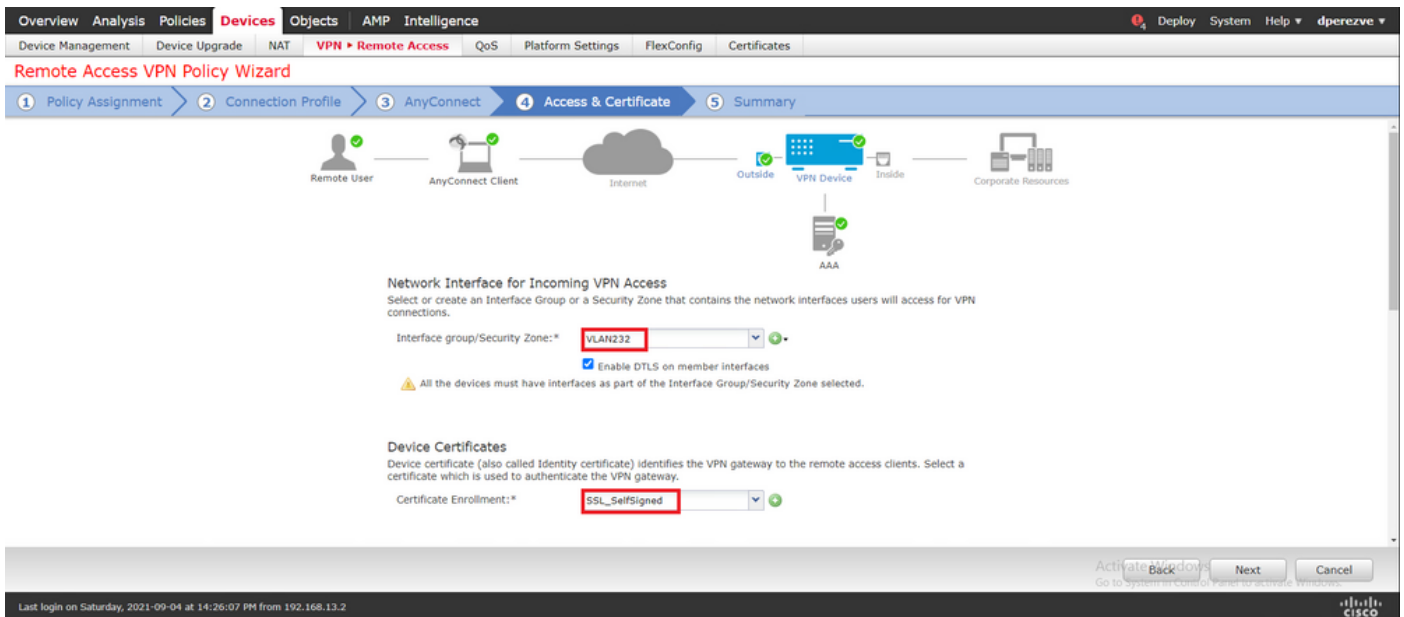
مسوق في صاصرللا ملقلا ةنوقيا رتخأ مث ، ةحفصللا سفن لىل ف لسأ لىل ريرم تلاب مق نم آلا Cisco ءالمع لبق نم مدختسم ال IP عمجت ديحتل IPv4 نيوانع عمجت



نم آلا Cisco ليمع ةروص رتخأ ، نآلا . مسوق AnyConnect لىل تلقن in order to كلذ دعب ترتخأ 2. ةوطخلال في اهليمحت مت يتلا



ة و م ج م ة ل د س ن م ل ا ة م ئ ا ق ل ل ا ي ف . ة د ا ه ش ل ل ا و ل و ص و ل ا م س ق ي ل ل ا ل ق ن ل ل ي ل ل ا ت ل ر ت خ ا
 Cisco Secure Client (AnyConnect) ن ي ك م ت م ز ل ي ي ت ل ا ة ه ج ا و ل ر ت خ ا ، ن ا م ا ل ا ة ق ط ن م / ة ه ج ا و ل ا
 ي ف ا ه و ا ش ن ا م ت ي ت ل ا ة د ا ه ش ل ل ر ت خ ا ، ة د ا ه ش ل ل ل ي ج س ت ة ل د س ن م ل ا ة م ئ ا ق ل ل ا ي ف ، م ت . ا ه ي ف
 3. ة و ط خ ل ل



ل ي ك ش ت ن و ب ز ن م ا ي cisco ل ن م ة ص ا ل خ ت ي ا ر ا r in order to ك ل ذ د ع ب ت ر ت خ ا ، ا ر ي خ ا .

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dpervez

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 Access VPN Policy Configuration

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

Name: SSL_AnyConnect_LocalAuth

Device Targets: ftdvha-dpervez

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-dpervez-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.

1 **Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

2 **NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

3 **DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

4 **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.

5 **Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'VLAN232'

Activate Windows
Go to System in Control Panel to activate Windows.

Back Finish Cancel

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

FTD. ىل ع تاريخي غتلا رشنو ءاهن ارتخا، ةححص تادادعإل عي مج تناك اذا

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help dpervez

Deployment Deployment History

1 device selected
Deploy time: Estimate Deploy

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

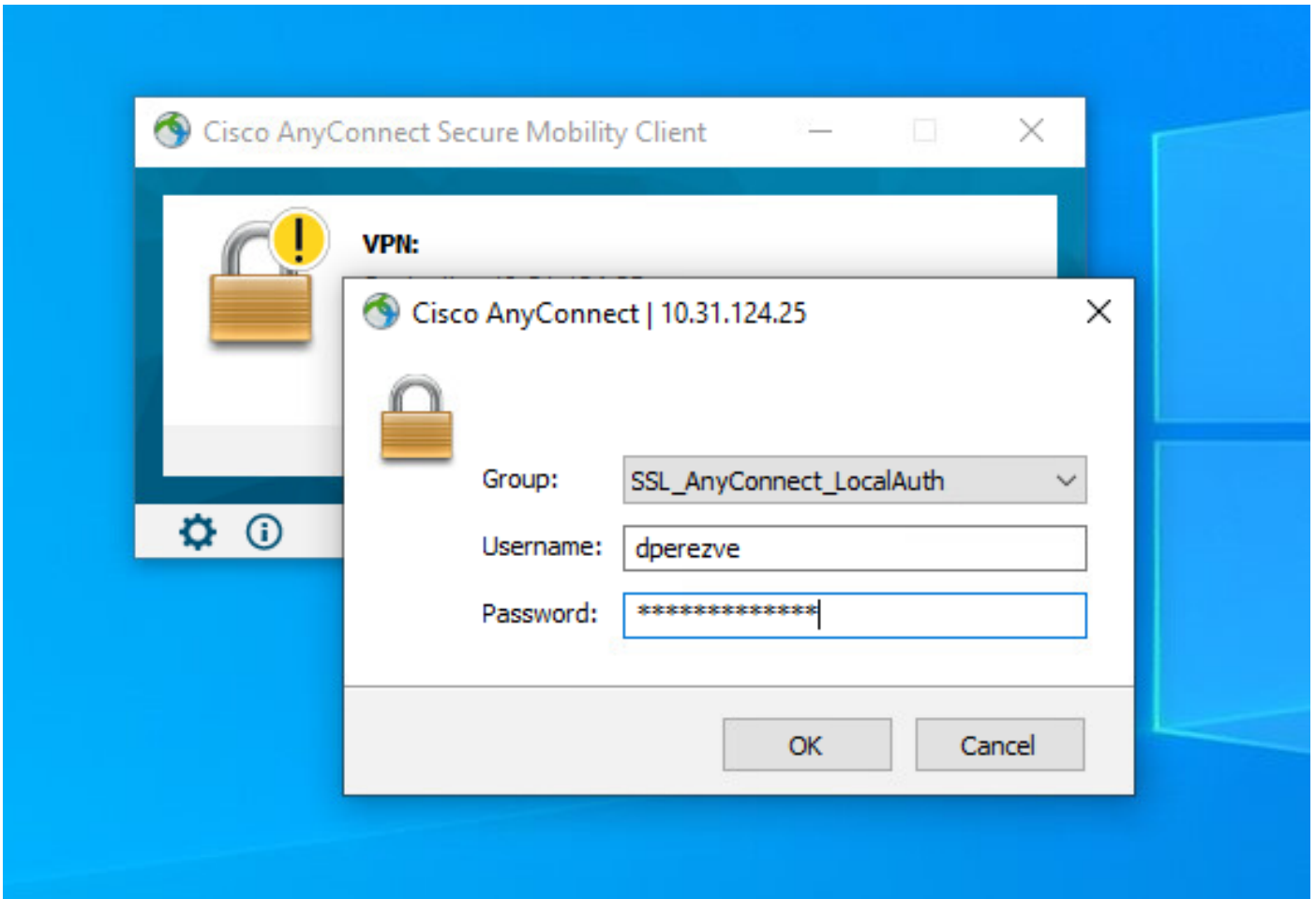
Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dpervez	dpervez		FTD		Sep 7, 2021 2:44 PM		Pending

Activate Windows
Go to System in Control Panel to activate Windows.

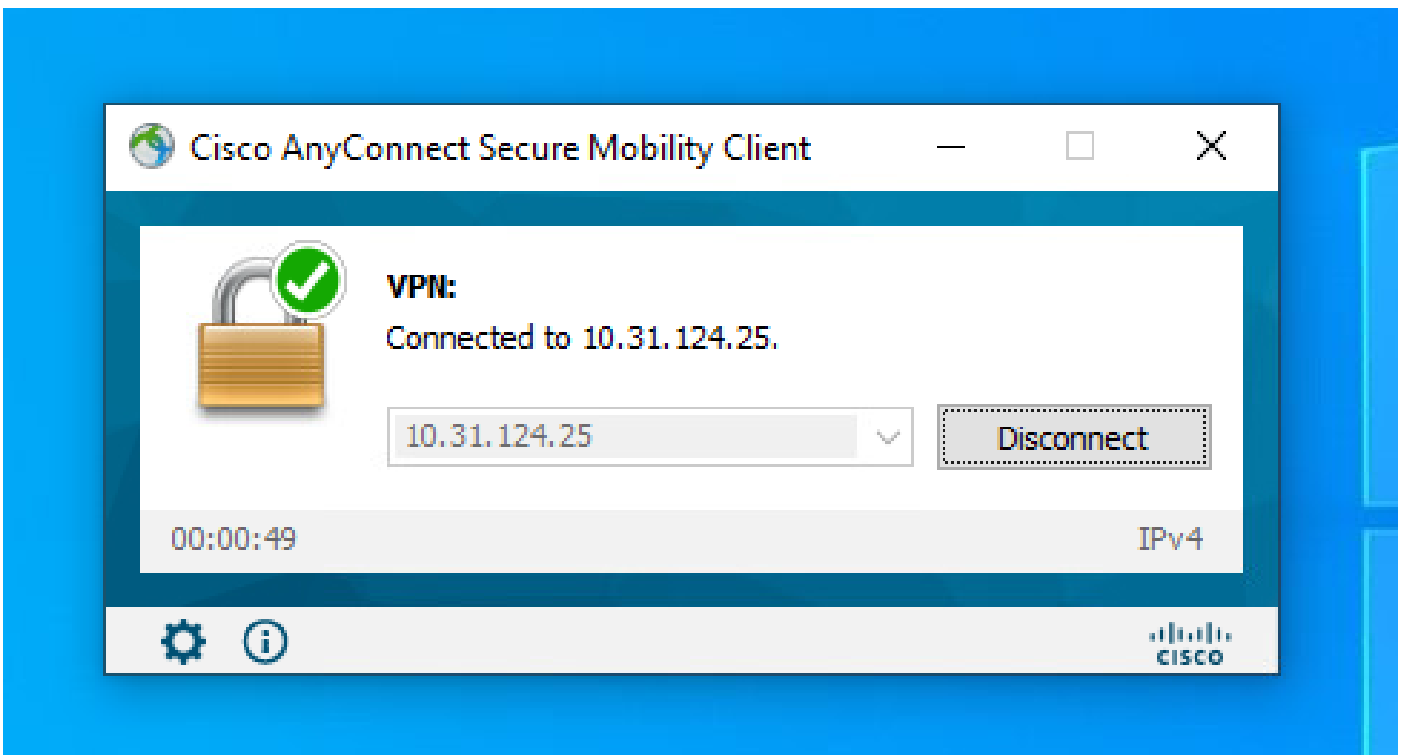
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

ةحصلال نم ققحتلا

ىل Windows ليمع نم Cisco AnyConnect Secure Mobility Client لاصتا ادبا، رشنلا حاجن درجمب امه ةقداصملا ةبلاطم ي ف ني مدختسملا رورملا ةملكوم مدختسملا مسا نوكي نأ بجي FTD. 4. ةوطخلا ي ف هؤاشنإ مت يذلا ءيشلا سفن



ل Cisco AnyConnect Secure Mobility Client قىببطت ضرعي نأ بجي، FTD لبق نم دامتعالا تانايب دامتعا درجب لاصتالا ةلج.



ليعمل ل لمع تاسلج ضرعل show vpn-sessionDB anyConnect رملأ ليغشت كنكمي FTD نم

ة.امحل رادج ىلع ايلاح ةطشنل Cisco نم ةنمآلا

```
firepower# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

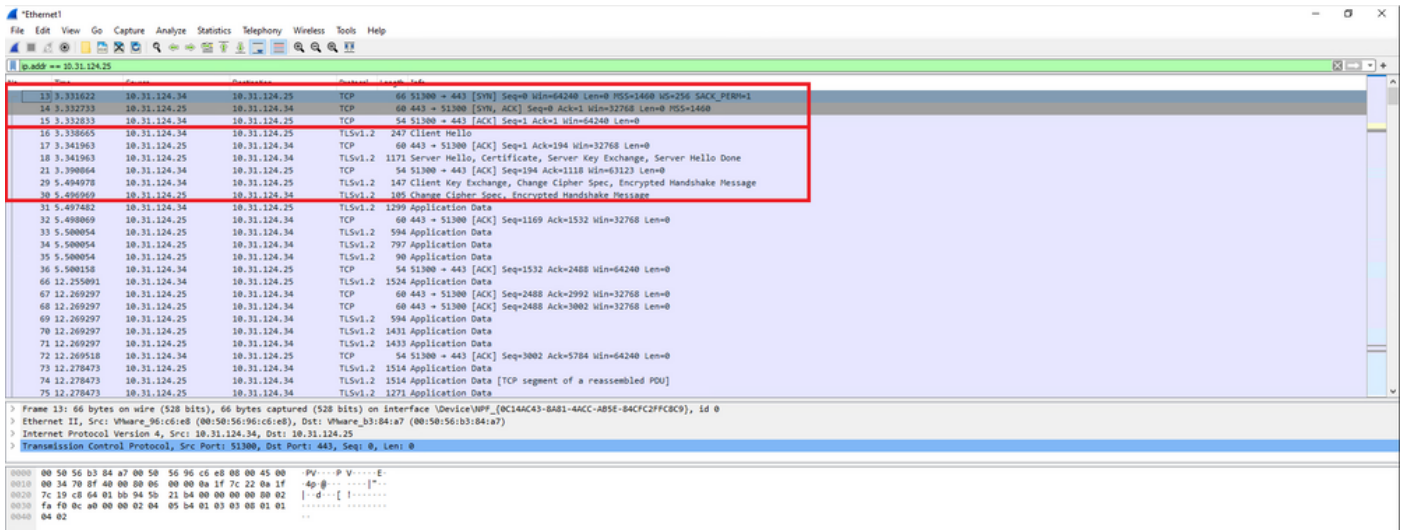
```
Username      : dperezve          Index      : 8
Assigned IP   : 172.16.13.1      Public IP  : 10.31.124.34
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
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
```

اهحالص او ءاطخال افاشك تسا

ىلع SSL لاصتا قفدت ىرتل FTD ىلع debug webVPN AnyConnect 255 رمألا ليغشتب مق FTD.

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

عم لاصتالا قفدت ةظحال نمك مي Cisco، نم نمآلا لي عم ءاطخال احيحصت ىل ةفاضالاب ةي رودة حفاصم تايلمع ثالث لامكإ متي، حجان لاصتا ىلع لاثم اذه. اضيأ TCP ةمزح طاقتلا تايلمع ىلع ةقفاوملل مدختست SSL ةحفاصم اهبتي، FTD و Windows لي مع نيب ري فشتلا.



تانايب ةحص نم ققحتلاب FTD موقى نأ بجي ،لوكوتوربلاب لاصتالا ديكأت تايلمع دعب
 يلحمل قاطنلا يف ةنخمل تامولعمل مادختساب دامتعالا

شحبلال نم ديزمل Cisco TAC ب لصتاو DART ةمزح عمجت

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا