

ةداهش ىلإ ةدنتسملا ةقداصملا نيوكت لقنتلا ءانثأ لوصولل AnyConnect

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[FTD ىلع Cisco AnyConnect نيوكت](#)

[ةكبشلال يطيطختلا مسرلا](#)

[FTD ىلإ ةداهش ةفاضلا](#)

[Cisco AnyConnect نيوكت](#)

[ةلومحملا ةزهجالا ىمدختسملا ةداهش ءاشنا](#)

[لومحملا زاهجالا ىلع تيبثتلا](#)

[فحصلا نم ققحتلا](#)

[اهخالص او ءاطخالا فاشكتسا](#)

[ءاطخالا ىحصت](#)

ةمدقملا

ةلومحملا ةزهجالا ىلع ةداهشلا ىلإ ةدنتسملا ةقداصملا ذيفنتلا الاثم دنتسملا اذه حضوي

ةيساسألا تابلطتملا

يه ليلدلا ىف ةمدختسملا ةزهجالا او تاودألا:

- Cisco FirePOWER (FTD) ديهت دض ءافدلا
- Firepower (FMC) ةرادا زكرم
- Apple iOS (iPhone, iPad) زاهج
- (CA) ةداهشلا حنم ةهج
- Cisco AnyConnect Client جم انرب

تابلطتملا

ةيلالاتلا ىض او ملاب ةفرعم كىدل نوكت نأب Cisco ىصوت:

- ةيساسألا VPN ةكبش
- SSL/TLS
- ماعلا حاتفملا ةيساسألا ةينبلا
- FMC عم ةبجرت
- OpenSSL

- Cisco AnyConnect

ةمدختسمل اتانوكملا

ةيلالاتل ةيدامل اتانوكملا او جم اربلا تارادصا اذف دننتسمل اذف ةدراولا تامولعمل دننتست

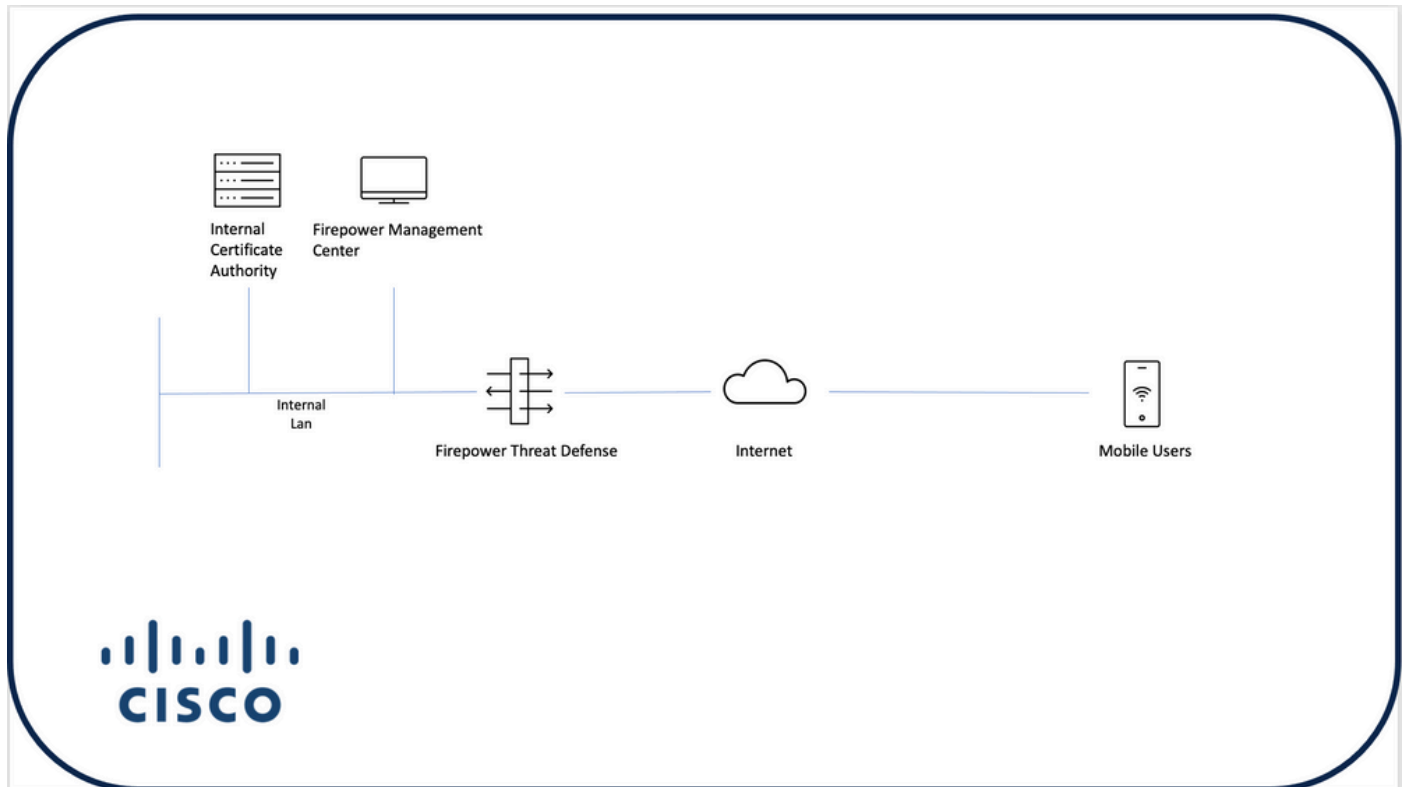
- Cisco FTD
- Cisco FMC
- Microsoft CA م داخ
- XCA
- Cisco AnyConnect
- داب ا لبا

ةصاخ ةيلمعم ةئيب يف ةدووملا ةزهجال نم دننتسمل اذف ةدراولا تامولعمل عاشن ا مت تناك اذف. (يضا رتفا) حوسمم نيوكتب دننتسمل اذف يف ةمدختسمل ةزهجال عيمج تادب رما ا ل لم تحملل ريثا تلل كمهف نم دكأتف ، ليغش تلا دي ق كتك ب ش

FTD لى Cisco AnyConnect نيوكت

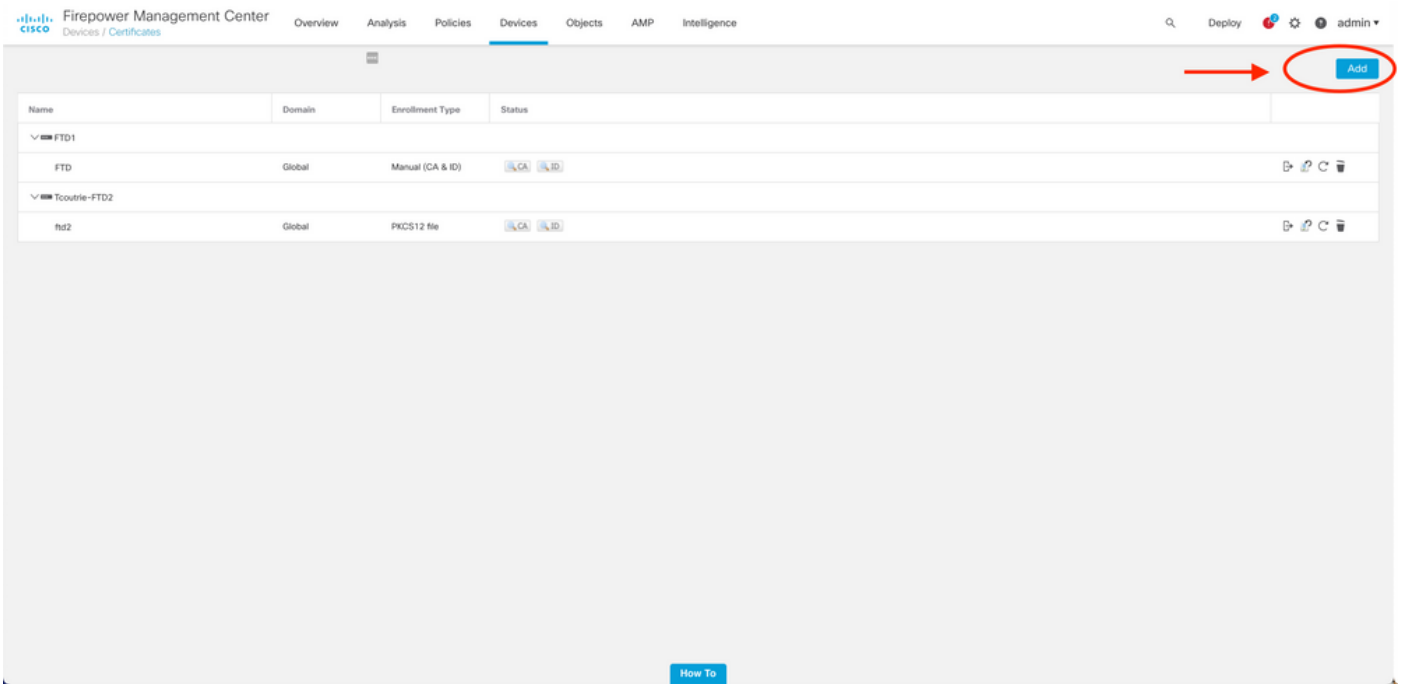
عيمج رشن نم دكأت ، عدبلا لبق . FMC ربع AnyConnect نيوكت تاوطخ مسقلا اذف فصى . اتانوكتلا

ةكبش لل يطي طختلا مسرلا

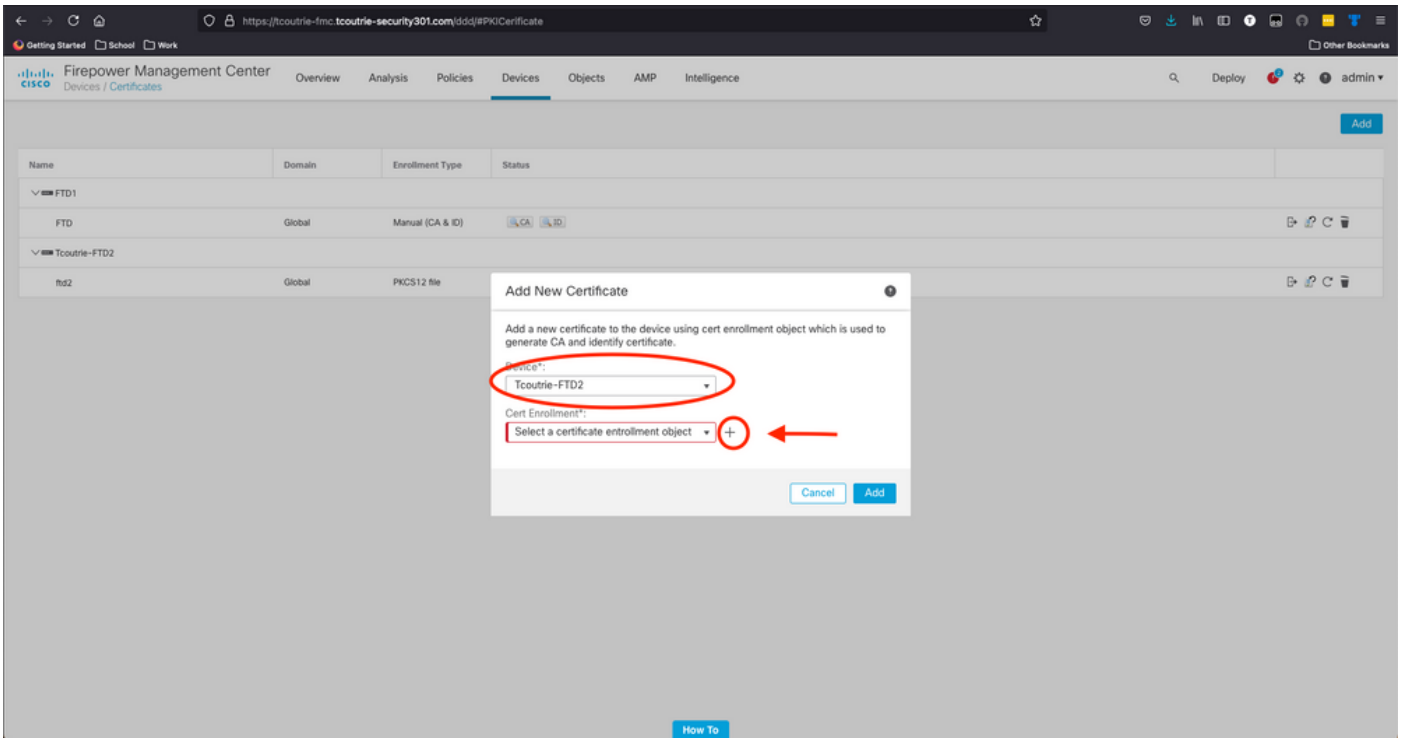


FTD لى ةداهش ةفاضل

رتخاو صيخرتلا > ةزهجالا يلا لقتنا FMC. زاخ يلع FTD ل ةداهش ءاشناب مق 1. ةوطخلا
ةروصلا هذه يف حضورم وه امك ، ةفاضلا



ةزهجالا ةلدسنملا ةمئاقلا نم FTD زاخ رتخأ. ليصوت VPN لال بغر ب FTD رتخأ. 2. ةوطخلا
ةروصلا هذه يف حضورم وه امك ، ديدج ةداهش ليحست بولسأ ةفاضلا + ةنوقيا يلع رقتنا



لوصحلل ةلفملا ةقيرطلا وه يذلا رايلخا رتخأ. زاخالا يلا تاداهشلا ةفاضلا مق 3. ةوطخلا
ةئيبلا يف تاداهشلا يلع

🔍 SCEP - اي لحمة عديج عدهاش عاشن | - ايتا ذة عقوم عدهاش : يه عحاتم ل تاراخي ل : حيم لت تي ب ت ، CA نم عدهاش ل ل ع لوصح ل ل طيس ب ل عدهاش ل ل ل ج س ت لوك و ت و ر ب م اد خ ت س ا ي و ه ل ل و ر ذ ج ل ل ب ع ر ف ش م ل عدهاش ل ل م ز ح ل ي م ح ت - PKCS12 ، ي و ه ل ل و ر ذ ج ل ل عدهاش ل ل - ي و د ي ص ا خ ل ل ح ا ت ف م ل ل و .

وه امك ، ظفح رقن او (طقف PKCS12) رورم ل زمر ل خ د ا . FTD زا ه ج ل ل عدهاش ل ل ل ي م ح ت . 4 ع و ط خ ل ل ع ر و ص ل ل ه ذ ه ي ف ح ص و م :

Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: Tcoutrie-ftd2.p12 [Browse PKCS12 File](#)

Passphrase:

Skip Check for CA flag in basic constraints of the CA Certificate

[Cancel](#) [Save](#)

✎ ل ي ص ا ف ت عدهاش م ل . ر و ف ل ل ل ع ت ا د ا ه ش ل ل ر ش ن م ت ي ، ف ل م ل ل ظ ف ح ذ ر ج م ب : ع ط ح ا ل م

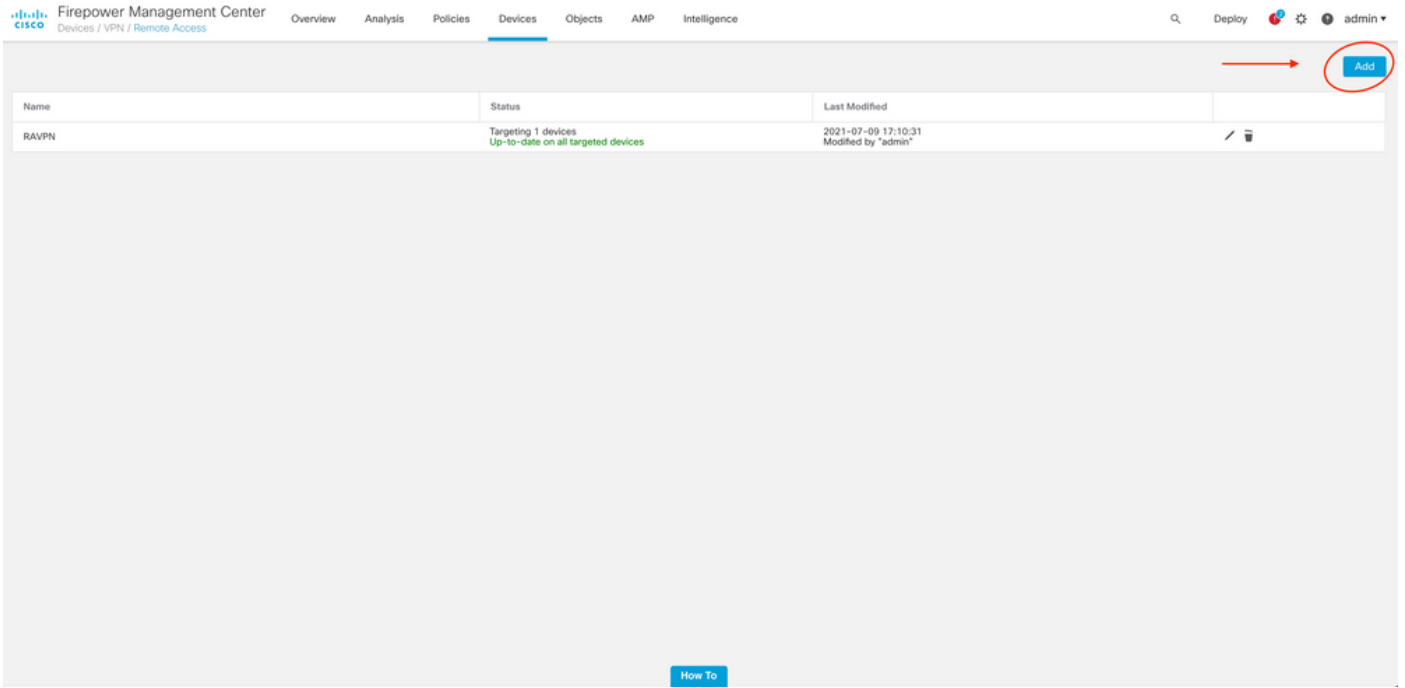
فروعنا رتخأ، ةداهشلا

Cisco AnyConnect نيوكت

دعب نع لوصول جلاعم مادختساب FMC ربع AnyConnect نيوكتب مق

AnyConnect نيوكتل Remote Access VPN جهن جلاعم ليغشت ادب. 1. ةوطخلا

Add رتخاو (دعب نع لوصول) Remote Access > ةزهألا ىلا لقتنا



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' tab is selected. The main content area displays a table with the following data:

Name	Status	Last Modified
RAVPN	Targeting 1 devices Up-to-date on all targeted devices	2021-07-09 17:10:31 Modified by "admin"

An 'Add' button is highlighted with a red circle and an arrow in the top right corner of the interface.

جهنلا نيوكت 2. ةوطخلا

جهنلا نيوكت لامك:

ا. ةسايسلا ةيمستب مق.

ب. ةبولطملا VPN تالوكتورب رتخأ.

ج. نيوكتلا قيبطتل فدهتسملا زاهجلا رتخأ.

Remote Access VPN Policy Wizard

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

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:

Description:

VPN Protocols:

SSL

IPsec-IKEv2

Targeted Devices:

Available Devices: FTD1 Tcoutire-FTD2

Selected Devices: Tcoutire-FTD2

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure RADIUS 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.

How To Cancel Back Next

3. لاصتال فيرعت فلم 3. ةوطخلال

لاصتال فيرعت فلم مسا أ.

طقف لي عمل ةداهش لىل ةقداصلال بولسا نيي عت ب.

ديج ةومجم جهن ءاشناب مق ،رمال مزلا اذوا ،IP نيوان ع عمجت نيي عت ب مق ج.

لكذ دع ب تقطوط د.

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet VPN Device 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:

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:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS or RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pool:

IPv6 Address Pool:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:

Edit Group Policy

تاسل لمل مدختس مل مسا لاخدال هم ادختسا دارمل ياساسأل لقحل رتأ: ةظالم ليل دل اذو في ةداهش لىل CN مدختس ي. ةقداصلال

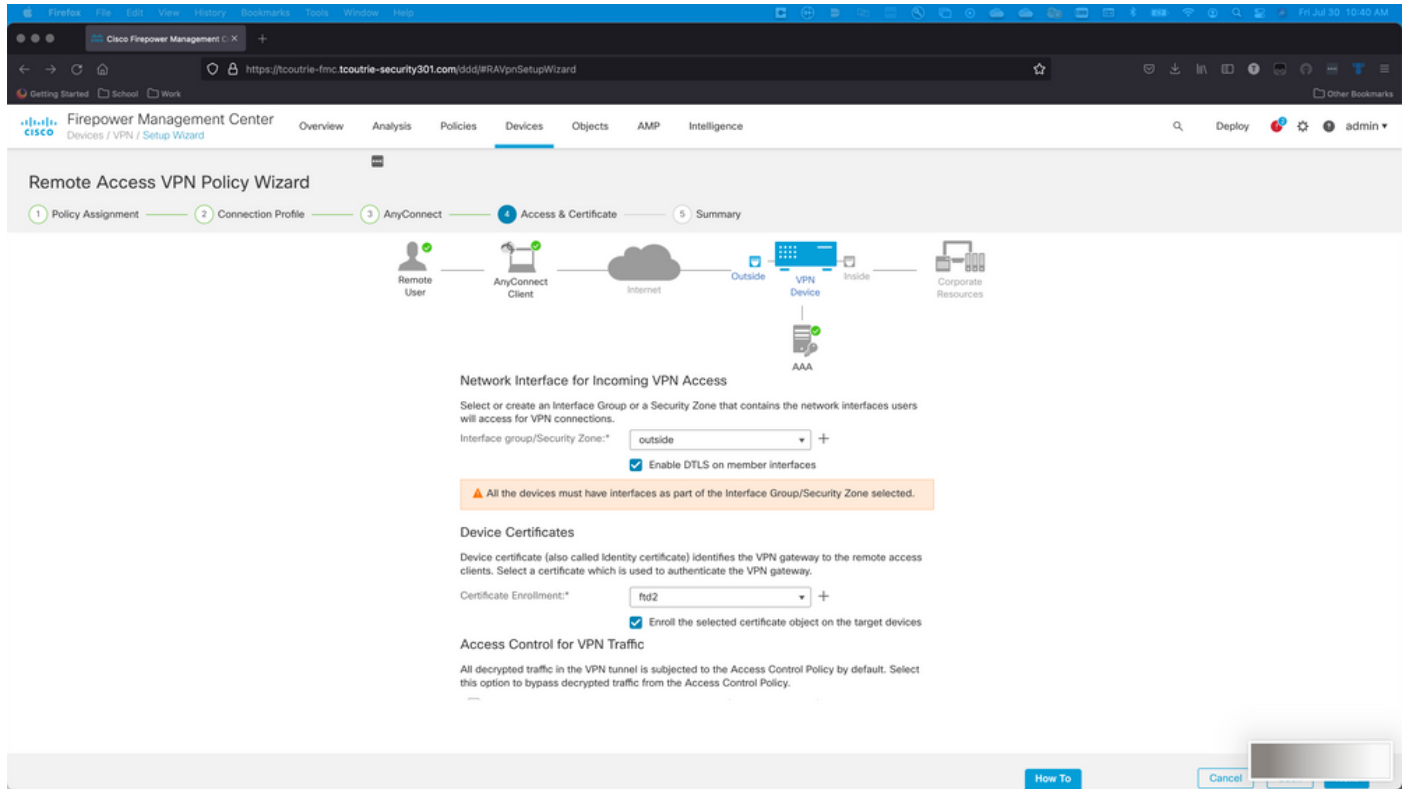
4. AnyConnect. ةوطخلال

رقن او AnyConnect نم لضفم ل رادصل ل ليمحتب مق .زاهل ل لى ل AnyConnect ةروص ةفاضل
يل ل قوف

 Cisco AnyConnect نم Software.cisco.com مزح ل ليزنت نكمي :ةظالم

ةداهش ل ل وصولا 5. ةوطخل

يف حضورم وه امك ،ةهجال ل ل وتسم لى ل AnyConnect ني كمتو ةهجال ل ل ع ةداهش ل ل قيبطت مق
يل ل قوف رقال ل ،ةروصل ل هذه



The screenshot shows the Cisco Firepower Management Center interface for the Remote Access VPN Policy Wizard. The wizard is currently on the 'Access & Certificate' step (step 4 of 5). The interface includes a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main content area displays a network diagram showing a Remote User connecting to an AnyConnect Client, which connects to the Internet, then to an Outside interface of a VPN Device, and finally to Corporate Resources. Below the diagram, there are configuration options for the Network Interface for Incoming VPN Access, Device Certificates, and Access Control for VPN Traffic. The 'Interface group/Security Zone' is set to 'outside', and 'Enable DTLS on member interfaces' is checked. A warning message states: 'All the devices must have interfaces as part of the Interface Group/Security Zone selected.' The 'Certificate Enrollment' is set to 'ftd2', and 'Enroll the selected certificate object on the target devices' is checked. At the bottom right, there are 'How To', 'Cancel', and 'Next' buttons.

صخلم 6. ةوطخل

رشنل ل م ءاهن ل قوف رقال ،بحس ل ل تاي لمع ةفاك بحس مت اذ . تانويكت ل ل عجار

ةلومحمل ل ةزهجال ل ل يمدختسمل ةداهش عاشن ل

ل ل يصوت ل ل ي ف ممدختسمل ل لومحمل ل زاهل ل ل ل اهتفاضل ل ةداهش عاشن ل

ةوطخل 1. XCA.

أ - حتف XCA

ةديج تاناي ب ةدعاق ل ل يغشت ءدب . ب

ةوطخل 2. عاشن ل ل CSR.

أ. (CSR) ةداهش ل ل عي قوت بلط رتخأ .

ب. ديدج بلط رايتخا .

ج. دةاهشلل ةمزاللا تامولعمللا لك عم ةميقلال لخدأ .

د. ديدج حاتفم عاشنا .

ه. قفاوم قوف رقنا ،ءاهتناالا دنع .

X Certificate and Key management

Create Certificate signing request

Source Extensions Key usage Netscape Advanced

Distinguished name

Internal name		organizationName	
countryName		organizationalUnitName	
stateOrProvinceName		commonName	Cisco_Test
localityName		emailAddress	

Type	Content
------	---------

Add
Delete

Private key

Cisco_Test_1 (RSA:2048 bit) Used keys too

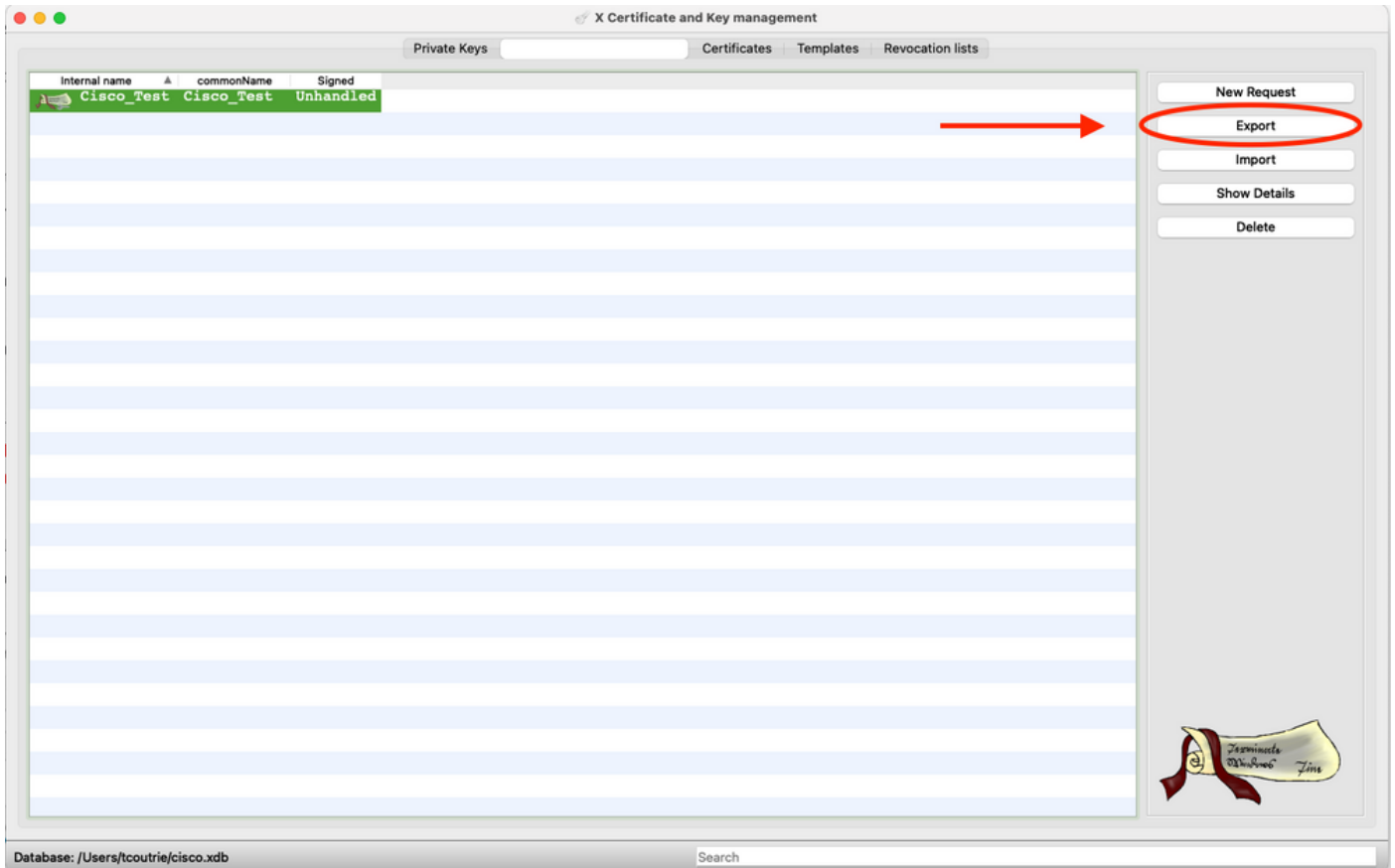
Cancel OK

د. دةاهشلاب صاخلا CN دنن سمللا اذه مدختسي :ةظحالم

CSR لاسرا .3 ةوطخلا

تاك رشلل ةيعامتجالا ةيلوؤسمللا ري دصت - أ

ب. ديدج ةداهش يلع لوصحلل CA لىل CSR مي دقت .



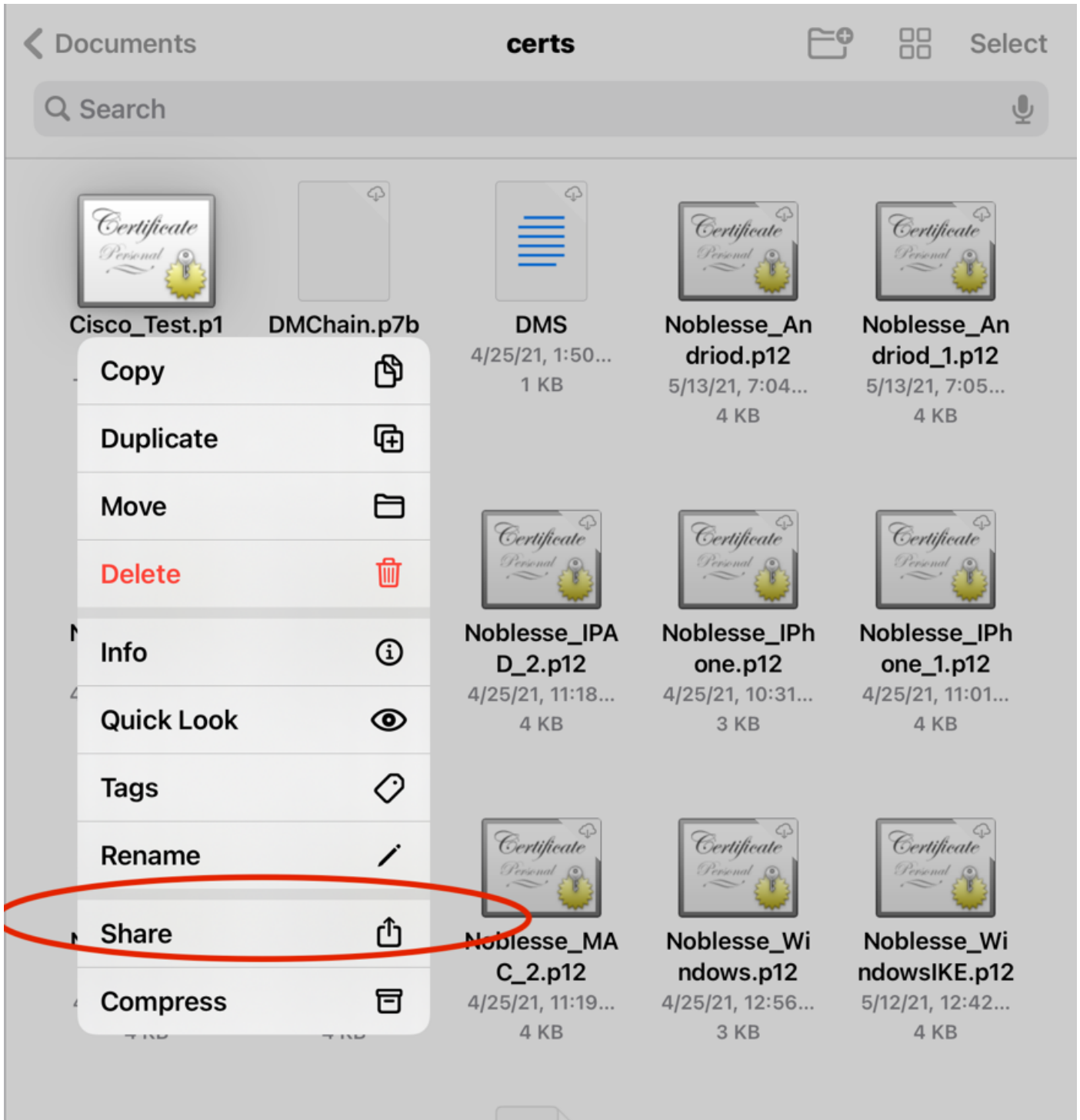
✎ ب صااال PEM قيسنت مداسأ: ةاال م

لومال زاهال ال ع ابااال

لومال زاهال ال ال زاهال ةااش ةااضا 1. ةواال

ااال ةااشال قبااال ةااضا ال AnyConnect قبااال عم ةااشال كراش 2. ةواال

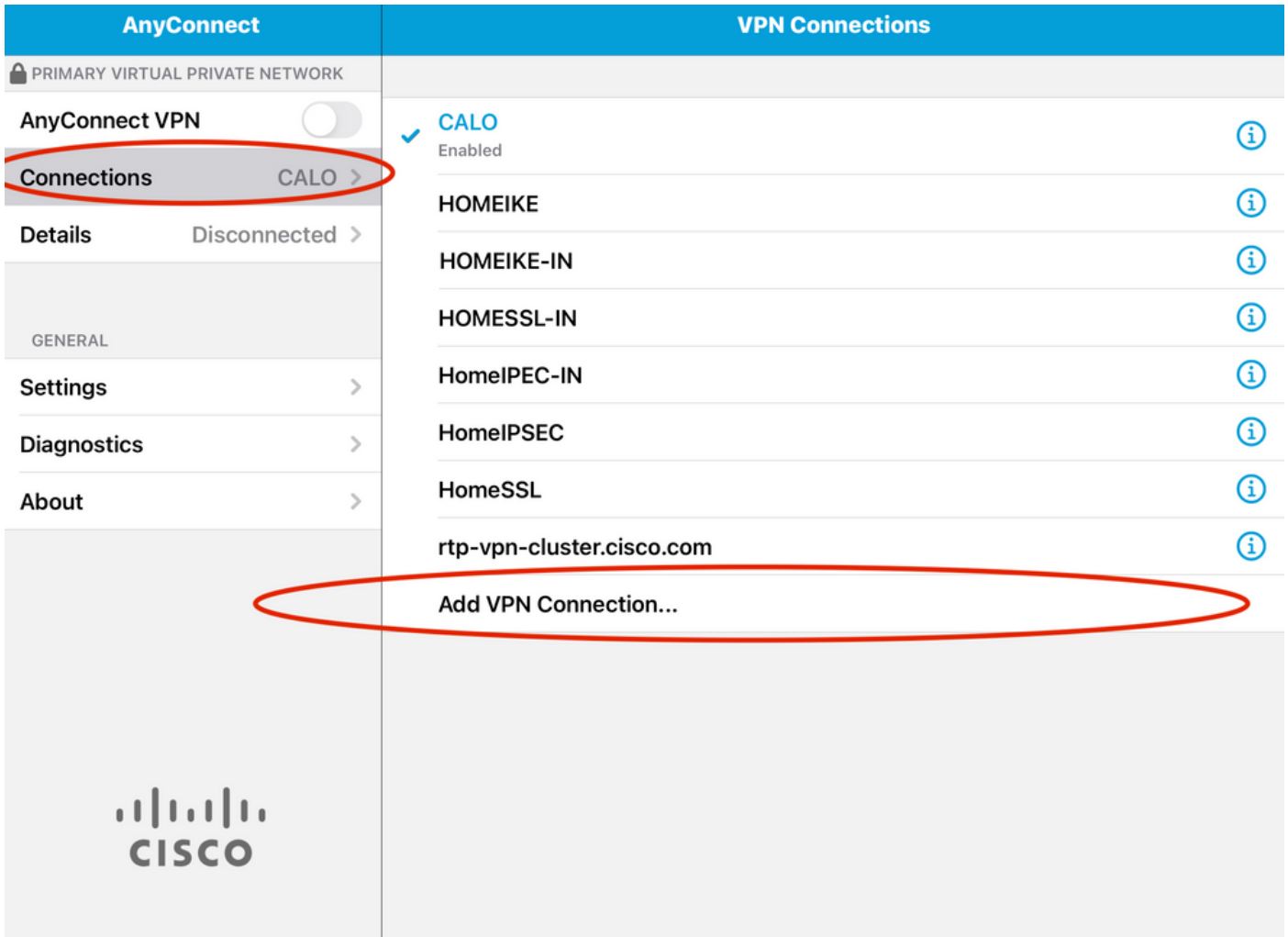
⚠ ال قبااال عم ةااشال ةكراشم مداسم ال نم وابل ابااال بلطال: ربااال مDMs رب اعف مابل ال اااشال ال ع ااال قبااال



3. ةوطخال PKCS12 فلمل ةداهشلا رورم ةم لك لخدأ.

4. ةوطخال AnyConnect لىل ةديج لاصتاءاشنإ.

5. ةوطخال VPN لاصتاءافاضإ > تالاصتإ؛ ةديج تالاصتإ لىل لقتنا.



ديدجل لاصتال تامولعم لخدأ 6. ةوطخل

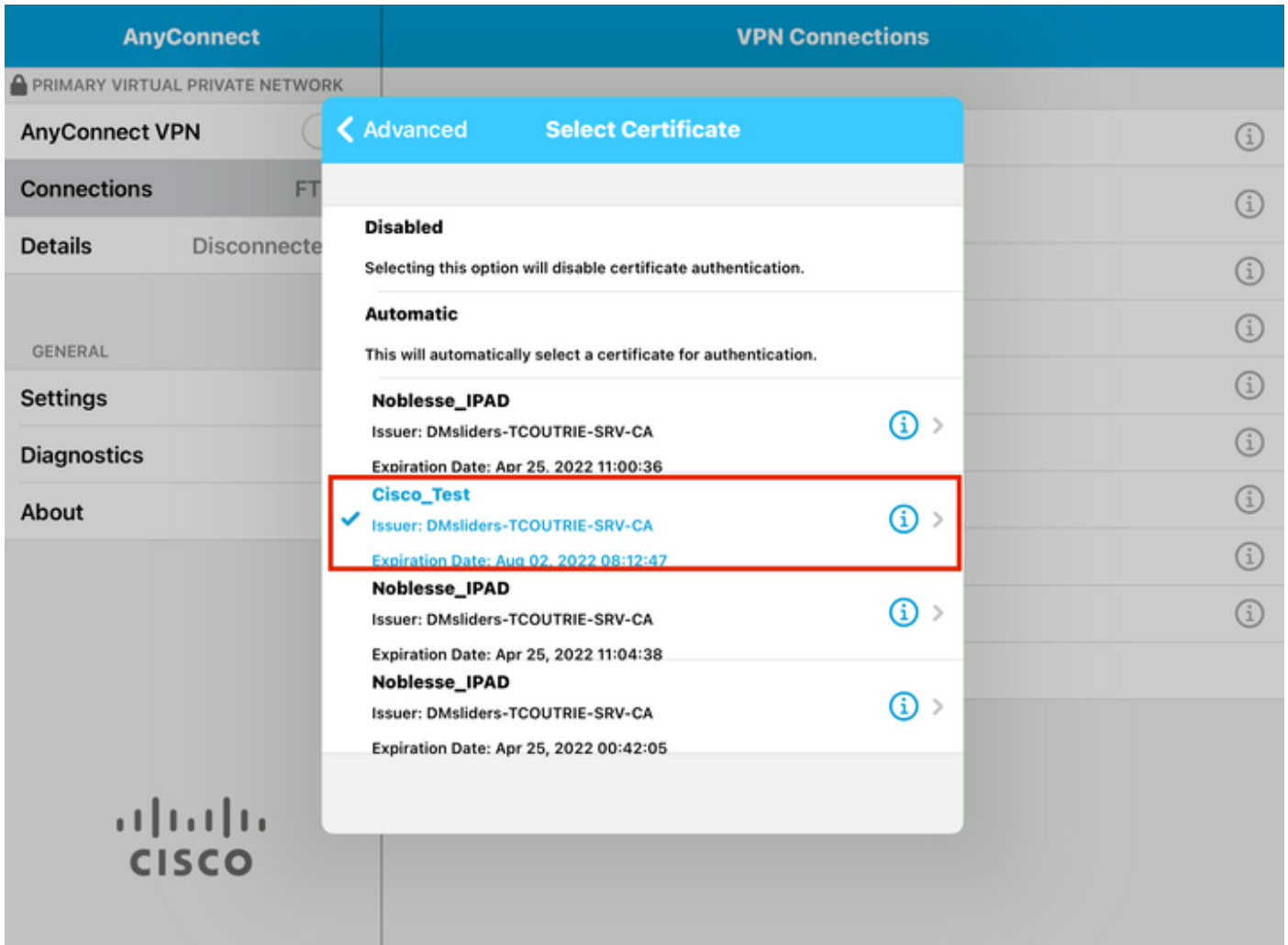
لاصتال ةيمست :فصولا

FTD ب صاخلا FQDN و IP ناوع :مداخل ناوع

ةيفاضا تانويك :مدقتم

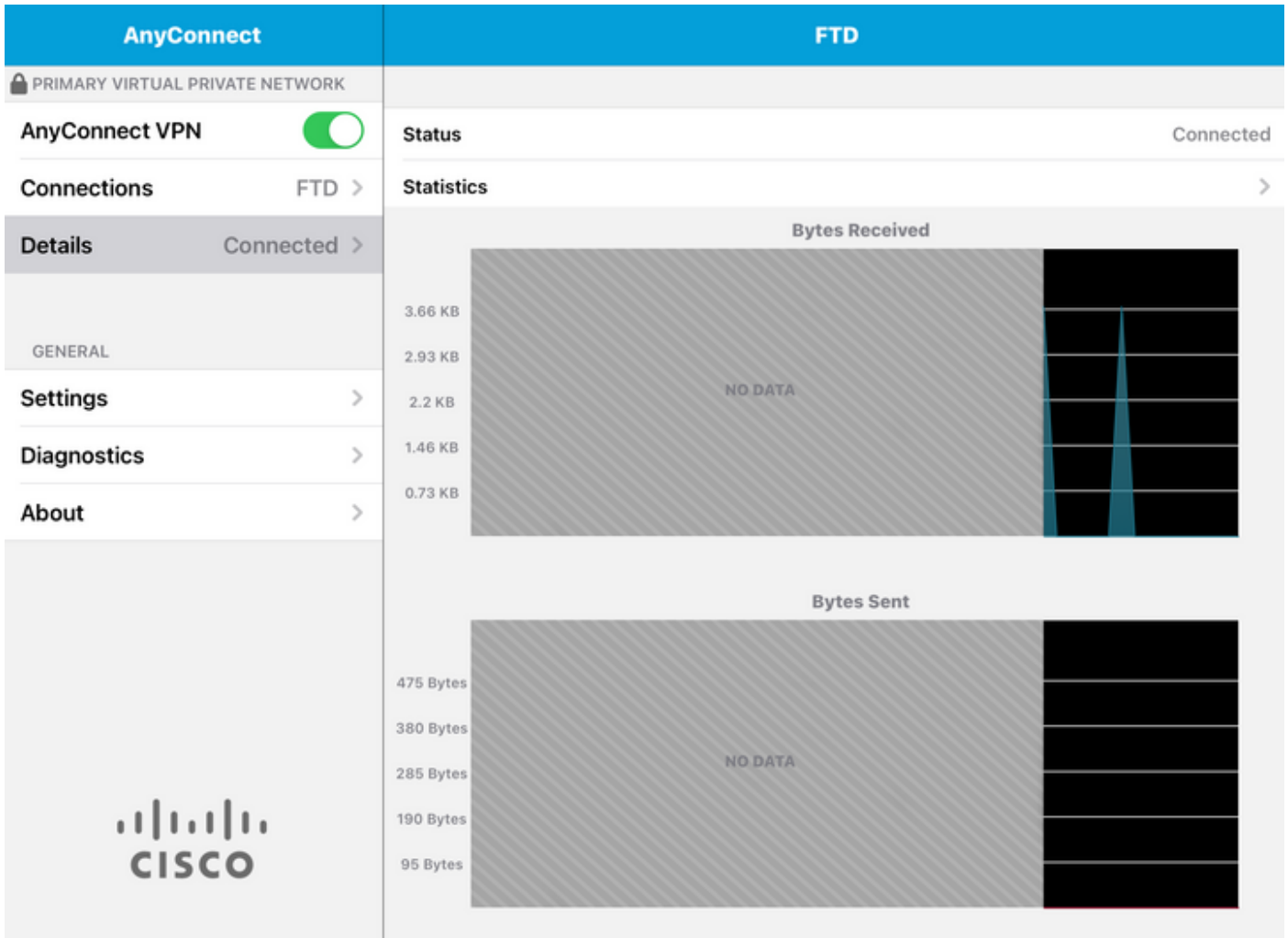
مدقتم رتخأ 7. ةوطخل

اثير اهتفاضل تمت يتلا كتداهش رتخاو صيخرت رتخأ 8. ةوطخل



رابط خال او اتالاصت الال إلى ىرخأ ةرم لاقتن الالاب مق 9 ةوطخال

ةالخال الالاصت الال رهظتو لىغشت الال دىق لىدبت الال ىقبى، لىدبت الال حاجن درجمب



ةحصلا نم ققحتلا

لصتملا فيضملا لوح تامولعمل اعيمج AnyConnect detail vpn-sessionDB show رمألا ضرعي.

تمت يتي التلا 'sort' وأ 'filter' ثحبلا تاملك وه رثكأ رمألا اذه فيصتلا راخلا: حيملت رمألا إلى اهتفاضاً

لثملا ليلبس لعل:

```
Tcourtie-FTD3# show vpn-sessiondb detail Anyconnect
```

```
Username : Cisco_Test Index : 23
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel
License : Anyconnect Premium, Anyconnect for Mobile
Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 8627 Bytes Rx : 220
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : SSL Tunnel Group : SSL
Login Time : 13:03:28 UTC Mon Aug 2 2021
```

Duration : 0h:01m:49s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a7aa95d000170006107ed20
Security Grp : none Tunnel Zone : 0

Anyconnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Anyconnect-Parent:
Tunnel ID : 23.1
Public IP : 10.118.18.168
Encryption : none Hashing : none
TCP Src Port : 64983 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : apple-ios
Client OS Ver: 14.6
Client Type : Anyconnect
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 6299 Bytes Rx : 220
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 23.2
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 64985
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : SSL VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 2328 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 23.3
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 51003
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : DTLS VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

اهحالصإو عاطخأل فاشكسا

ءاطخأل احيصت

وه اءال صإوءة لكشمل اءه ءاطخأ فاشك تسال بولطمل احيصتال

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

اذل SSL سئل و IPsec وه لالصتال ناك اذل

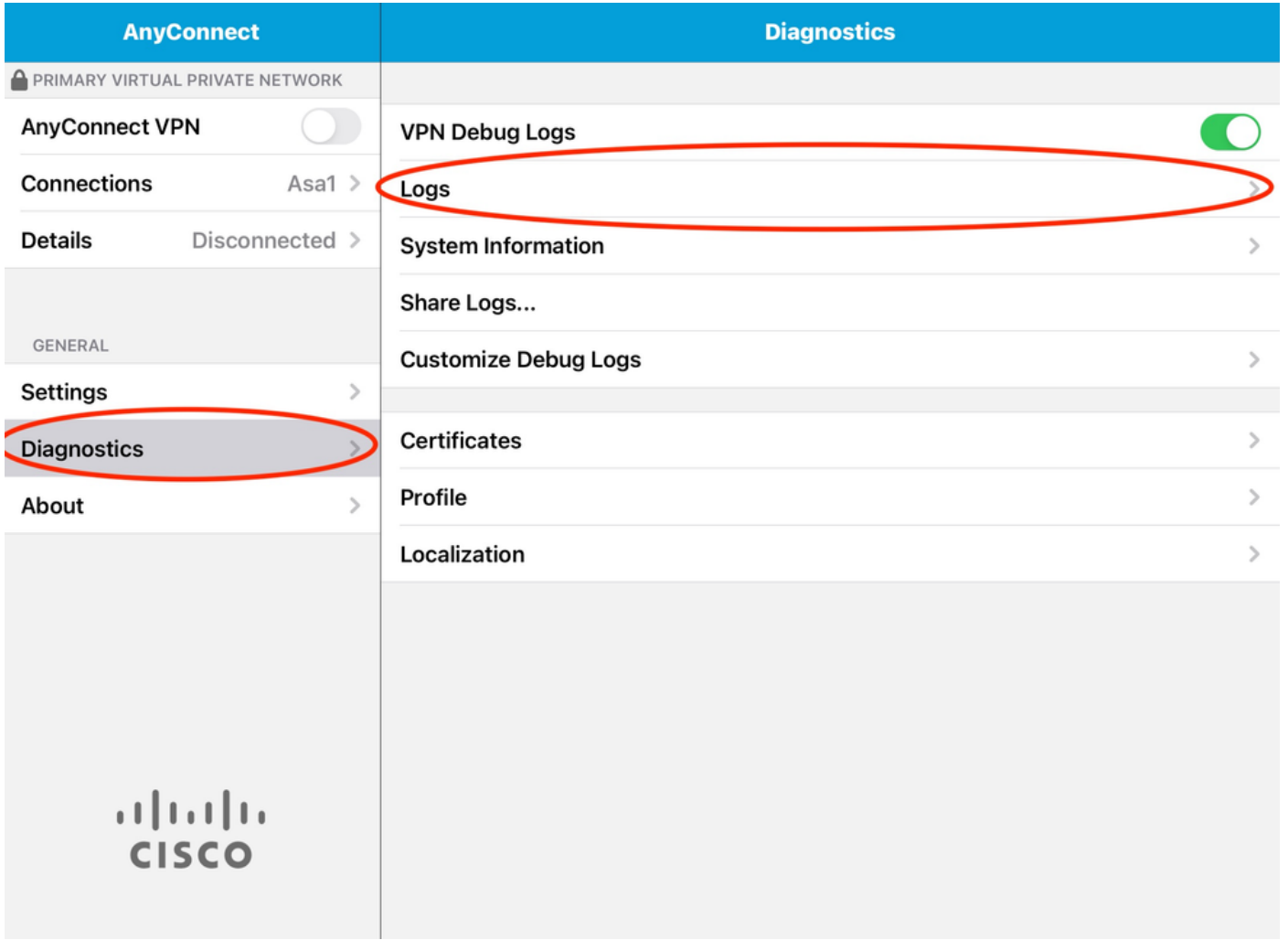
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

ةلومءملا ءزهألل AnyConnect قيبطت نم تالءسل

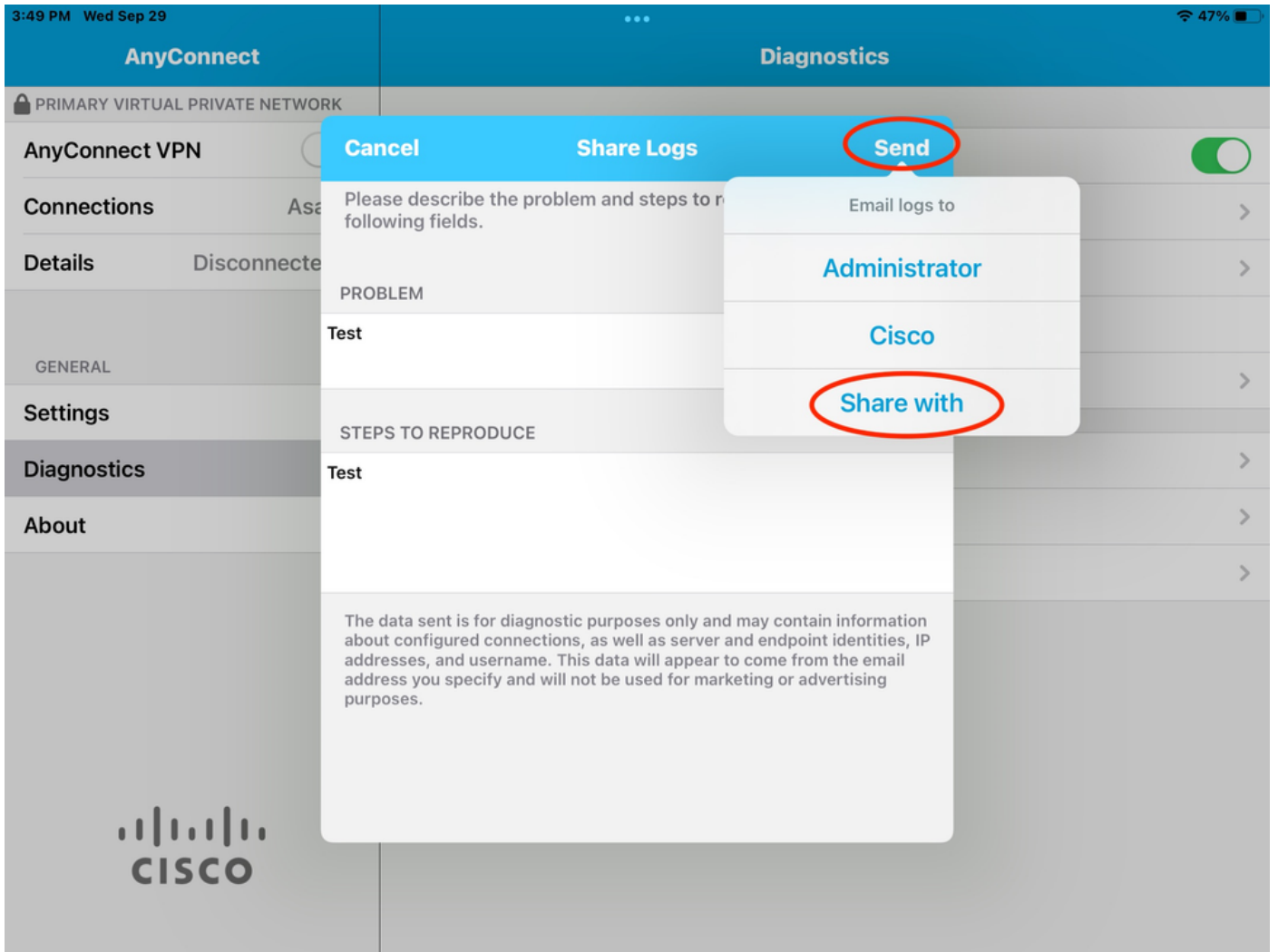
.تالءسل ءكراشم > VPN ءاطخأ احيصت تالءس > صيخشتال للاقنا



تامولعملالخدأ:

- ةلكشملا
- رثاكتلل تاوطخ

عم ةكراشم > لاسراىللقتنا مث



تالچس لاس رال ینورثک ل دیرب لی مع مادختس ا رایخ مدقی اذو.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا 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 ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م اء 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 (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا