

ةقداصملا مادختساب نمآلا SSL ليمع نيوكت ةقداصملا فTD لة ةيلحملا

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[تانوكتلا](#)

[صيخرتلا نم ققحتلا 1. ةوطخلا](#)

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

[ايتا ةقوم ةداهش ءاشن 3. ةوطخلا](#)

[FMC لة ليمحت قاطن ءاشن 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 متت يتللا Cisco FTD لة ةيلحملا 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 ةيلعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ م تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتك تكبش

ةيساسأ تامولعم

ةصاخلا ةكبشلل عاشنإل (SSL) ةنمألا ليصوتلا ذخأم ةقبط مادختسا متي ،لا ثمل اذه يف 10 Windows ليمعو FTD نيب (VPN) ةيرهاظلا

ةيلحمل ةقداصملا FMC ةطساوب هترادإ متت يذلا FTD لوكوتورب معددي ،7.0.0 رادصإلا نم ةيظايتح| ةقيرطك وأ ةيساسأ ةقداصم ةقيرطك اذه فيرعت نكميو .ني نمألا Cisco ءالمعل ةيلحمل ةقداصملا نيوكب متي ،لا ثمل اذه يف .ةيساسألا ةقيرطلا لشف ءلاحي يف ةيساسأ ةقداصمك

طقف اجاتم FTD لىل Cisco Secure Client Local Authentication اذه جم انربلا رادصإل نوكتي نأ لبق Cisco Firepower Device Manager (FDM) لىل

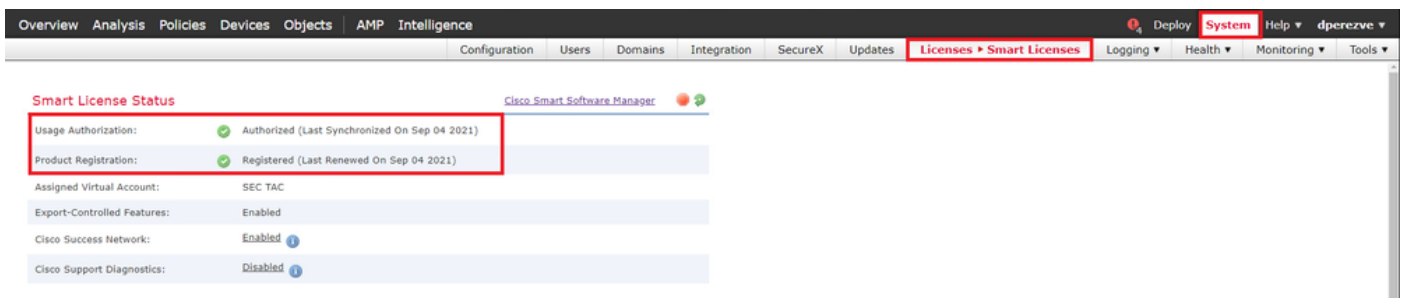
نيوكتلا

تان نيوكتلا

صخيخرتلا نم ققحتلا 1. ةوطخلا

صخيخرتلا لخدم عم ةقفاوتم نوكت نأو FMC ليجست بجي ،Cisco Secure Client نيوكب لبق VPN وأ APEX وأ PLUS صخيخرت FTD ل نكي مل اذا Cisco Secure Client رشن كنكمي ال .يكدلا طقف حلص

عم اهقفاوتم و FMC ليجست نامضل ةيكدلا صخيخرتلا > صخيخرتلا > ماظنلا لىل لقتنا .يكدلا صخيخرتلا ةباوب



ةيكدلا صخيخرتلا ططخم نم يلفسلال عزالا يف .ةحفصلال سفن لىل لفسأل ريرمتلاب مق ةرفوتملا (AnyConnect) نمألا Cisco ليمع صخيخرت نم ةفلتخمل عاونألا ةيؤر كنكمي (FTD) ةعرسلال قئاف لاسرإل جم انرب" ليجست نم دكأت .اهنم لك يف ةكرتشملا ةزهجالا او تائفلا هذه نم ي نمض يلا حلال

Smart Licenses

Filter Devices... Edit Performance Tier Edit Licenses

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
ftdva-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.

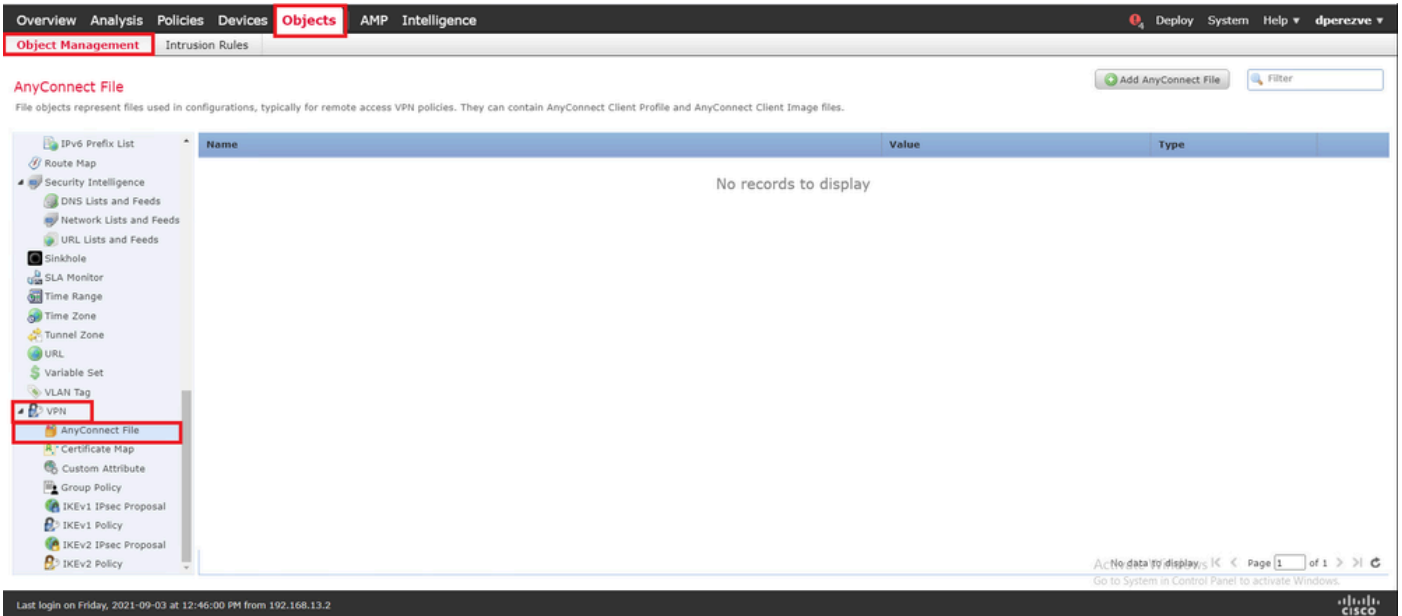
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

2. عوطخال Cisco Secure Client ليمحت

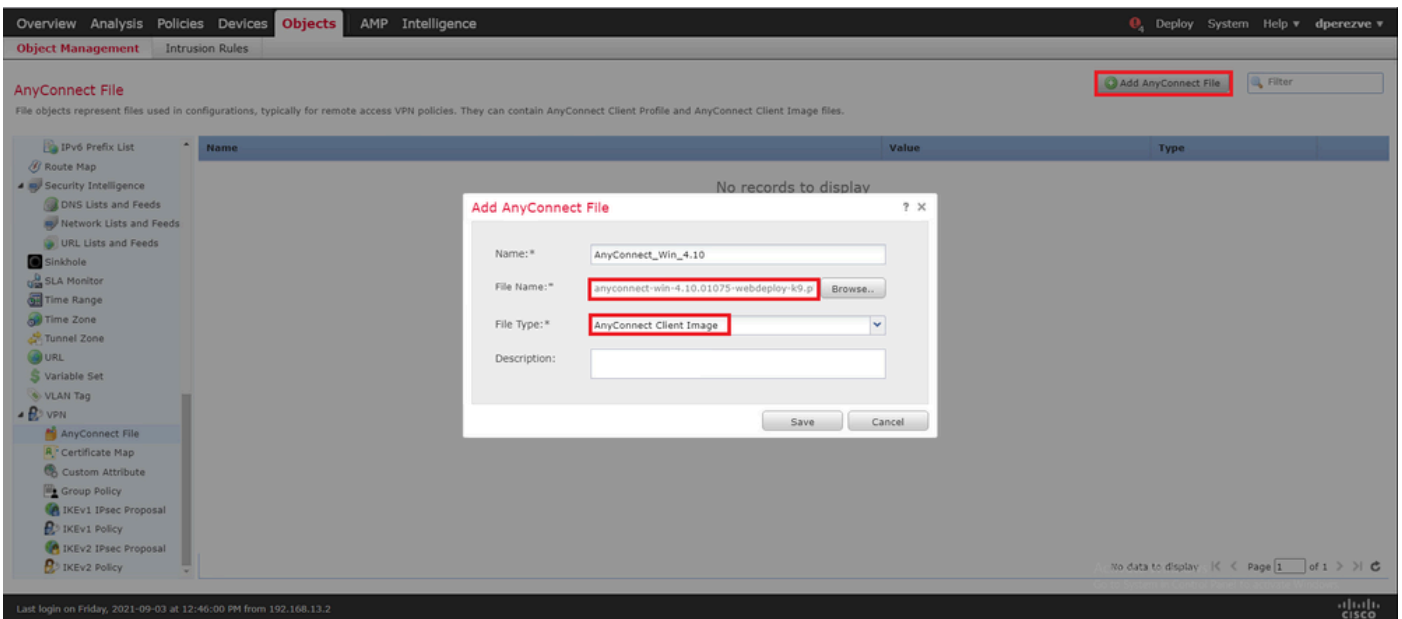
Cisco Secure Client (AnyConnect) بة صخال ثل لاول لابق تسال اءو رشن ءم زل ليزن تب مق cisco.com نم ليعش تال ماظنل

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 			

Cisco ليمع فلم رتخاو نئال ءراءا > تانئال ال ال لقتنا ، نم آل Cisco ليمع ءروص ليمحتل :
تايوتحمل لودج في VPN ءئف نمض نم آل



مق، نم آل AnyConnect ليم مع فلم ةفاض اذفان يف AnyConnect فلم ةفاض ازل رتخأ رتخأ، اريخأو. نم آل Cisco ليم مع ةمزح راي تخال.. ضارعت سا رتخأ م، نئ الك لل مسا ني عت ب ةل دس نم لا ةمئاق ل يف فلم لا عونك AnyConnect ليم مع ةروس:



تانئ الك لا ةمئاق لى لئ الك لا ةفاض ا ب جي. ظفح رزل رتخأ:

The screenshot shows the Cisco AMP Objects configuration page. The 'AnyConnect File' object is selected, and its configuration is displayed in a table:

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

The left sidebar shows a tree view of configuration objects, with 'AnyConnect File' selected under the 'VPN' category.

ايتاذ ةعقوم ةداهش عاشنإ. 3 ةوطخلا

يف اهم ادختسإ متيل ةحل اص ةدحاو ةداهش دوجو (AnyConnect) SSL Cisco Secure Client ب لطي ليمعلاو VPN ةكبش ب ةصاخلا ثبلاو لابلقتسالا ةدحو ني ب SSL ةحفاصم

كذىل ةفاضلاب. ضرغلا اذهل ايتاذ ةعقوم ةداهش عاشنإ متي، لاثملا اذه يف: ةظحالم لبق نم ةعقوم ةداهش ليمحت نكمملا نم، ايتاذ ةعقوملا تاداهشلا لىل ةفاضلاب اضيا فورعم ق دصم عجرم و ا ةيلخاد ةداهش ةطلس.

تاداهش > زهجا لىل لقتنا، عيقتولا ايتاذ ةداهش عاشنإل

The screenshot shows the Cisco AMP Devices configuration page. The 'Certificates' tab is selected, and the configuration is displayed in a table:

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

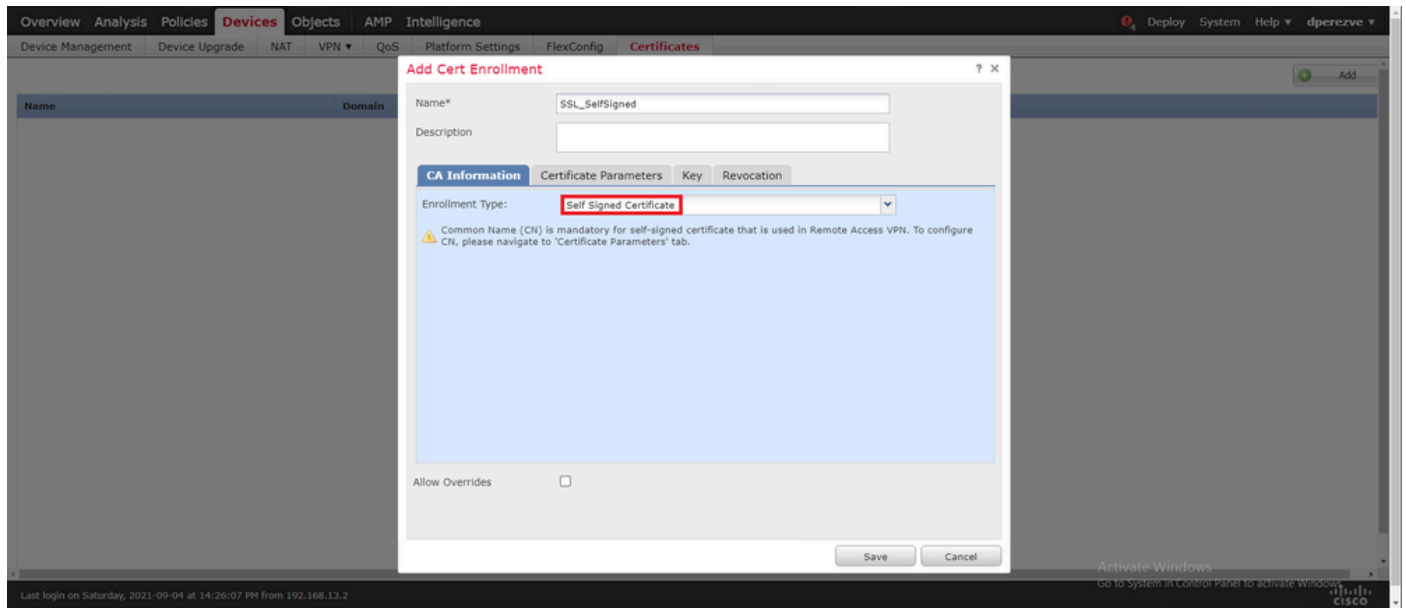
ةفاضلا ةذفان يف زاهجلل ةلدسنملا ةمئاقلا يف دوجوملا FTD رتخأ مث. ةفاضلا رزلا رتخأ ةديج ةداهش.

The screenshot shows the 'Add New Certificate' dialog box in the Cisco AMP Devices configuration page. The dialog box contains the following fields:

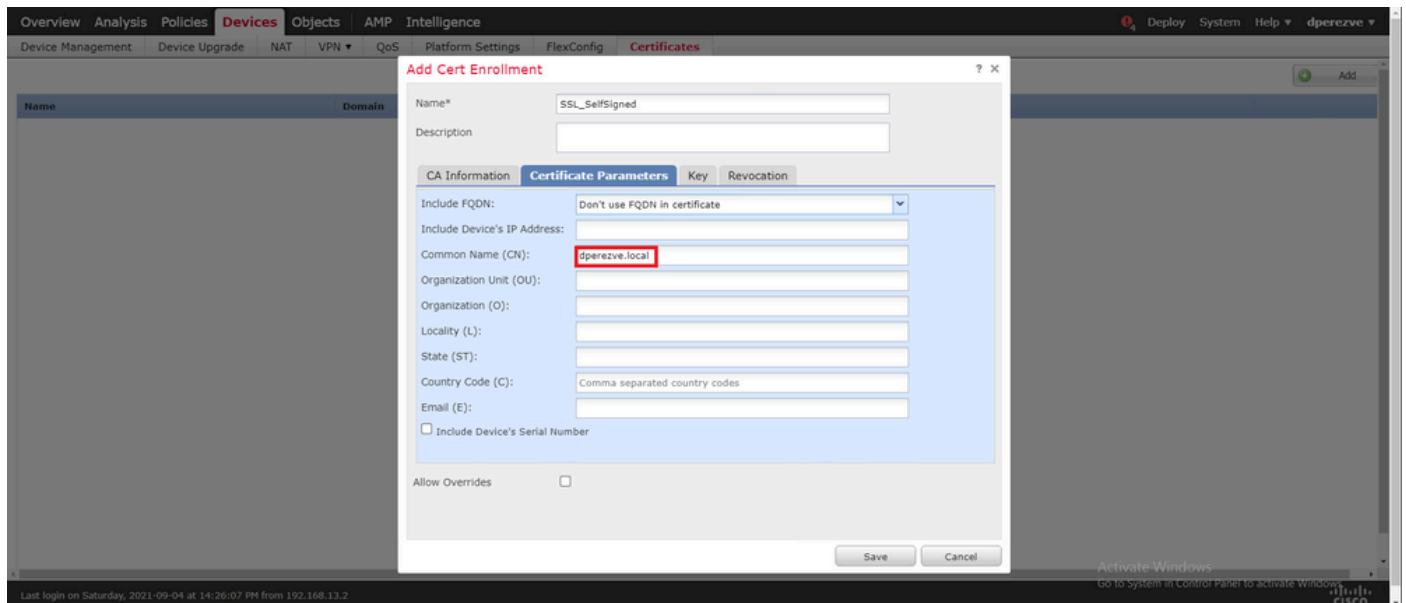
- Device*: ftdvha-dperezve
- Cert Enrollment*: Select a certificate enrollment object

The 'Add' button is highlighted, indicating the next step in the configuration process.

ةذفان يف ،نآلا مق .ديج ليجست نئاك عاشنإل (زمر + رضخأ) لوصولا ليجست ةفاضل رزرتخأ 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 ،اربخأ CN: فيرعتل ةداهشلا تاملعم بيوبتلا ةمالع ىلإ لقتنا



تاداهشلا ةمئاق ىلإ ةديجل ةداهشلا ةفاضل بجي ،ناوٲ عضب دعب . ةفاضل وظيفح رارزأ رقنا



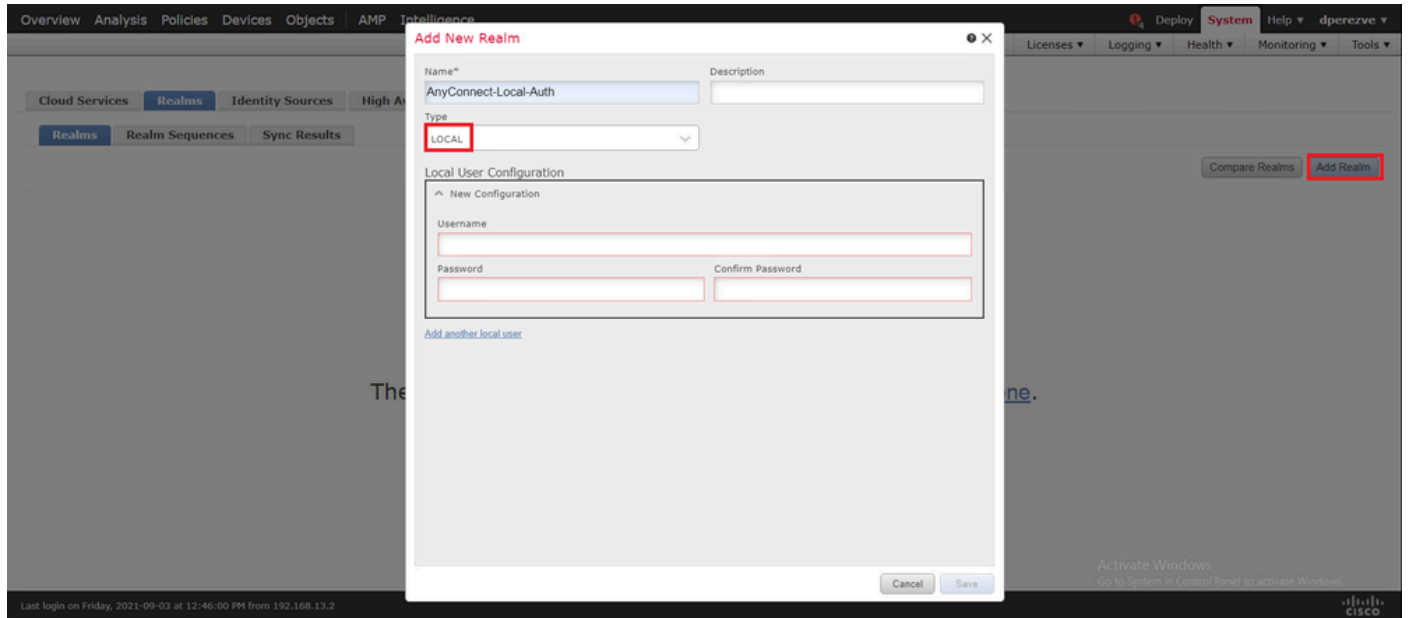
FMC ىلع يلحم قاطن عاشنإ 4 ةوطخل

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

زيمير > لمات > ماظن ىلإ لقتنا ،يلحملا لاجملا عاشنإل

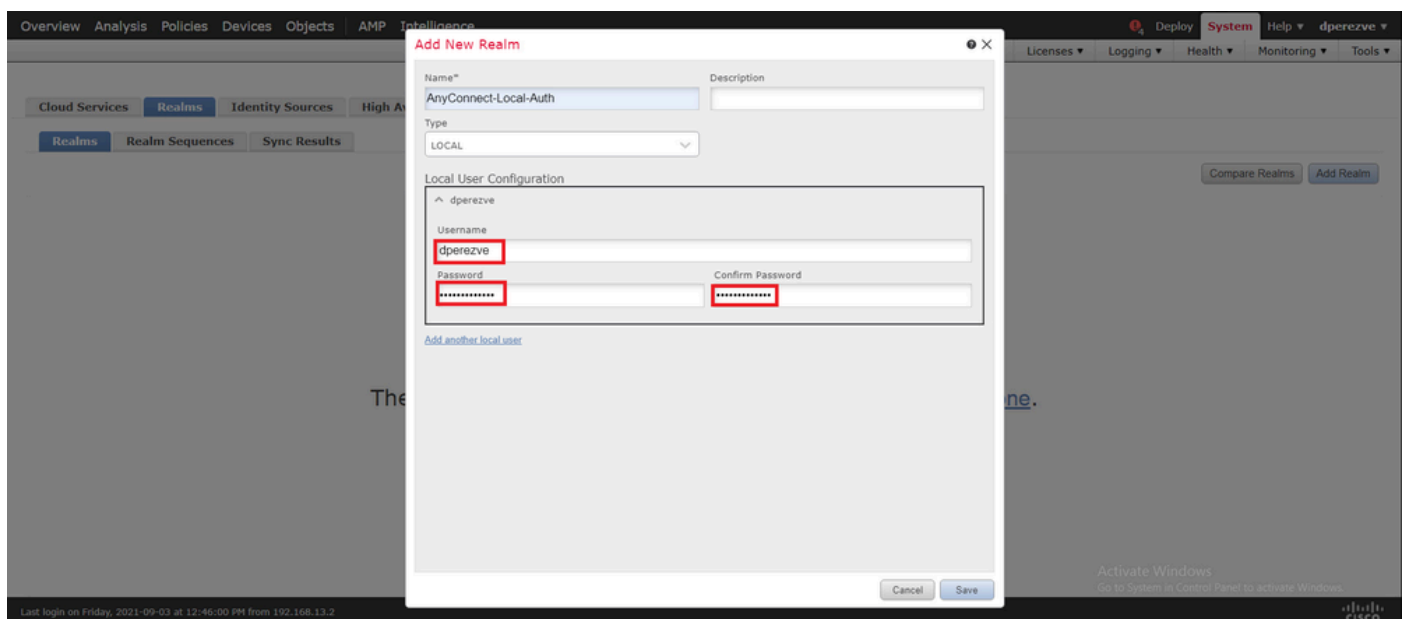


يف يلحم راىخ رتخاو مسا نييعتب مق ،ديج قاطن ةفاضل ةذفان يف .زيح ةفاضل رزرتخأ
عونلا ةلدسنملا ةمئاقلا

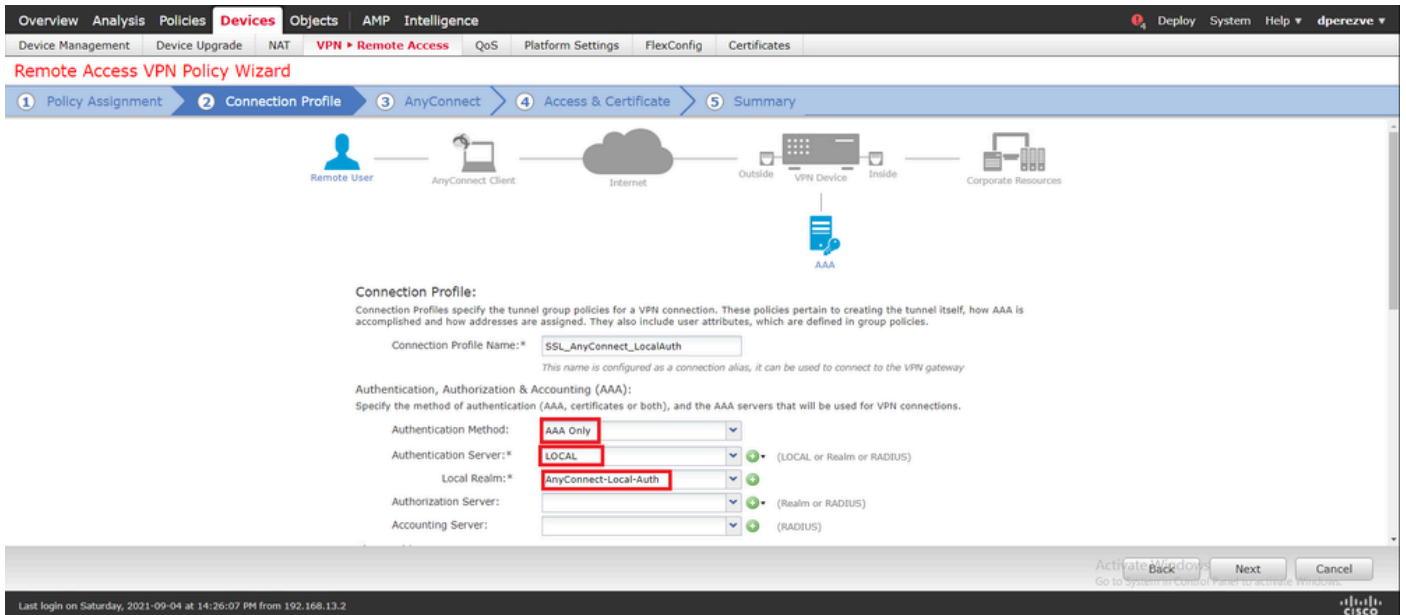


يلحملا مدختسملا نيوكت مسق يف رورملا تاملكو ني مدختسملا تاباسح عاشنإ متي

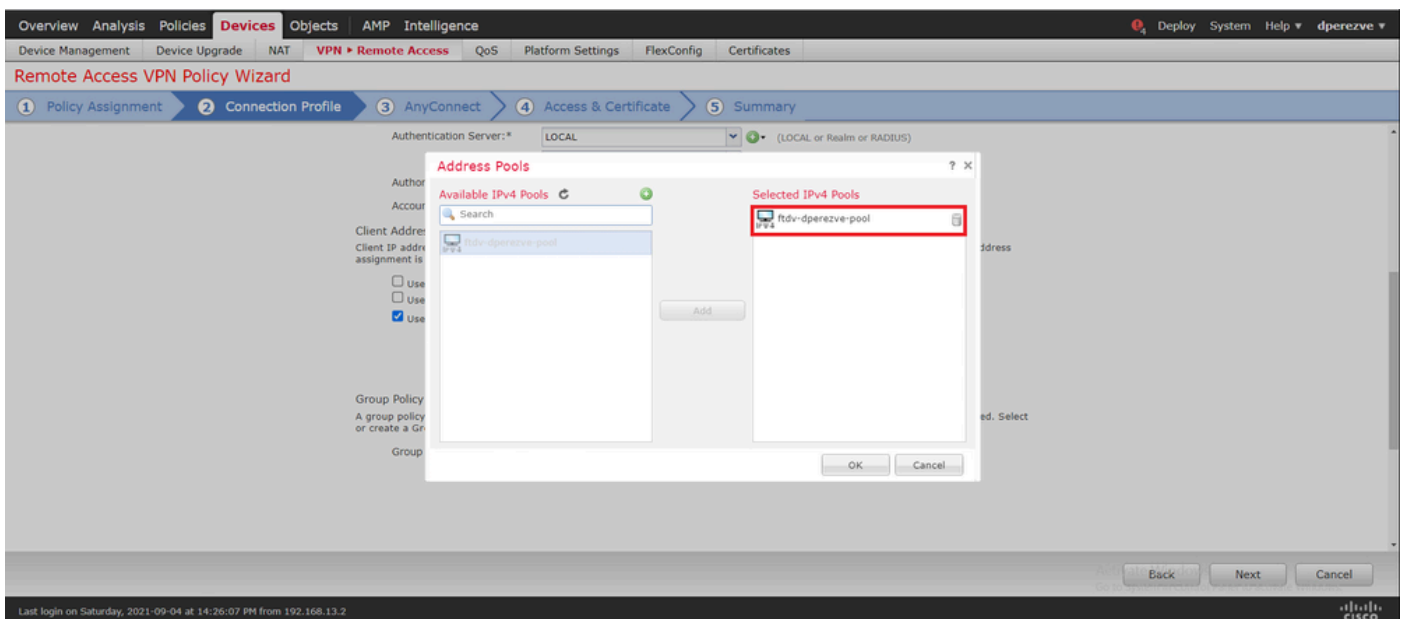
✎ فرح فرحو لقالا ىلع دحاو ريكبك فرح فرح فرح رورملا تاملكل نوكي نأ بجي :ةظالم
دحاو صاخ فرحو دحاو مقرروريغص



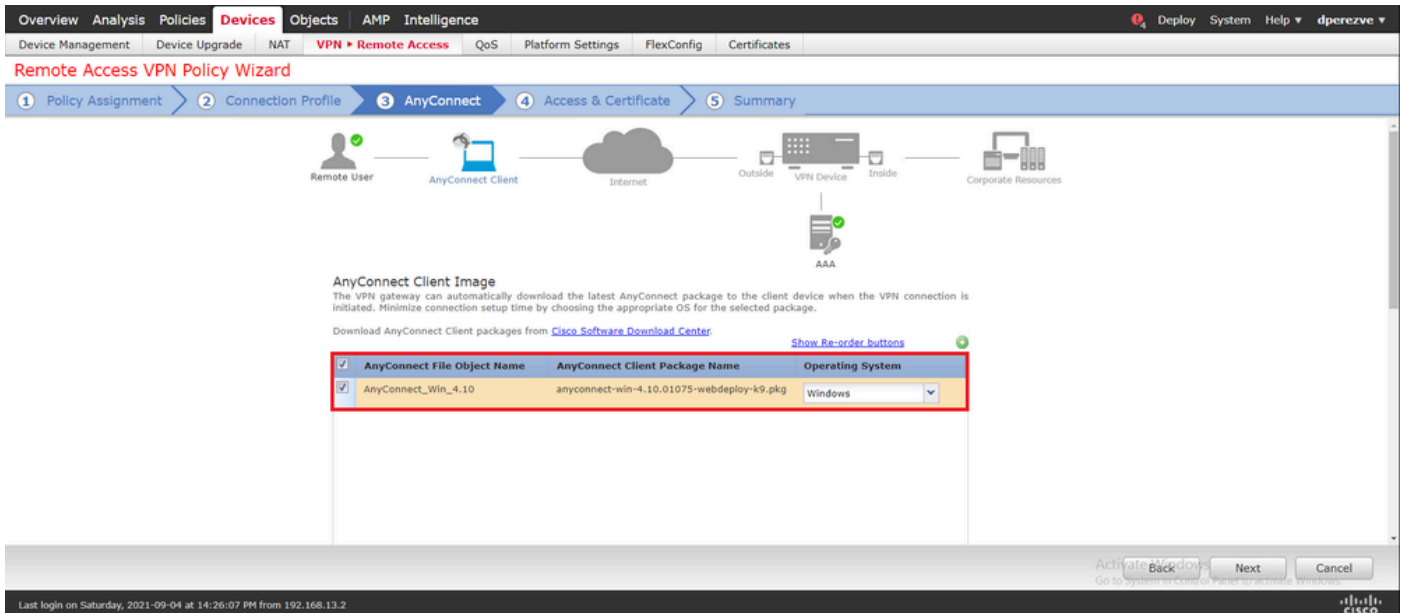
تالماملا ةمئاق ىلإ ديج قاطن ةفاضل زيح ةفاضل قوف رقنا مث ،تاريغيغتللا ظفح



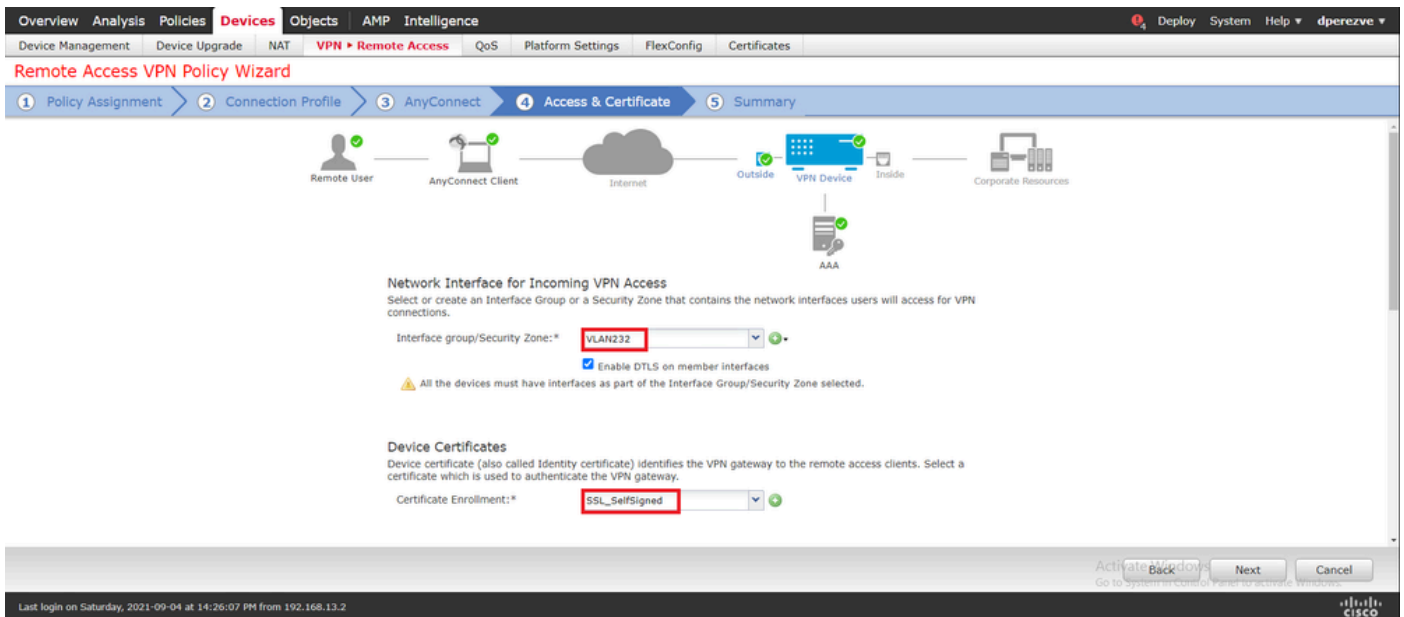
مسق ي ف صاصرل م لقل ءنوق ي أ قوف ر قنا م ث ، ءحفصل ل س فن ل ع ل ف س أ ل ر م ت ل اب م ق
نم آل Cisco ءالمع ل بق نم م ءخ ت س الم IP ءم ت ء ء ل IPv4 ن ي وان ع ءم ت



نم آل Cisco ل ي مع ءروس ء ءح ، نم آل . مسق AnyConnect ل ل ت ل قن in order to ء ل ذ ء ب ت ق ط ق
2: ءو ط ء ل ي ف ا ه ل ي م ت م ت ي ت ل



لقد سنملا عمئاقلا يف .م سق Access & Certificate الى تلقن in order to كذ دعب تقطوط
 Cisco Secure Client نيكمت مزلي يتلا هجاولا رتخأ ، نامألا قطنم/هه جاولا عومجم
 مت يتلا هه شال رتخأ ، هه شال ليجست لهدسنملا عمئاقلا يف ، مث .اه يف (AnyConnect)
 3: ةوطخلال يف اهؤاشن



لجكشت نوبز نمأي Cisco ل نم ةصالخ ىري نأ كذ دعب تقطوط ، اريخأ:

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): ftdvha-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:

- 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'.

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. دل تاريخي غتلا رشنو واهن قوف رقنا، 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

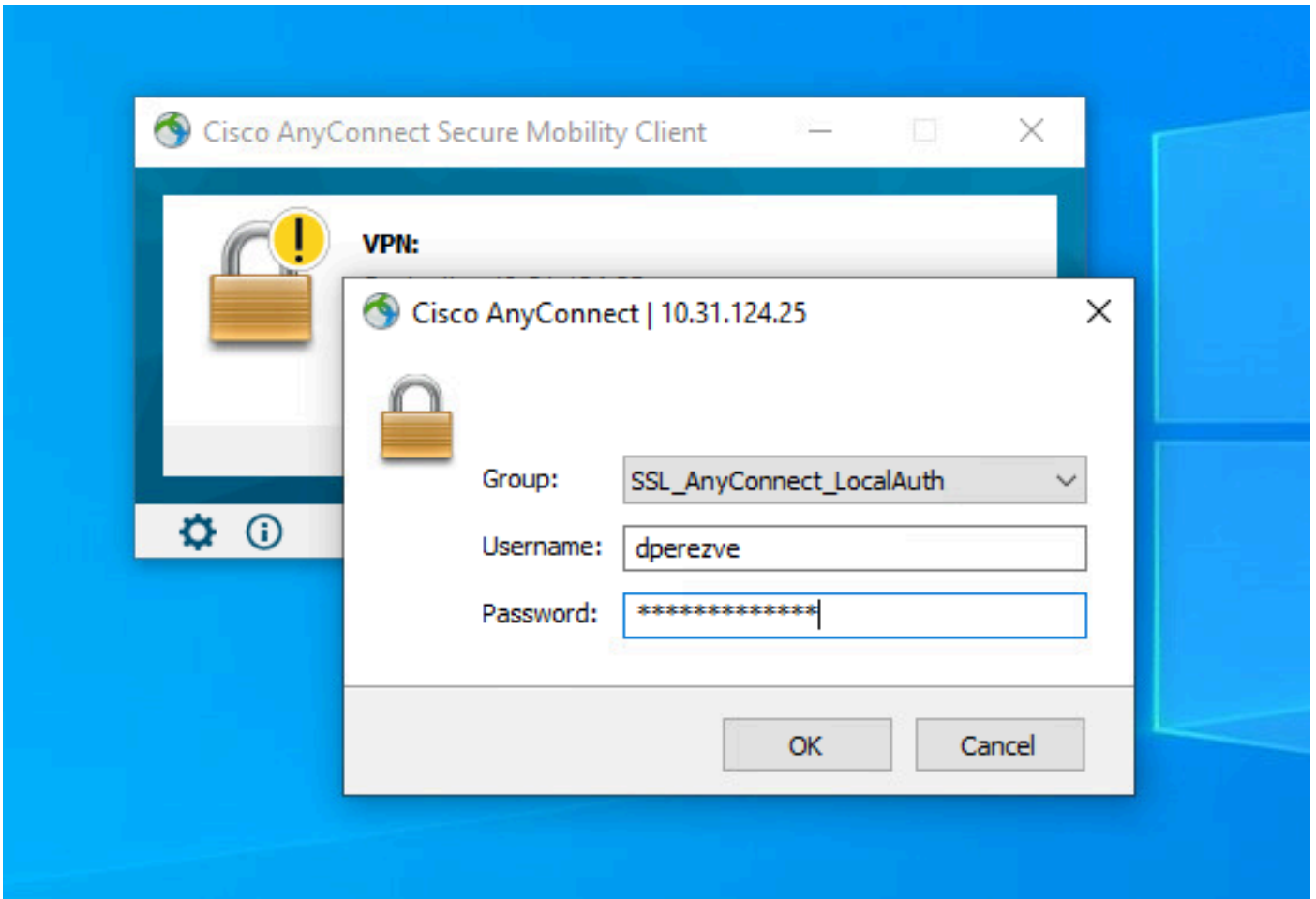
Device	Modified by	Inspect	Interrupt	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dpervez	dpervez			FTD		Sep 7, 2021 2:44 PM		Pending

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

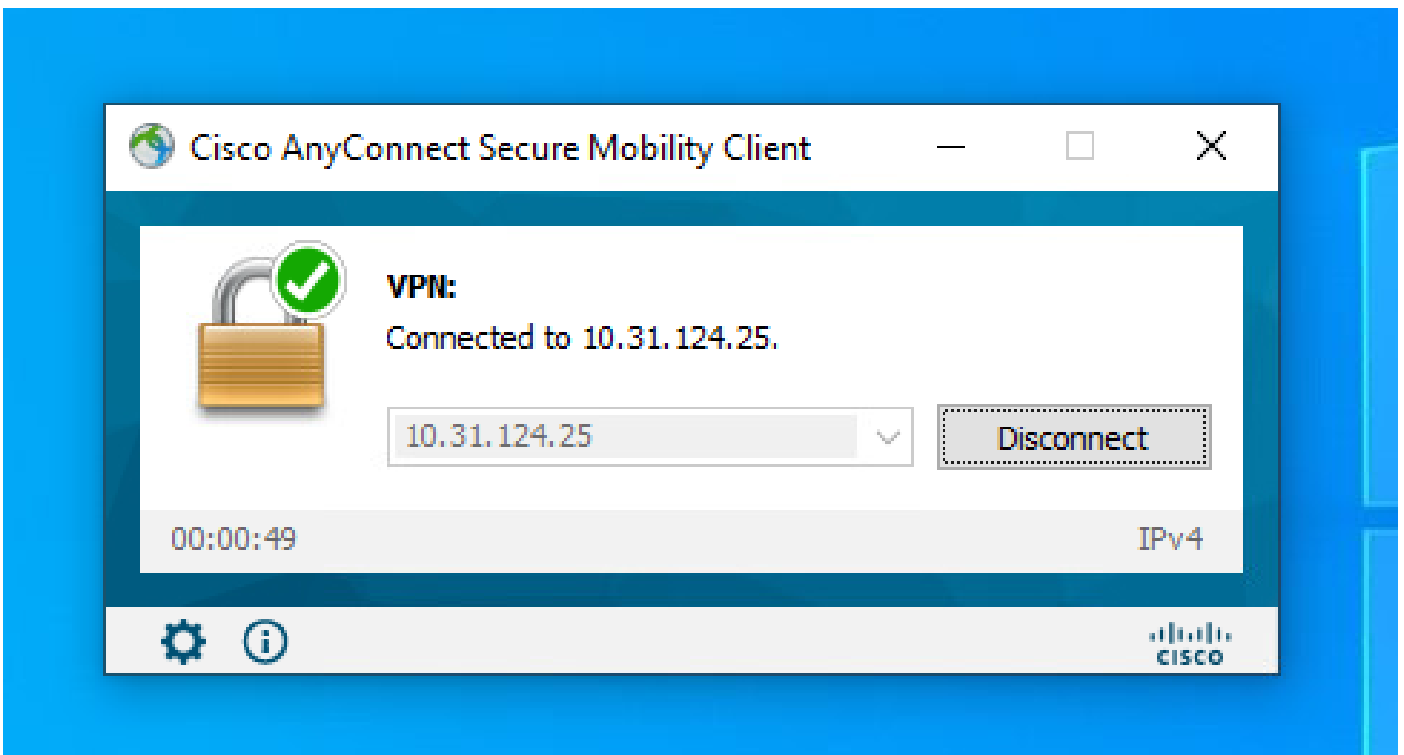
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

ةحصلال نم ققحتلا

إل Windows ليمع نم Cisco AnyConnect Secure Mobility Client لاصتا أدبا، رشنللا حان درجم ب قو داصملا رم او هجوم يف ني مدختسملا رورملا ةم لكوم مدختسملا مسا نوكي نأ بجي FTD. 4: ةوطخلال يف هؤاشنإ مت ام سفن



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



Cisco لى تضرع in order to رمأ anyConnect vpn-sessionDB تضرع تضرع طسې تنأ، FTD نم

ة:يامحل راج ىلع ايلاح طشن ةسلج نوبز نمأي

```
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
```

اهحالصإو ءاطخال فاشكسا

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

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

عم لاصتالا قفدت ءظحال نمك مي Cisco، نم نمألا لي عمال ءاطخال حيحصت ىل ءفاضالاب ءرود ءحفاصم تايلمع ثالث لامكإ متي، حجان لاصتا ىلع لاثم اذه. اضيأ TCP ءمزح طاقتلا تايلمع ىلع ءقفاوملل مدختست SSL ءحفاصم اءبتي، FTD و Windows لي مع نيبري فشتلا.

The image shows a Wireshark capture of a network session. The top pane displays a list of captured packets. A red box highlights the first three packets:

- 13. 3.331222 10.31.124.34 → 10.31.124.25 TCP 66 51300 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 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 56 51300 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Below the packet list, the packet details pane shows the structure of the selected packets, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

تانايب ةحص نم ققحتلاب FTD موقى نأ بجي ،لوكوتوربلا لاصتالا ديكأت تايلمع دعب
 ي.لحمل قاطنلا يف ةنخمل تامولعمل مادختساب دامتعالا

ثحبل 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