

عداهش ىلإ ةدنتسملا ةقداصملا نيوكت لقننلا ءانثأ لوصولل AnyConnect

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تاب لطلتلا](#)

[ةمدختسملا تانوكملا](#)

[FTD ىلغ Cisco AnyConnect نيوكت](#)

[ةكبش لىطىطختلا مسرلا](#)

[FTD ىلغ عداهش ةفاضلا](#)

[Cisco AnyConnect نيوكت](#)

[ةلومحمل ةزهجالا يمدختسملا عداهش ءاشنلا](#)

[لومحمل زاهجالا ىلغ تيبثتلا](#)

[فحصلا نم ققحتلا](#)

[اوخالص او عاخذالا فاشكتسا](#)

[عاخذالا حيحصت](#)

ةمدقملا

ةلومحمل ةزهجالا ىلغ عداهش ىلإ ةدنتسملا ةقداصملا ذيفنتل الاثم دنتسملا اذه حضوي.

ةيساسالاب لطلتلا

يه ليلدل ي ف ةمدختسملا ةزهجالا او تاودالا:

- Cisco FirePOWER (FTD) ديهت دض عافدلا
- Firepower (FMC) ةرادا زكرم
- Apple iOS (iPhone, iPad) زاهج
- (CA) عداهشلا حنم ةهج
- Cisco AnyConnect Client حمانرب

تاب لطلتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

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

- Cisco AnyConnect

ةمدختسمل تانوكمل

ةيلاتلا ةيداملا تانوكمل اوجماربل تارادصا ىلإ دنتسمل اذه يف ةدراول تامولعمل دنتست

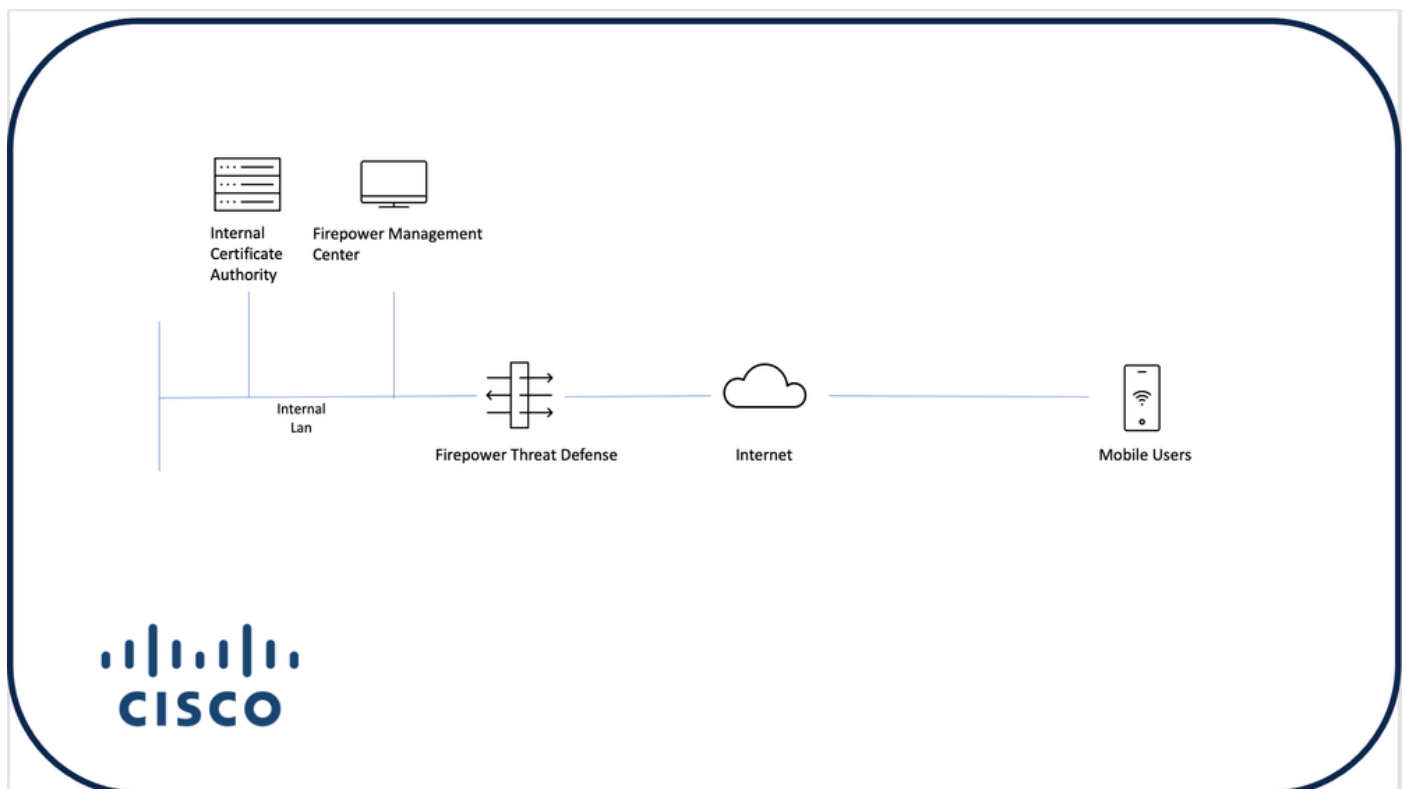
- Cisco FTD
- Cisco FMC
- Microsoft CA مداخ
- XCA
- Cisco AnyConnect
- داب يآ لآ

ةصاخ ةيلمعم ةئيىب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتك كتبش

FTD ىلع Cisco AnyConnect نيوكتب

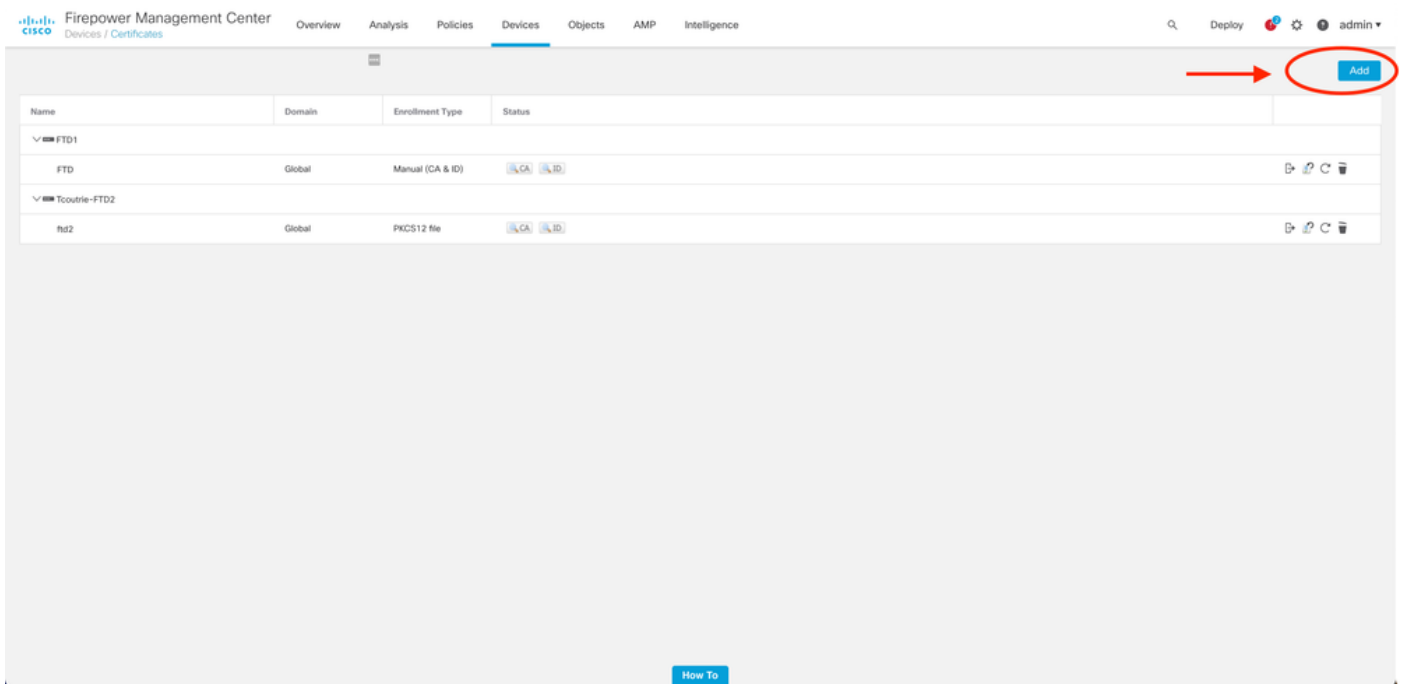
عيمج رشن نم دكأت ،ءدبل لبق .FMC ربع AnyConnect نيوكتب تاوطخ مسقلا اذه فصى تانوكتبلا .

ةكبشلل يطيختلا مسرلا

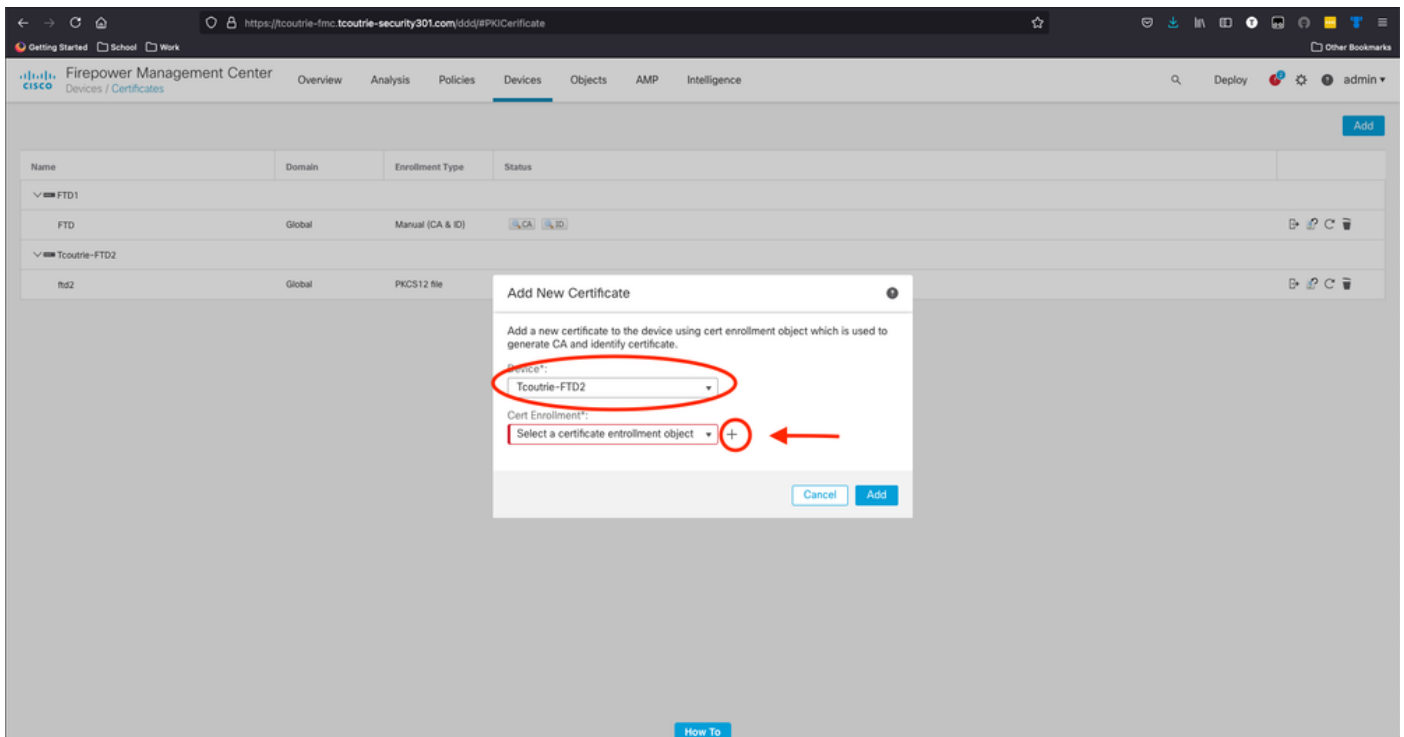


FTD ىلإ ةداهش ةفاضإ

رتخاو صيخرتل > ةزهجالا ىلا لقتنا FMC زاهج ىلع FTD ل ةداهش عاشناب مق 1. ةوطخلا
 ةروصلال هذه يف حضوم وه امك ، ةفاضل:



ةزهجالال ةلدسنملا ةمئاقلا نم FTD زاهج رتخأ . ليصوت VPN لال ب غر ب FTD لال 2. ةوطخ تترتخأ
 ةروصلال هذه يف حضوم وه امك ، ديدج ةداهش ليحست بولسأ ةفاضلال + ةنوقيأ ىلع رقتنا



ىلع لوصحلل ةلصفملا ةقيرطال وه يذلا راىخل رتخأ . زاهجالا ىلا تاداهشال فضا 3. ةوطخلا
 ةئيبال يف تاداهشال

🔍 SCEP - اي لحم ةديج ةداهش ءاشن | - ايتاذ ةعقوم ةداهش :يه ةحاتم ل تاراخي ل :حيملت تيبتت ، CA نم ةداهش ىل ع لوصحلل طيسب ل ةداهش ل ليحست لوكوتورب مادختسا ةيولال و رذلابل ةرفشم ل ةداهش ل ةمزل ليحت - PKCS12 ، ةيولال و رذلال ةداهش ل يودي صاخال حاتفم ل و .

وه امك ، ظفح رقناو (طقف PKCS12) رورم ل زمر لخدأ . FTD زاهج ىل ةداهش ل ليحت 4. ةوطخل ةروصلال هذو يف حضورم :

Add Cert Enrollment

Name*

ftdcert

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

✎ ةداهشمل .اروف ثدحت تاداهش ل رشن ةيلمع نإف ، فلم ل ظفحب موقت نأ درجبم :ةطخالمل

✎ فرع مالا رتخأ ،ةداهش لال لي صافات

Cisco AnyConnect ني وكت

دع ب نع لوصولال جلالع م مادختساب FMC ربع AnyConnect ني وكت ب مق

AnyConnect ني وكت ل Remote Access VPN جهن جلالع م لي غشت ادب .1 ةوطخال

Add. رتخاو (دع ب نع لوصولال) Remote Access > ةزهجالا لال 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 columns: Name, Status, and Last Modified. The table contains one entry: 'RAVPN' with status 'Targeting 1 devices' and 'Up-to-date on all targeted devices'. The 'Last Modified' column shows '2021-07-09 17:10:31' and 'Modified by "admin"'. A red arrow points to the 'Add' button in the top right corner of the table.

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

جهنلالي ني عت 2. ةوطخال

جهنلالي ني عت لامك:

جهنلالي م ستب مق أ.

ب. رغ رب لوكوتورب VPN لال رتخأ .

ني وكت لال قيبطتل فدهتسم لال زاهجال رتخأ .c.

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

Tcoute-FTD2

Selected Devices: Tcoute-FTD2

How To

Cancel Back Next

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.

للاصتال فيرعت فلم 3. ةوطخل

للاصتال فيرعت فلم ةيمستب مق أ.
طقف لي عمل ةداهش لىل ةقداصل بولسأ نييعت ب.

ديج ةومجم هن ءاشناب مق، رمال مزلا اذوا، IP نيوانع عمجت نييعت مق ج.

(يلاتال) Next قوف رقنا د.

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet Cloud VPN Device AAA Corporate Resources

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 Pools:

IPv6 Address Pools:

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



تاسللج مدختسمال مسا لاخداال هم ادختسا دارمال ياسالال لقحلال رتخأ: ةطخالما
لليلللا اذه يف ةداهشلل CN مدختسري. ةقداصلما

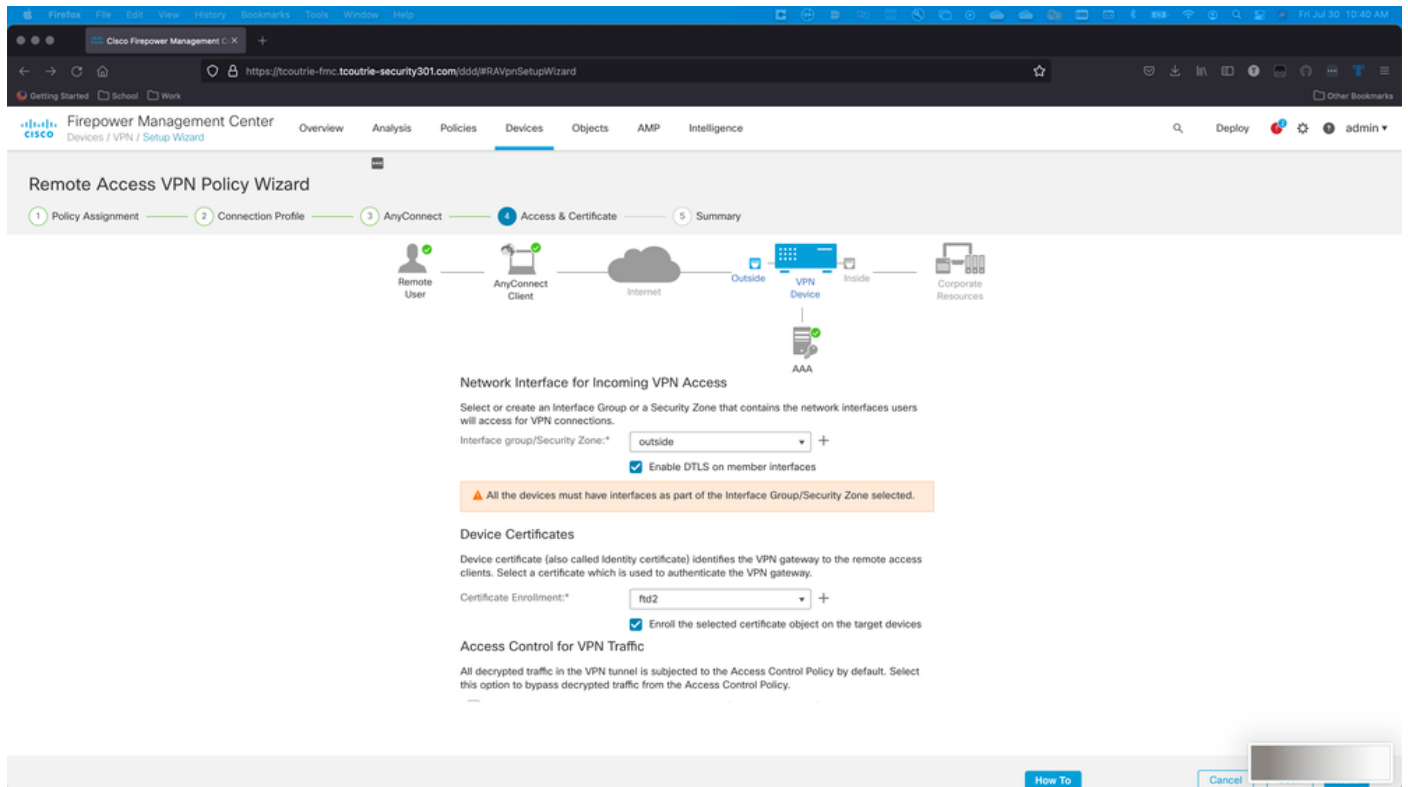
للاصتال فيرعت فلم 4. AnyConnect.

رقن او AnyConnect نم لصفم لادصل ليمحتب مق .زاهل الى AnyConnect ةروص ةفاضل
يلال قوف .

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

ةداهشل او لوصول 5. ةوطخل

يف حضوم وه امك ،ةهاولا يوتسم يل AnyConnect نيكمتو ةهجاو يل ةداهشل قيبطت مق
يلال قوف رقن او ،ةروصل هذه



صخلم 6. ةوطخل

رشنل مث ءاهنل قوف رقن ،بحسل تاي لمع ةفاك بحس مت اذ .تانويكتل عجار

ةلومحمل ةزهأل يمدختسمل ةداهش ءاشنل

ليصوتل ي ف ممدختسمل لومحمل زاهل الى اهتفاضل ةداهش ءاشنل

1. XCA. ةوطخل

XCA حتف أ.

ةديج تاناي ب ةدعاق ءدب .ب

CSR ءاشنل 2. ةوطخل

(CSR) ةداهشل عي قوت بلط رتخأ أ.

ديج بلط رايتخا ب.

ةداهشلل ةمزاللا تامولعمل لك عم ةميقلال لخدأ ج.

ديج حاتفم عاشنا د.

قفاوم قوف رقنا، ءاهتنال دن ع ه.

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 Generate a new key

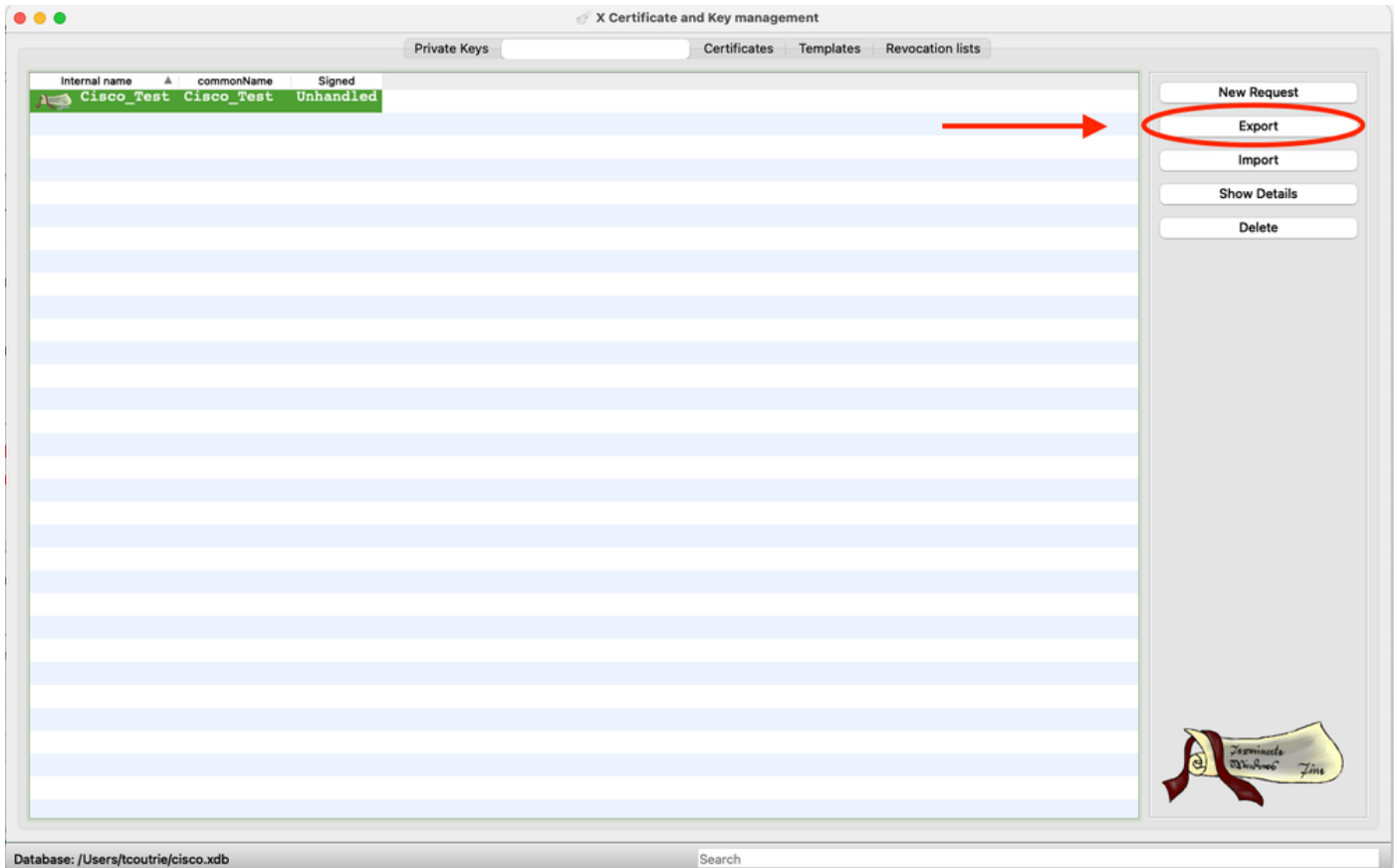
Cancel OK

ةداهشلاب صاخلا CN دنتسملا اذه مدختسي :ةظحالم

CSR لاسرا 3. ةوطخلا

CSR ري دصت أ.

ةديج ةداهش يلعل لوصحلل CA يلإ CSR لاسرا ب.



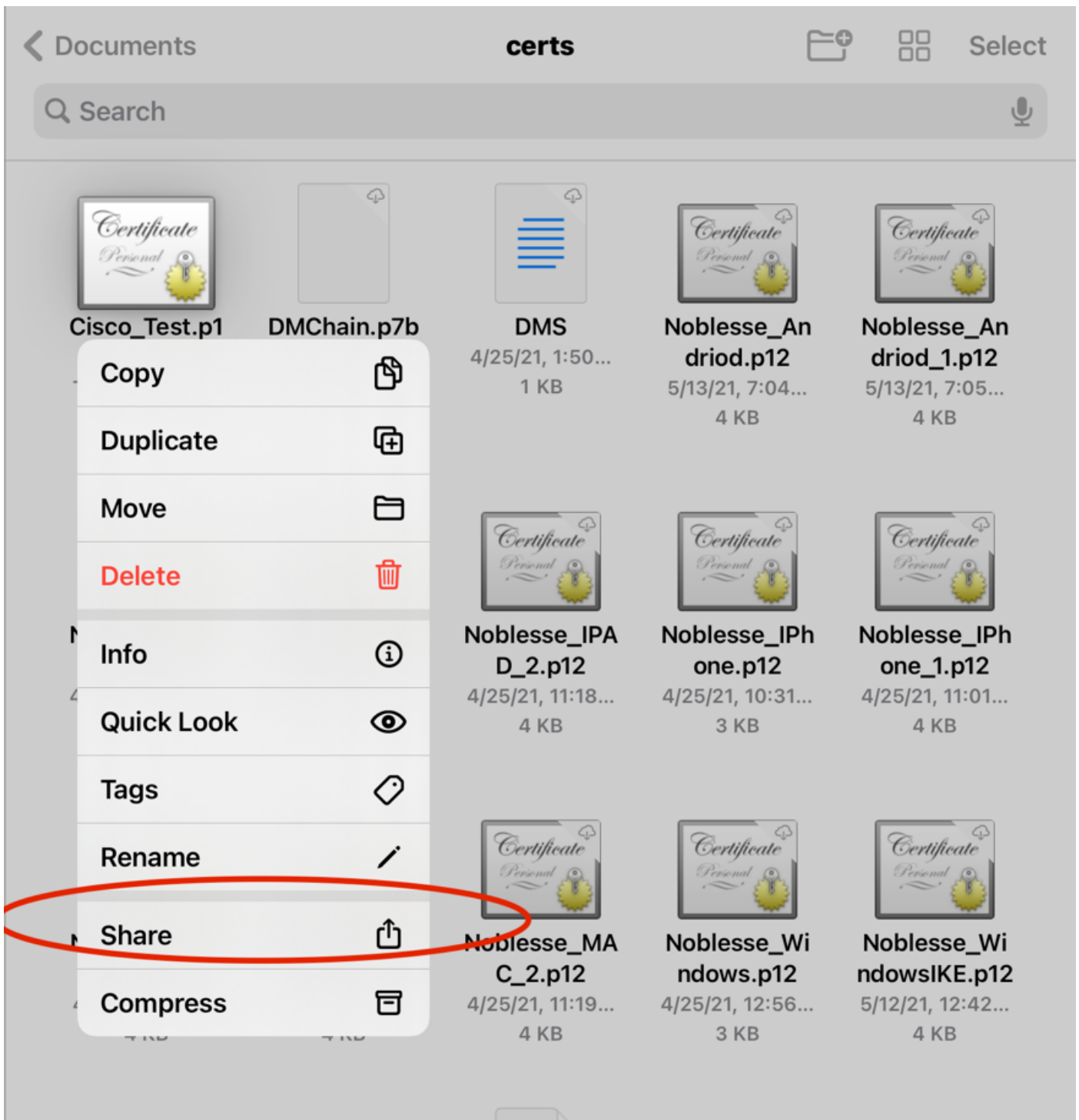
✎ CSR ب صاخال PEM قيسنت مدختسأ: ةطخال م

لومحمل زاهال لىل ع تيبتال

لومحمل زاهال لىل زاهال ةداهش ةفاضل 1. ةوطخال

ديج ةداهش قيبطت ةفاضل AnyConnect قيبطت عم ةداهشال كراش 2. ةوطخال

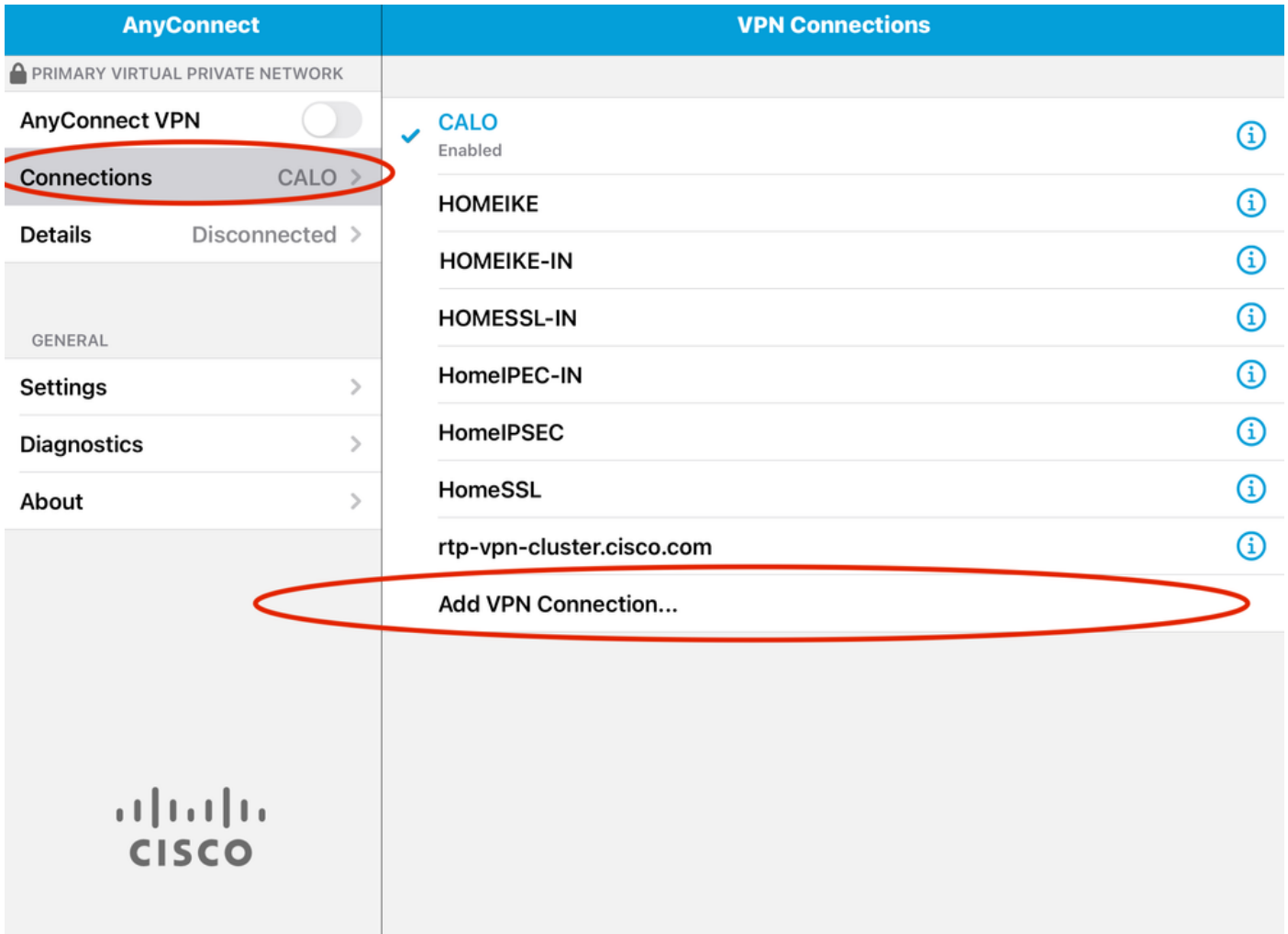
⚠ ال قيبطتال عم ةداهشال مدختسمال كراشي نأ يوديال تيبتال بلطتي: ريذحت
MDMs ربع اهعفد متي تيبتال تاداهشال لىل اذه قبطني



دربم PKCS12 ل ەملك ەداهش 3. ەوطخ لخدې

AnyConnect ىل ع دېدج لاصتاءاشن 4. ەوطخال

VPN لاصتاءافاضا > تالاصتالا؛ ەدېدج تالاصتالا لىلقنتا 5. ەوطخال



دي دجل لاصتال لة مولعمل ال 6. ةوطخ لخد

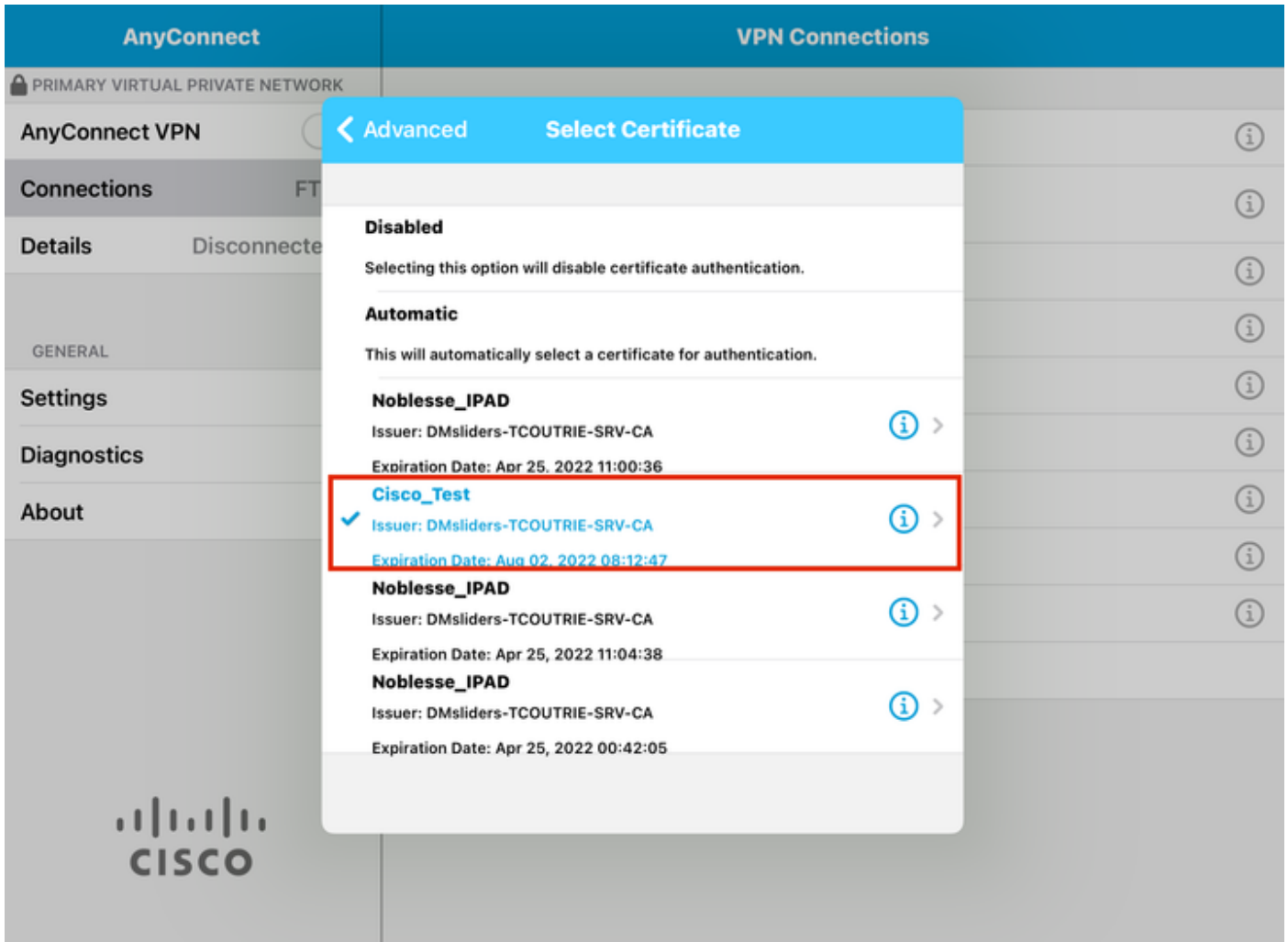
لاصتال الة يمستب مق :فصول

FTD ب صاخ ال FQDN و IP ناوع :مداخل ناوع

ةيفاضا تانيوكت :مدقتم

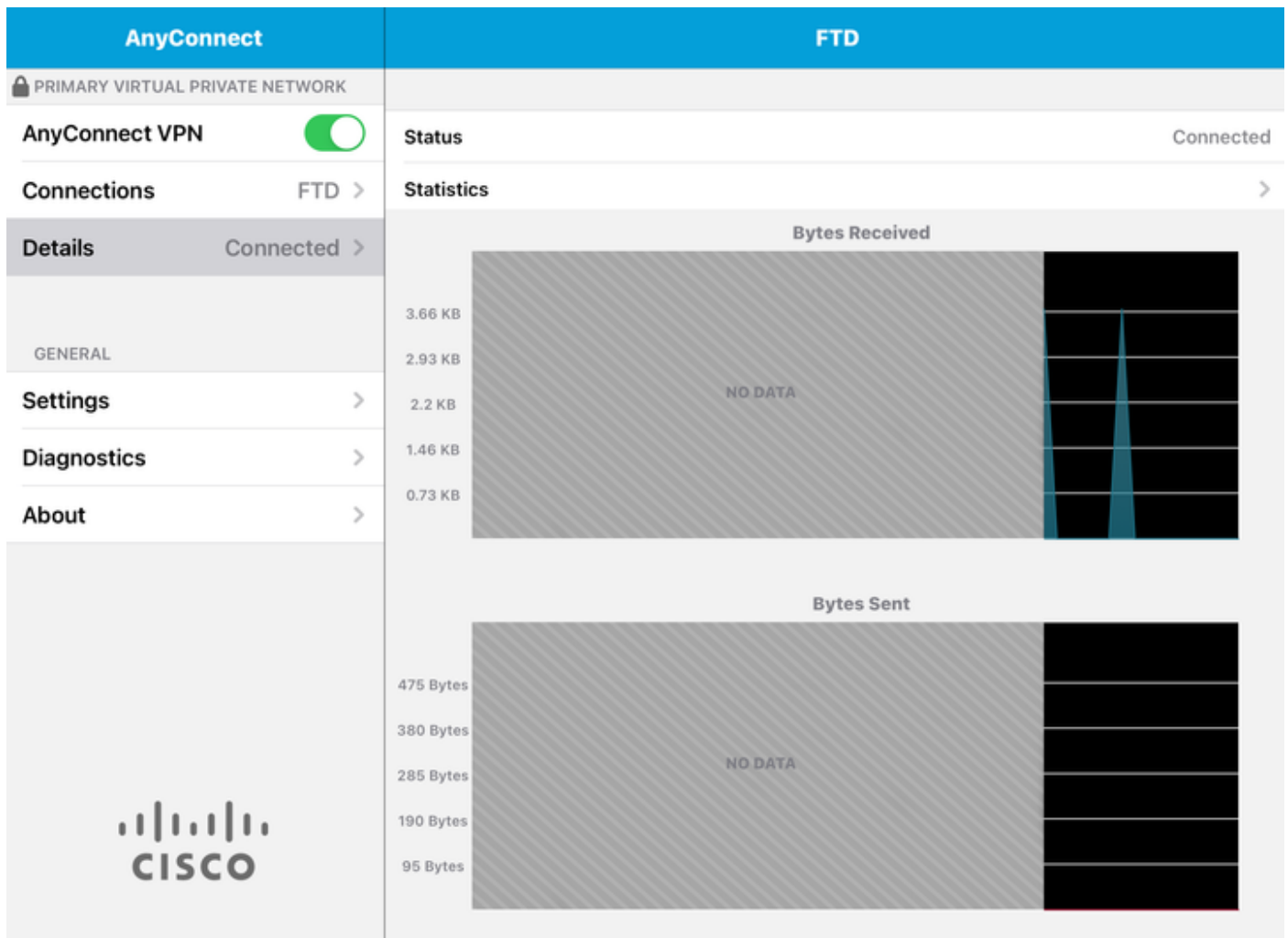
مدقتم رتخأ 7. ةوطخل

اثير اهتفاضلا تمت يتل كتداهش رتخاو ةداهش رتخأ 8. ةوطخل



رابط الخاواص اتال الى رخا ةرم لقتنا 9. ةوطخا

ةالخال في الصم لى صافاتا رهظتو لى غشتا لى ق لى دب تا لى ق بى ، لى دب تا لى حان درجم ب



ةحصلا نم ققحتلا

لصتملا فيضملا لوح تامولعمل عيمج AnyConnect show vpn-sessionDB detail رملأل ضرعي



'filter' و 'sort' ةيساسلأا تاملكل وه رثكأ رملأل اذه حيشرتب موقي نأ راخلا :حيملت رملأل إلا اهتفاضلا تمت يتلا

لالثملا ليبس إلع

Tcoutrie-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 فاشكتسا

ءاطخأل احيصت

وه اءال صإوءة لكشملا هءه ءاطخأ فاشك تسال بولطملا احيصتلا

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

SSL: سيو IPsec وه لاصتالناك اءا

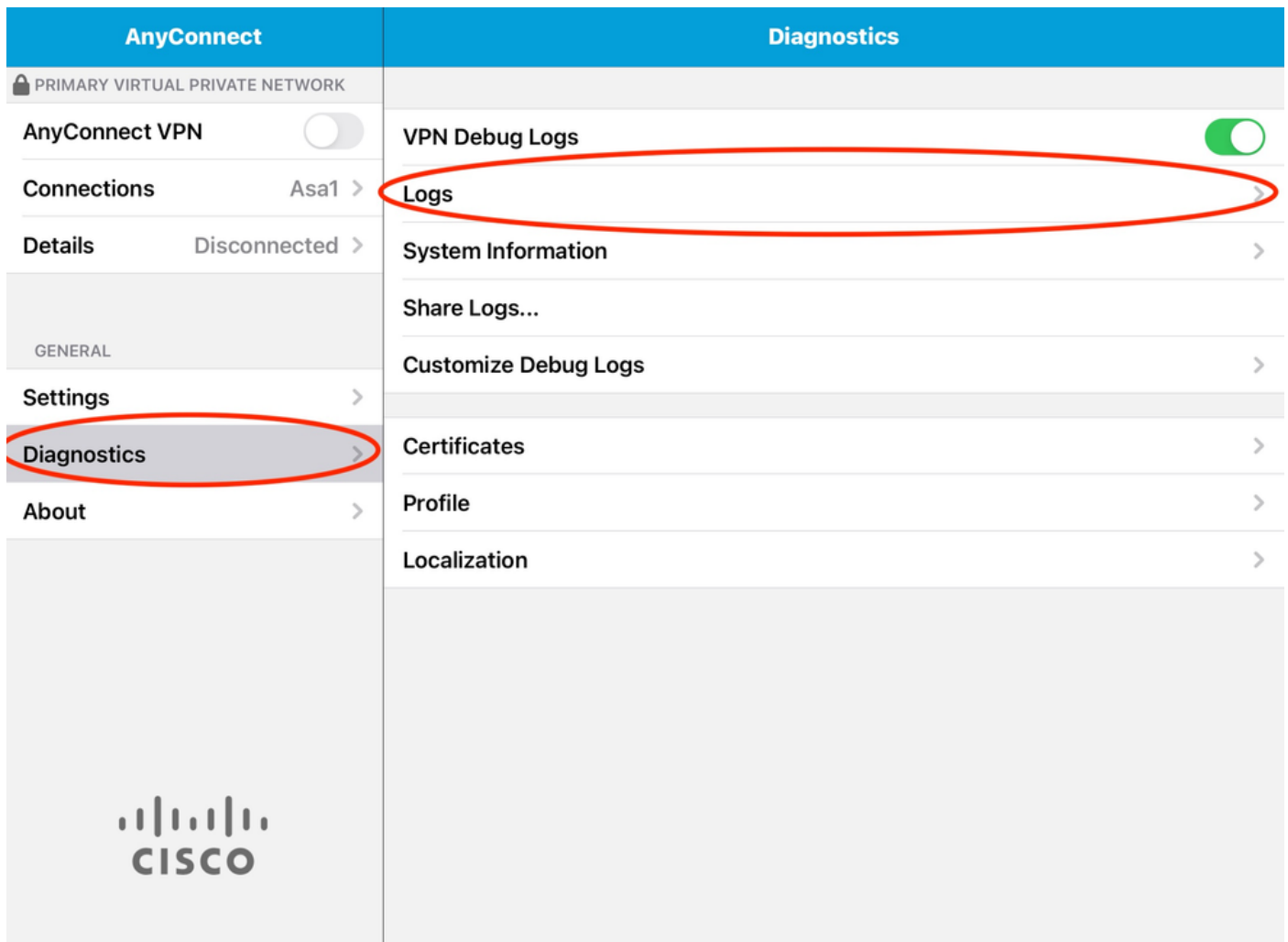
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

ءةومحملل ءهءألل AnyConnect قيبطت نم تالءسلل

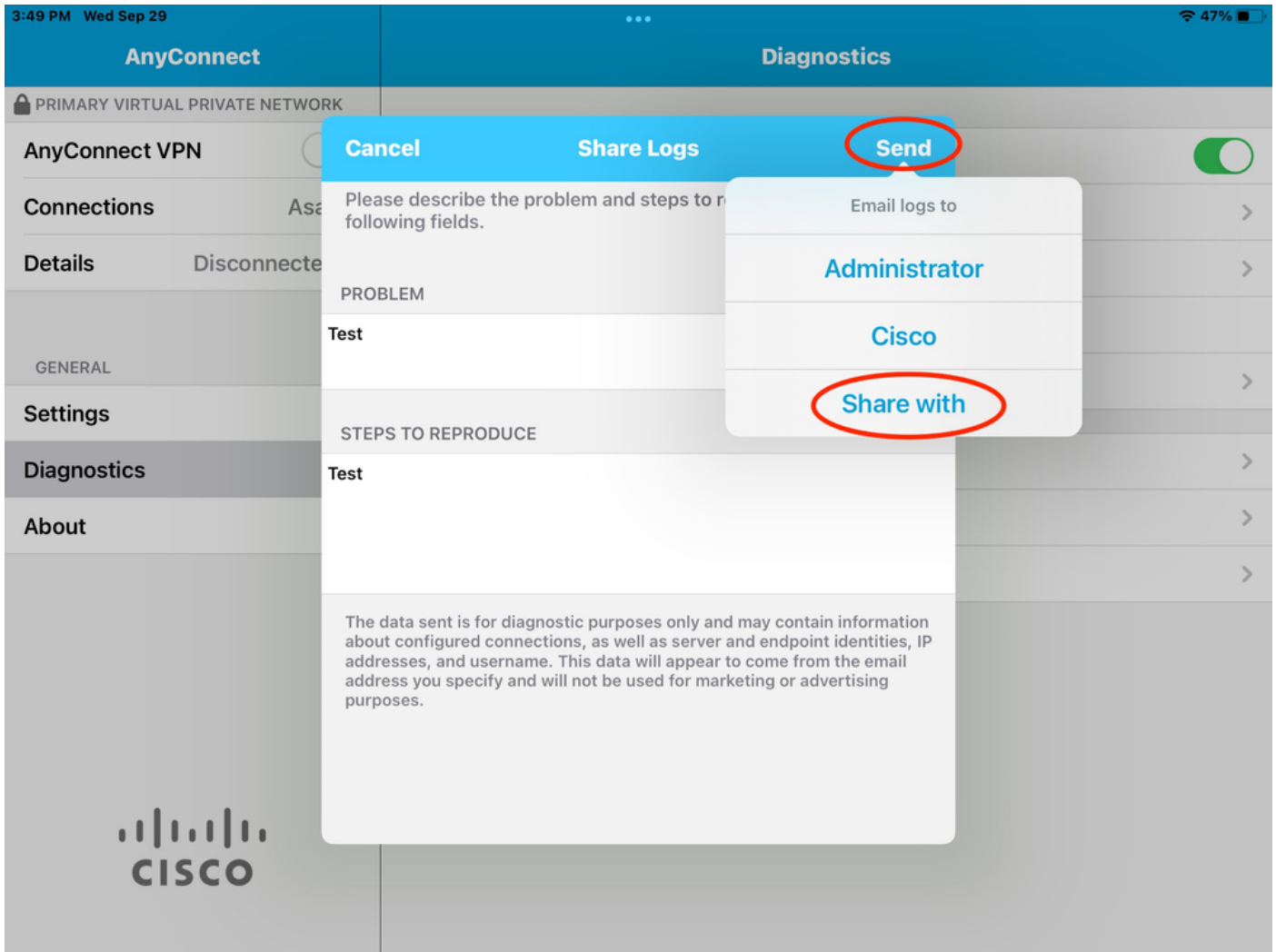
.تالءسلل ءكراشم > VPN ءاطخأ احيصت تالءس > صيخشتلل إلل لقتنا



تامولعملالخدأ:

- ةلكشملا
- رثاكتلل تاوطخ

عم ةكراشم > لاسرا ىلإ لقتنا مث.



تالچسلا لاسرال ينورتكلال ديرب ليمع مادختسا راڤ مدي اذهو.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا