

ىلع ةنمآلا ليمعلا ةداهش ةقداصم نيوكت FMC لبق نم ةرادملا FTD

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[ةكبش لىطىطختلا مسرلا](#)

[تانىوكتلا](#)

[مداخل ةقداصم لم مدختست ةداهش دارىتس/عاشنا](#)

[ةيلخاد/ةوقت قدصم عجرم ةداهش ةفاضاب](#)

[VPN ىمدختسملا نيوانعلا عمجت نيوكت c.](#)

[ةنمآلا لىمعلاروص لىمختد](#)

[هلىمخت XML فىرعت فلم عاشنا - ه](#)

[دعب نع لوصولل VPN نيوكت](#)

[ةحصللا نم ققحتلا](#)

[اهجالص او اعاطخألا فاشكتسا](#)

ةمدقملا

ديدهت نع عافدلا ىلع دعب نع لوصولل VPN ةكبش نيوكت ةىلمع دنتسملا اذه فصى
ةداهشلا ةقداصمب FirePOWER (FMC) ةرادا زكرم لبق نم رادملا FirePOWER (FTD).

عباتلا ةينفلا ةدعاسملا زكرم سدنهم ،لاوراغأ هباشيرو نيچ يلود لبق نم ةمهاسملا تم
ةكركشل Cisco.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت ناب Cisco يصوت:

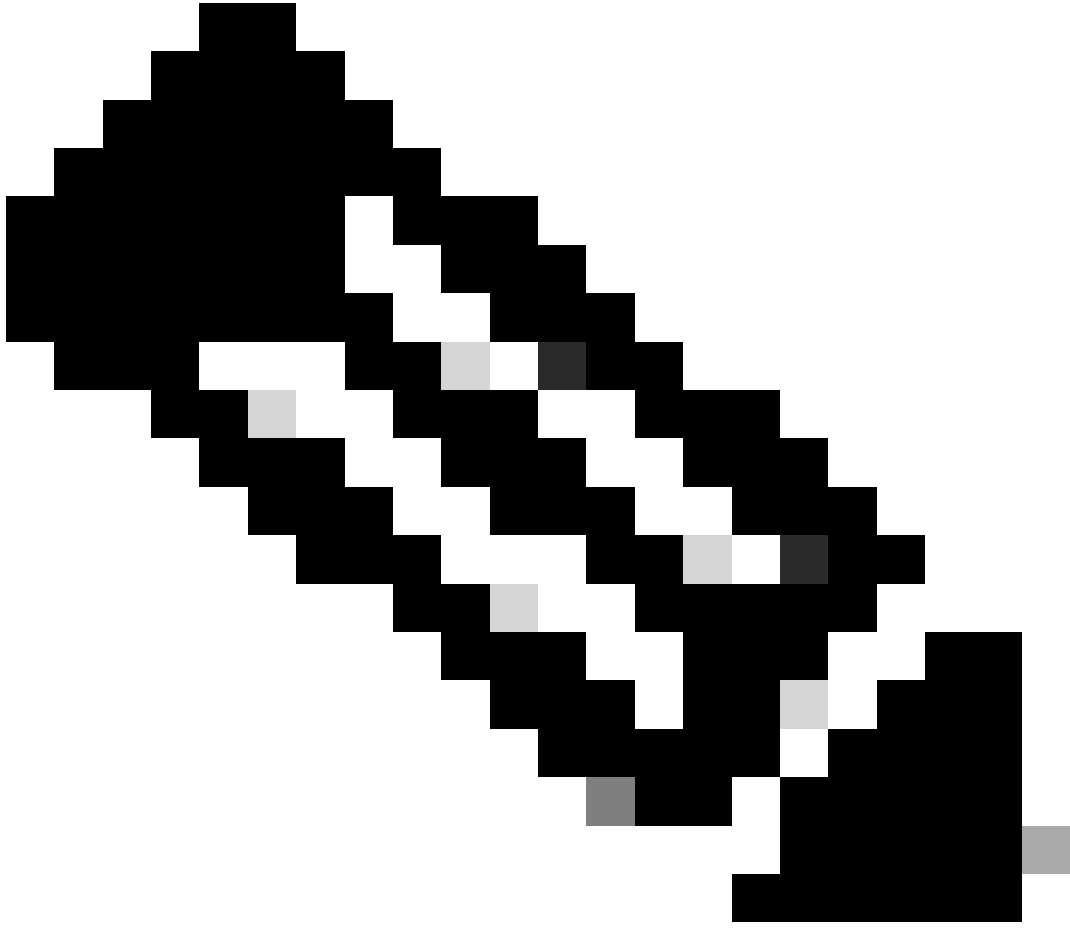
· SSL تايساسأو ةداهش لى يوديلا لىجستلا

· FMC

· دعب نع لوصولاب ةصاخلا VPN ةكبش لى ةيساسألا ةقداصملا ةفرعم

· Thawte و GoDaddy و Geotrust و Entrust لثم (CA) ةيجراخ ةهجل عباتلا قدصملا عجرملا
VeriSign

ةمدختسملا تانوكملا



ءاشنإ مء اذإ CSR ءاشنإ نم نكمءء نأ لبق CA ءءاهش ءوؤ مزلئ، FMC ئ ف: ءظءالم
بؤئو لشفئ ئو ءل بولسألأ نإف، (ءئءراؤ ءهؤ أو OpenSSL) ئءراؤ رءصم نم CSR
PKCS12 ءءاهش قئسنء مءءءسإ

"نارئقالا لئءسء" نمض (+) عمءلأ ءمالع قوف رقناو "زاهءلأ" ءء Add. رقناو Devices > Certificates ئل لققءنا 1. ءوطءلأ

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cancel

Add

ةداهشلا ليجست ةفاضلا

ةمدختسملا (CA) قدصملا عجرملا ةداهش قصلال او Manual ةئيه ىلع ليجستلا عون ددح ،كلذ CA Information تحت 2. ةوطخلال
عقوتل CSR.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
HQYDVQQDEZXiewRyYwS0S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=ZeeQw
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



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

Cancel

Save

قد يصل حجم الملف إلى 100 كيلوبايت.

3. في الخطوة 3، حدد IPsec Client، SSL Client و Skip Check for CA flag in basic constraints of the CA Certificate.

4. في الخطوة 4، انقر فوق Certificate Parameters، ثم انقر فوق Save.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

Email (E):

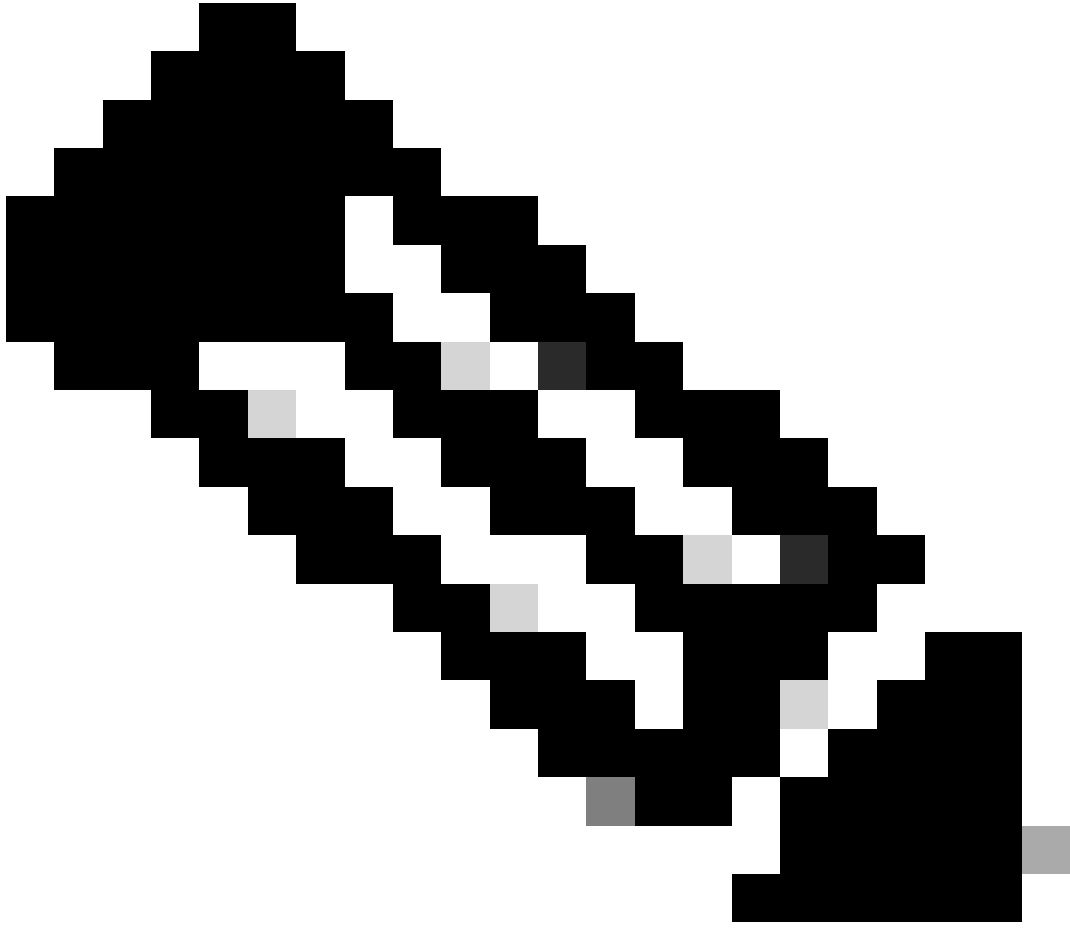
Include Device's Serial Number

Cancel

Save

داهش تاملعم ةفاضإ

Save قوف رقنا .همجوححاتفم مساب RSA كحاتفملا عون ديدحتKey تحت 5 ةوطخال



ت.ب 2048 حاتفملا مچحل یندألا دحلا نوكي، RSA حاتفم عونل ةبسنلاب :تظحالم

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Key Type:

RSA ECDSA EdDSA

Key Name:*

rsa_key

Key Size:

2048

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel

Save

RSA حالات مفصلة

Add. رقبناو طقف اهؤاشن| مت يتلا ةلدسنملا ةمئاقلا نم ةقثلا ةطقن ددح. Cert Enrollment تحت 6. ةوطخلال

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

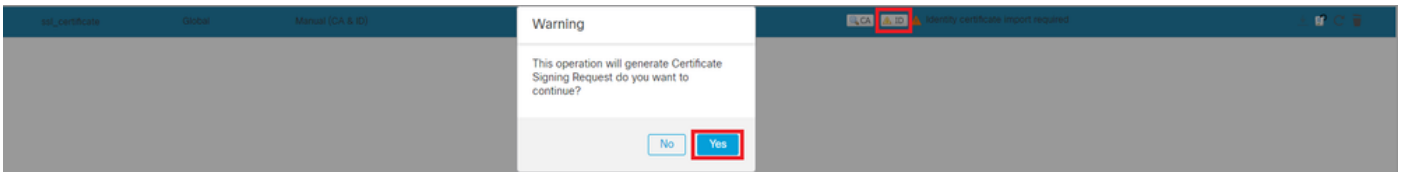
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

ةديج ةداهش ةفاض|

CSR ءاشنإل ةيفاضإ ةبلاطم Yes قوف رقنا م ث ، فرعم قوف رقنا 7. ةوطخلال



ءاشنإ CSR|

م ق ، CA لبق نم ةيوهلا ةداهش رادصإ م تي نأ درجم ب . قدصملا عجرملا لبق نم هعيقوت ىلع لصح او CSR خسن ا 8. ةوطخلال Import قوف رقنلا او Browse Identity Certificate قوف رقنلا اب اءاداري تساب .

Import Identity Certificate



Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC
SU4wgglIIMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP
ppzi0ulIbVmb5iKQexllaur/e2PDccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

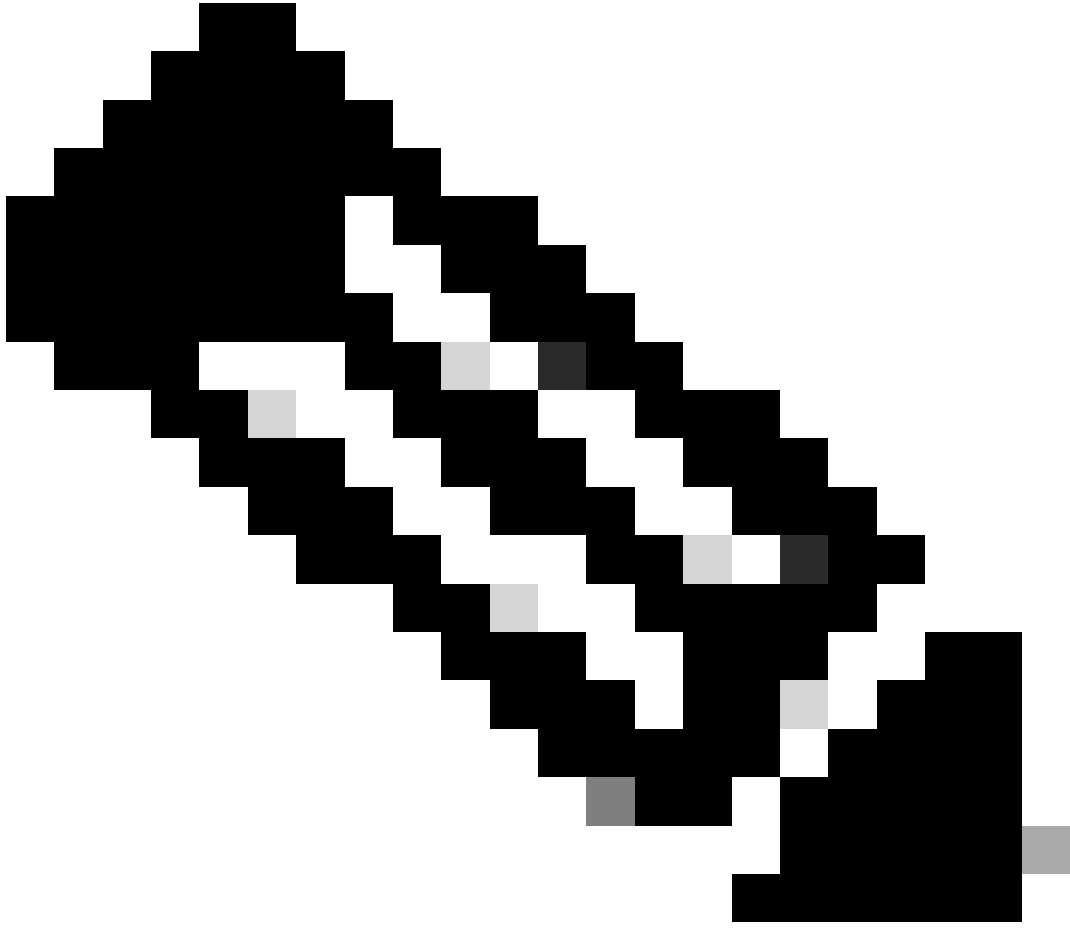
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

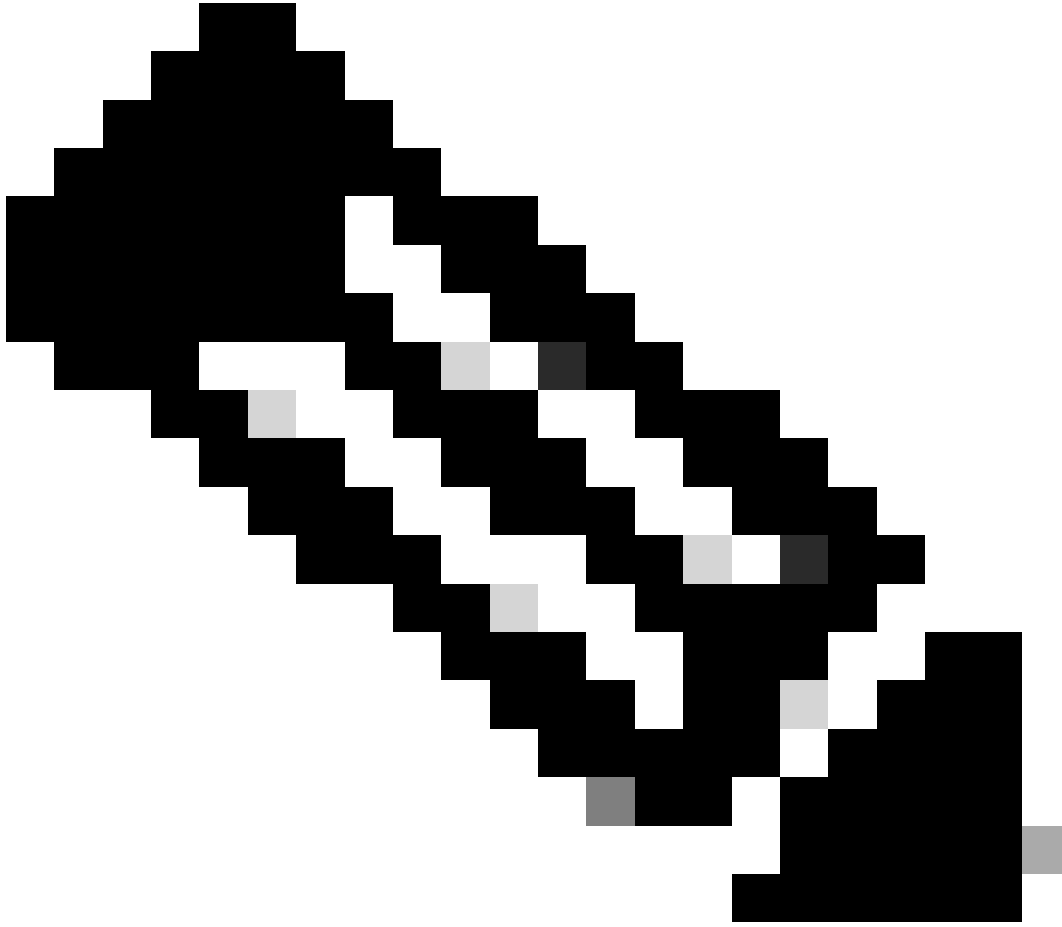
[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)



هسفن CSR عاشن | ل اذه يدؤيس . اقحال 7 ةوطخال راركت كنكمي ، اتقو فرعلم اءءاش راءص | قرغتسا اذا : ةظحالم فرعلم اءءاش ءاريتسا | اننكمي و .



اضي ا ردصي "،مداخلا ققداصمل مدختست ةداهش داريتس/ءاشن" (أ) ةوطخلا يف مدختسمل قدصملا عجرملا ناك اذا :تظالم ةداهش سفن ةفاضلا ةجاج دجوت ال . "ةلخاد/ققث قدصم عجرم ةداهش قفاض" (ب) ةوطخلا يطخت كنكمي ،مدختسمل تاداهش متيسف ،رخأ ةرم اهسفن قدصملا عجرملا ةداهش ةفاضلا تمت اذا .اضي اهب نجت بجوي رخأ ةرم قدصملا عجرملا RAPN ل ةداهشلا قداصم يلع رثوي نا نكمي يذلا "Validation-use none" ب TrustPoint نيوكت

Add. قوف رقناو Devices > Certificates ىلا لقتنا 1. ةوطخلا

"نارتقالا ليجست" نمض (+) عمجالا ةمالع قوف رقناو "زاهجا" دح

مدختسمل/ةيوهلا تاداهش رادصال "auth-risaggar-ca" مدختست ،انه

General

Details

Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: auth-risaggar-ca

Issued by: auth-risaggar-ca

Valid from 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

اك-راغاسيرثو ايدان

CA information لفسأ ليحست عونك Manual ددحو TrustPoint م سا لخدأ 2. ةوطخلال

PEM قيسنتب اهب قوومل/يلخادلل قوصملا عجرملا ةداهش قصلو CA Only عجار 3. ةوطخلال

Save. رقن او Save. Skip Check for CA flag in basic constraints of the CA Certificate ققحت 4. ةوطخلال

Add Cert Enrollment



Internal_CA

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGV  
u  
VHJ1c3QgQ29tbWV5Y2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

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

Cancel Save

TrustPoint ةفاض

Add. قوف رقن او وتلل اهؤاشن مت يتل ةلدسنم ال ةمئاق ال نم TrustPoint دح Cert Enrollment تحت 5. ةوطخلال

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name: Internal_CA
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Cancel

Add

يخذاد قدصم عجرم ةفاض

يلتال وحنال لىع اقبسما ةفاضت مت يتال ةداهشال ضرع متي 6 ةوطخال

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	-------

ةفاضم ال ةداهشال

c. VPN يمدختسمل نيوانعال عمجت نيولكت

Objects > Object Management > Address Pools > IPv4 Pools . 1. ةوطخال

عانقب IPv4 ناوعومسال قاطن لخدأ 2. ةوطخال

Edit IPv4 Pool



Name*

vpn_pool

Description

IPv4 Address Range*

10.20.20.1-10.20.20.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

► Override (0)

Cancel

Save

IPv4 ع م ح ت ة ف ا ض ا

ة ن م آ ل ا ل م ع ل ا ر و ص ل م ح ت . د

Cisco [ج م ا ر ب](#) ع ق و م ن م ل م غ ش ت ل ا م ا ط ن ل ا ق ف و ة ن م آ ل ا ع ا ل م ع ل ا ر و ص ل WebDeploy ل م ز ن ت ب م ق . 1 ة و ط خ ل ا

2 ة و ط خ ل ا . Objects > Object Management > VPN > Secure Client File > Add Secure Client File ل ل ل ق ن ت ن ا .

3 ة و ط خ ل ا . ص ر ق ل ل ا ن م ن م آ ل ا ل م ع ل ا ف ل م د د ح و م س ا ل ا ل خ د ا .

4 ة و ط خ ل ا . Save ق و ف ر ق ن ا و Secure Client Image م س ا ب ف ل م ل ا ع و ن د د ح .

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

ةنم آل لم ع ةروص ةفاض ا

هل لمحتو XML في رعت فلم ءاشن ا - ه

Cisco Software [جمارب](#) ع قوم نم Profile Editor هت ببتو نم آل لم ع ل لزن بت مق 1. ةوطخل ا

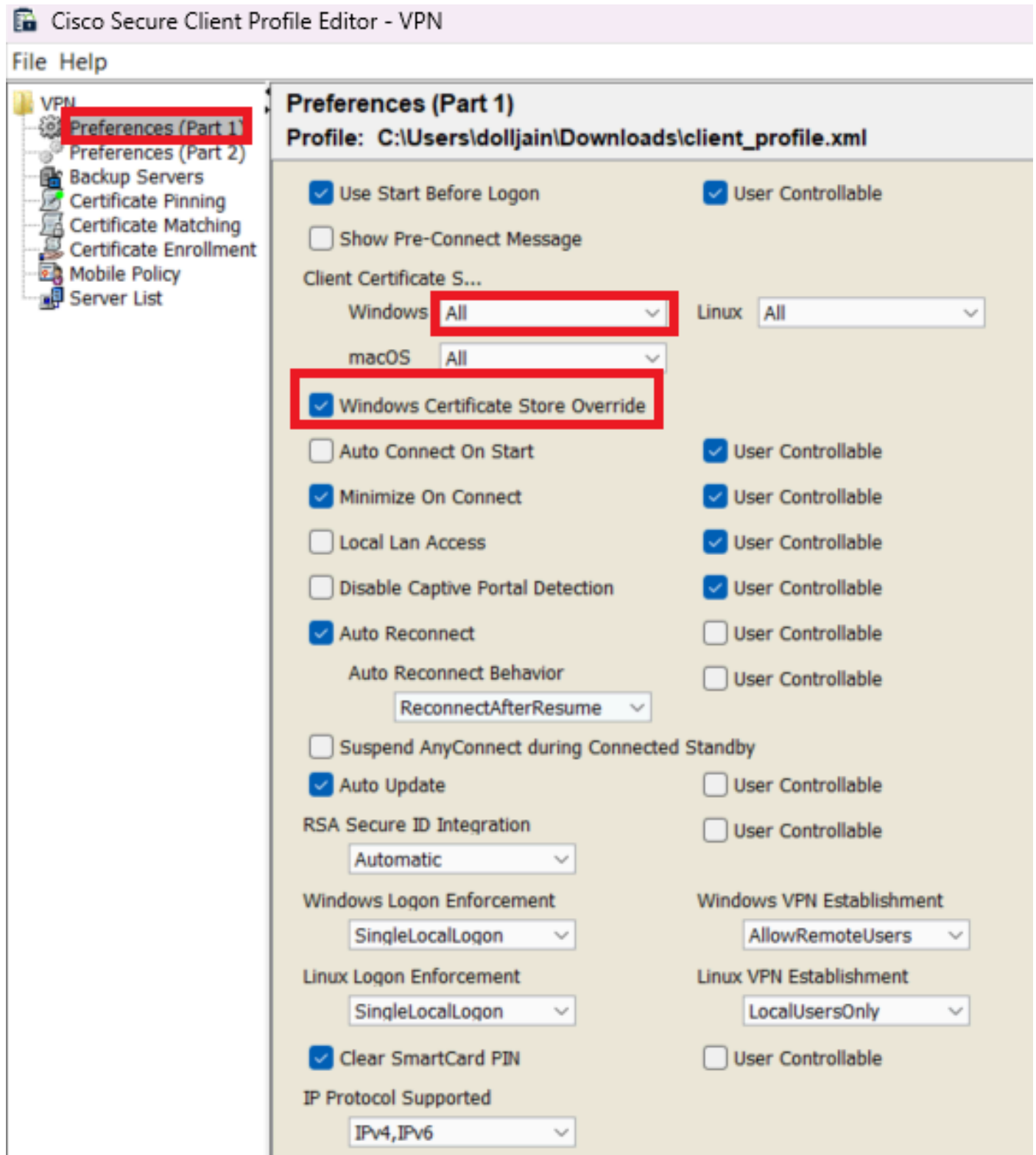
ف ف ساس ل كش ب مكحتي وهو. لم ع ل ا ةداهش دي دحتل ةلدس نم ل ةمئ اقل نم All دي دحتو دي دج ف في صوت ءاشن ا. 2. ةوطخل ا
اهت ءارقو تاداهش ل ل نيزختل اهم ا دختس ا "نم آل لم ع ل" ل نكمي يتل تاداهش ل ل (نزاخم) نزم

امه ناحاتم نارخا نارايخ

- Windows ل ل حمل ل زاهج ل تاداهش نزم ف ةداهش ل ل ع شحل ل "نم آل لم ع ل" دي دقت مت - زاهج ل
- حمل ل Windows م دختس م تاداهش نزم ف ةداهش ل ل ع شحل ل ل نم آل لم ع ل دي دقت مت - م دختس ل

True . تاداهش ل ل نزم زواجت ني عت

ماظنل) Windows زاھج صاخال تاداهشل نزم يف ءءوءومل تاداهشل مااءآساال "نمآل ليمعلا" هءوءب لوؤسملل ءمس ي اءو
 يضاااا لءشب ،لاصاال اءب مءي ءي ء ،ءق ف SSL لء "تااءهشل نزم زواآ" قبطن ي .ل يمعلا ءءهش ءقءاصمل (ي لءملا
 .نمآل ليمعلا ف يءرءء فلم يف ءءوءومل ءيميلا هءه قبطنء ال ،IPSec/IKEv2 مااءآساا ءع .مءءساا ءءهء ءقءاصم ءسءاوب



1) ءءهءل) ءال يضااا ءءهءل

ءءهءل ءي ءءءب مءءسااا زاع يءل ال بءءي هءل رمل ءي ءءءب ءاغل ب Disable Automatic Certificate Selection مءق (ي رايءءل) .3 ءوءءل
 ءقءاصملا

- VPN
- Preferences (Part 1)
- Preferences (Part 2)**
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

Disable Automatic Certificate Selection

User Controllable

Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

4

Performance Improvement Threshold (%)

20

Automatic VPN Policy

Trusted Network Policy

Disconnect

Untrusted Network Policy

Connect

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Closed

Allow Captive Portal Remediation

Remediation Timeout (min.)

5

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

Disable

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Same User Only

Authentication Timeout (seconds)

30

إلى أن تم اتاراسم ة فاضال "نمأل ليمعل" لبق نم هذه (ACL) لوصولا يف مكحتل ةمئاق مادختسا متي: ةظحالم ة لخدال دراومل.

Add. قوف رقنا و Remote Access > VPN > Devices | لقتنا 2. ةوطخل

ي. لالتا لىل ع رقنا م م FTD زا ه دد م في صوالتا م سا لخدأ 3. ةوطخل

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 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	Selected Devices
<input type="text" value="Search"/> FTD-A-7.4.1 FTD-B-7.4.0 FTD-ZTNA-7.4.1	FTD-A-7.4.1

Before You Start

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

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client 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.

في رعتل فل م سا ة فاضا

ة قداصملا نمضوه امك ة قداصملا بولسأ Client Certificate Only ودد و Connection Profile Name ة قداصملا بولسأ لخدأ 4. ةوطخل
ة بسا حمل او ضيوفتلا و (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:*

i 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: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)


ةقد اصم لبولسأ دي دحت


اقبس م هؤاشنإ م ت يذلا IPv4 نيوان ع م ح ت د دحو "ل م عمل ناو ن ع ني ي ع ت" ن م ض Use IP Address Pools قوف ر ق ن ا 5. ة و ط خ ل ا

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 (Realm or RADIUS only) **i**
- Use DHCP Servers
- Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

ل م عمل ناو ن ع ني ي ع ت دي دحت

ة و م ح م ل ا ج ه ن ر ح ت 6. ة و ط خ ل ا

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](#)

ةوعومجملا جهن ريرحت

ةمئاق عون تحت Standard Access List ددحو Tunnel networks specified below ددح مئ ، General > Split Tunneling ىل لقتنا 7. ةوطخلال مسقملال قفنلال تاكبش.

اقبس م اهؤاشنلا مت يتلا (ACL) لوصولال يف مكحتلال ةمئاق ددح.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List Extended Access List

Standard Access List:

Split_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

يقف النماذج لاصحات الامتيازات

Save. رن او Client Profile دح ، Secure Client > Profile ل لقتنا. 8 ة و ط خ ل ا

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:

Anyconnect_Profile-5-0-05040 +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

نم آ ليم ع فيرعت فلم ة فاضا

Next. رقن او Secure Client Image ددح مث، Next. قوف رقن ا. 9 ة ووطخلا

Secure Client Image

The VPN gateway can automatically download the latest Secure Client 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 Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows

نم آ ليم ع ة روص ة فاضا

Next. ة قوطو vpn-حم سي sysopt تصحفو Device Certificates ل، ذفنم VPN ل نراق ة كبشلا ترتخأ. 10 ة ووطخلا

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:* +
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

VPN رورم ة كرحل لوصولا يف مكحتلا ةفاض

Finish. روناو تانويككتلا عي مج عجار، اريخأ. 11 ةوطخل

Remote Access VPN Policy Configuration

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

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

دع ب ن ع لوصول ل VPN ة سايس نيوك ت

م ت ي ذل لاصت ال في ر ع ت فلم ر ي ر ح ت ب م ق ، د ع ب ن ع لوصول اب ة ص ا خ ال VPN ة ك ب ش ل ي ل و ال ا د ا د ع ال ا ل ا م ت ك ا د ر ج م ب 12 ة و ط خ ال Aliases. ال ل ق ت ن ا و ه و ا ش ن ا

(+) ع م ج ال ة م ال ع ز م ر ق و ف ر ق ن ل اب group-alias نيوك ت ل اب م ق 13 ة و ط خ ال

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth


Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of URL following URLs, system

URL

Edit Alias Name

Alias Name:

ssl-cert

Enabled

Cancel OK

Cancel Save

ةومجملل راعتسملال مسالا ريرت

هنيوكت مت يذلاةومجملل URL ناونع سفن مدختسأ (+) عمجال عمالع زمر قوف رنناب group-url نيوكتلاب مق 14 ةوطخلال لمعملال فيرعت فلم يف اقبسم

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

Client Address Assignment AAA **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off.

Edit URL Alias

URL Alias:

certauth

Enabled

Cancel OK

URL Alias:

Configure the list of URL aliases. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

Cancel Save

ةومجم ل URL ناونع ريحت

SSL تادادع نمض SSL Global Identity Certificate و Interface Trustpoint دح . لوصول تاهج اول ل لقتنا 15 ةوطخل

RAVPN

Enter Description

Connection Profile **Access Interfaces** Advanced

Local Realm: cisco-local Policy Assignments (1) Dynamic Access Policy: None

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: ssl_certificate

Note: Ensure the port used in VPN configuration is not used in other services

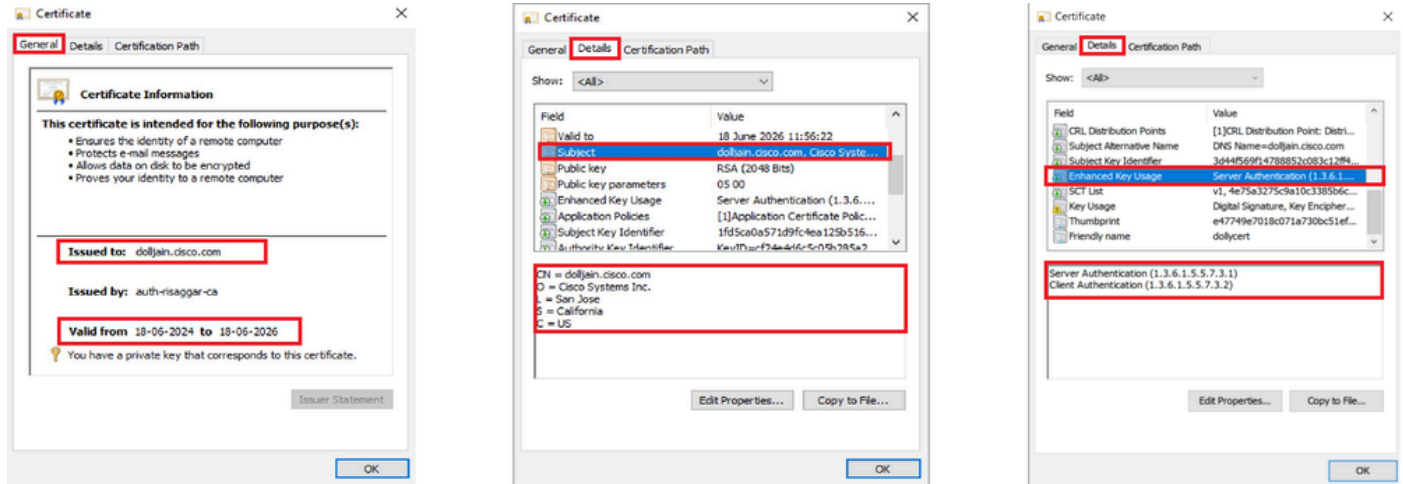
لوصول تاهج او ريحت

تارييغتلل هذه رشنو Save قوف رقنا 16. ةوطخلا

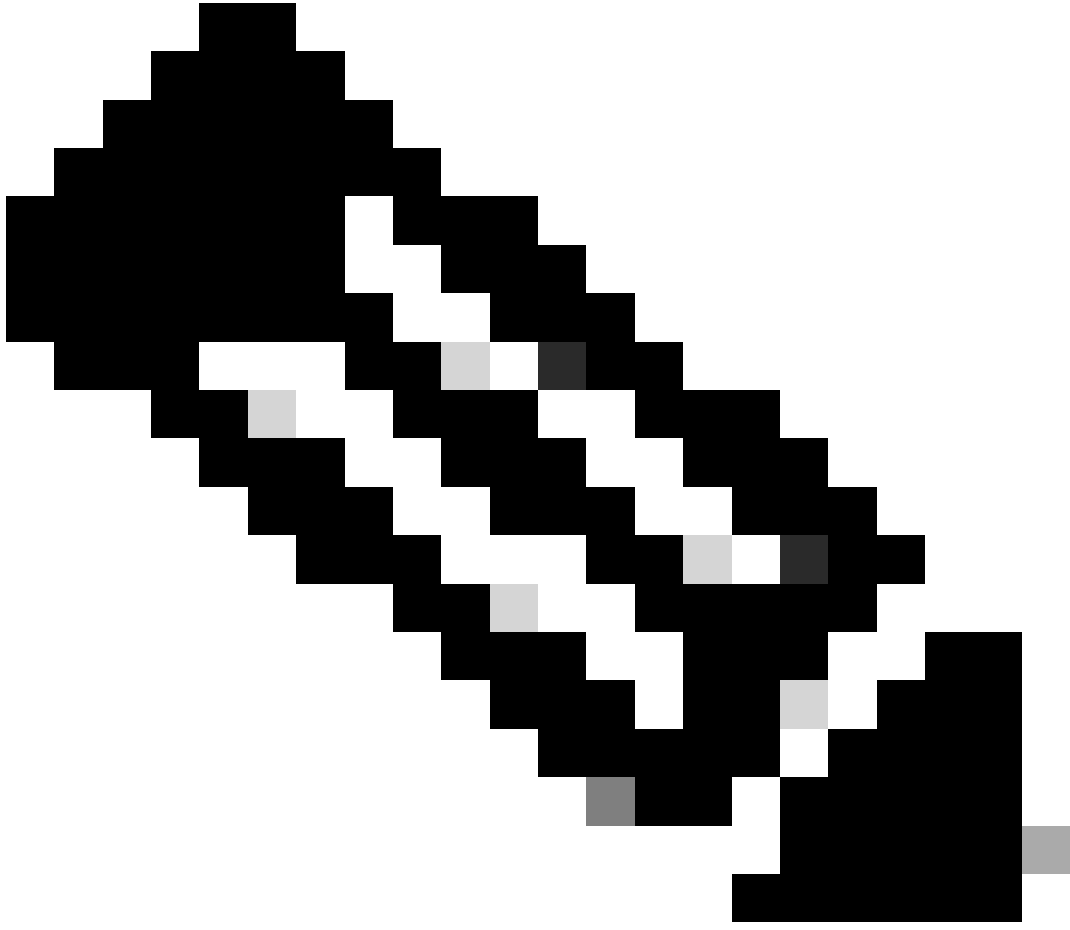
ةحصلال نم ققحتلال

جحص لكشب نيوكتلل لمع ديكأتلل مسقلا اذه مدختسا

رتويبمكلل زاهاج ىلع EKU وخالص عوضوم وخريراتب ةتبثملل ةداهشلل ىلع نمآلال لمعل رتويبمكلل زاهاج يوتحي نأ بجي 1. حوضوم وه امك FTD ىلع ةداهش تبثت مت يذلا قدصملا عجرملا نع ةرداص ةداهشلل هذه نوكت نأ بجي. مدختسملاب صالحا "auth-risaggar-ca". ةطساوب مدختسملا ةداهش وأ ةيوهال رادصا متي، انه. اقبس



ةداهشلا تازيم



"لېمعالا ؤقداصم" (EKU) نسحملا حاتفملا مادختسا ىلع لېمعالا ؤداهش يوتحت نأ بجي: ؤظحالم

لأصتالا ؤاشنإ "نمألا لېمعالا" ىلع بجي 2.

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل