

لوکوتورب مادختساب ةداهشلا ليجست نيوکت ةيامحل رادج ديدت نع نمآلا عافدلا ىلع ACME FMC ةطساوب هترادإ متت يذلا

ةمدقملا

ةئيب لوکوتورب لالځ نم (TLS) لقنلا ةقبط نامأ ةداهش ليجست ةيلمع دنتسمل اذہ فصی
Secure Firewall Firepower Threat Defense (FTD) ساسألماظنلا ىلع (ACME) ةتمتؤملا تاداهشلا ةرادإ
Defense (FTD).

ةيساسألما تابلطتملا

تابلطتملا

عوضوم اذہ ىلع ةفرعم تنأ ىقلتي نأ يصوي cisco

- (SSL) ةنمآلا ليصوتلا ذخآم ةقبط تاي ساسألما ةيوديلا ةداهشلا ليجست تاي لمع
- دعب نع لوصولل (VPN) ةيره اظلا ةصاخلا تاكبشلل ةيساسألما ةقداصملا ميه افم
- (CAs) قي دصتلا تائيه عم ةربځلا

ةمدختسمل تانوكملا

- Cisco FTDv. نم 10.0.0-35 رادصلإ
- Cisco FMC، رادصلإ 10.0.0-35.
- ACME لوکوتورب معدي يذلا (CA) ةداهشلا حنم ةهځ مداځ

ةصاخ ةيلمعم ةئيب ي ف ةدوجوملا ةزهجال نم دنتسمل اذہ ي ف ةدراول تامولعملما عاشنإ مت
تناك اذإ. (يضا رتفا) حوسمم نيوکتب دنتسمل اذہ ي ف ةمدختسؤلما ةزهجال عي مج تادب
رماً يأل لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتل دي قكتكبش

دودحل او تابلطتملا

ةيامحل رادجل FTD في ACME ليجستل ةيلالحل دويقل او ةيساسال تابللطتمل نمضتت
يللي ام نملال

- ثدحلال تارادصلال او 10.0.0 رادصلال FMC و FTD تارادصلال يلل موعدم
- ددحم لاجم مسا ةداهش بللط لك ددحي نأ بجي؛ لدبلال فرح تاداهش رادصلال ACME حمست ال
- ةكراشم نكمي ال كلذل، ةدحاو ةهجاوب ACME لالح نم ةلجسم ةقث ةطقن لك دييقت متي
- ةددعتم تاهجاو ربع ACME ربع اهليل لوصحلال متي يتللا تاداهشلال
- امم، ACME لالح نم ةلجسم ةداهش لكل ةديرف يهو ايئاقلت حيتافملا جاوزأ عاشن متي
نيمأتلل نسحيو حاتفملا مادختسا ةداعل عنمي

ضفخلال تارابتعا

وأ (7.7 رادصلال) ACME ليجستل معددي ال يذل نملال ةيامحل رادجل FTD رادصلال يلل ضفخلال دنع
(مدقأل)

- وأ 10.0.0 رادصلال في ةمدقملا ACME ب ةلصلال تاذا TrustPoint تانويكت عيجم دقف متي
ثدحلال
- اهحيتافم نإف، كلذ عمو؛ انكمم ACME ربع ةلجسملا تاداهشلال يلل لوصوللا لازي ال
ضفخلال دعبل ليغشت ةداعل او ظفح لوأ دعبل ةطبترم ريغ حبصت ةصاخلا

هب ىصوملا ليدبلا لالحل مدختسأ، ايرورض ضفخلال ناك اذا

- PKCS12 قيسننتب ACME تاداهش ريصدت ب مق، ضفخلال لبق
- ACME TrustPoint نيويكت ةلازاب مق، ضفخلال لبق
- ىتح ةحلصل ةدروتسمل TrustPoint لظت. PKCS12 ةداهش داريتساب مق، ضفخلال دعبل
ACME نع ةرداصلال ةداهشلال ةيحلصل يهتنت

ةيساسأ تامولعم

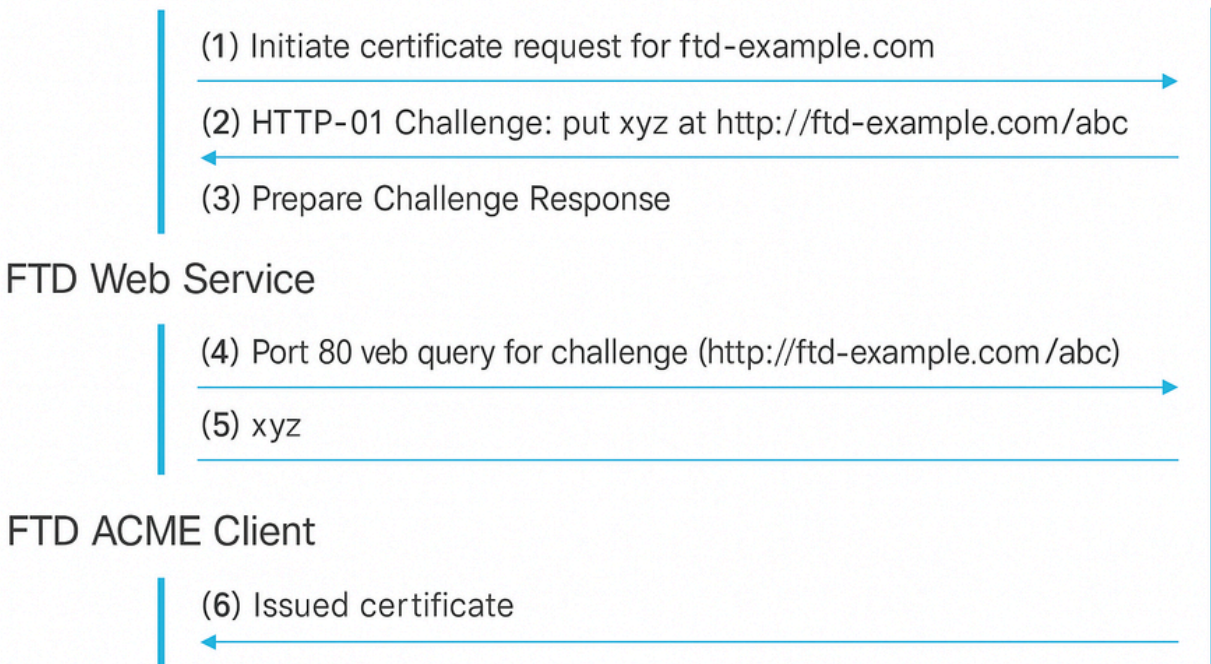
جمانرب لالح نم. ةكبشلال يلوؤسمل TLS تاداهش ةرادا طيسبت يلل ACME لوكتورب فدهي
اذه TLS تاداهش ديدجتو باسكتكاب ةقلعتملا ماهملا ةتمتأ نيولوؤسملل نكمي، ACME
Let's Encrypt لثم (CA) ةقدصملا عجارملا عم لمعلا دنع صاخ لكشب ديفم يئاقلتل ليغشتلا
لوكتورب ربع ماع لكشب اهليل لوصوللا نكميو ةتمتؤم ةيناجم تاداهش رفوت يتللا Encrypt،
نأ نم تاداهشلال هذه ققحتت. (DV) لالحملا ةحص نم ققحتل تاداهش رادصلال ACME لهسي. ACME
لالح نم ةداع ةحصلا نم ققحتللا ةيلمع متت. ةددحملا تالاحملا يلل مكحت هل ةداهشلال بلاط
مداخ يلل نيعم فلم عوضوب بلطلال مدقم موقبي شيح، HTTP يلل دننتست ضارتعا ةيلمع
HTTP مداخ ربع فلملا اذه يلل لوصولاب (CA) "قدصملا عجرملا" موقت مث. هب صاخلا بيوللا
ةداهش رادصلال نم قدصملا عجرملا يدحتللا اذه زايحتا نكمي. لالحملا ب مكحتللا ديكتل لالحملا
حاجن ب DV

ة:للاتال تاوطخال ليجستلة لملع نمضت

1. لاجملا ددحي و، ACME مداخل لةداهش بلط لاسراب ليمعلا موقوي :ةداهشلا بلط ادب ه.لجأ نم ةداهشلا لعل لوصحلا بولطملا (تالاجملا)
2. بجي زيمم زمر لعل يوتحي HTTP-01 يديحتب ACME مداخل بيحتسي :HTTP-01 يديحت يقلت لاجملا ةيكلم تابثال همادختسا ليمعلا لعل
3. يديحتلة باجتسا ريضحت
1. مداخل نم زيمملا زمرلا عيحت قيرط نع حاتفم ضيوفت عاشناب ليمعلا موقوي هب صاخلا باسحلا حاتفم عم ACME
2. راسم يفاذه حاتفملا ضيوفت ةمدخل هب صاخلا بيو مداخل نيوكتب ليمعلا موقوي URL لددحم
4. ااونع لعل HTTP GET بلط ذي فننتب ACME مداخل موقوي :يديحتلة ديحتسي ACME مداخل حاتفملا ضيوفت لعل لوصحلا رفوتملا URL
5. مت يذلا حاتفملا ليوخت ةنراقمب مداخل موقوي :ةيكلملا نم ققحتلاب ACME مداخل موقوي لاجملا ليمعلا مكحت نم ققحتلل ةقوتملا ةميقلاب هدارتسا
6. SSL/TLS ةداهش ACME مداخل ردصي ،حاجنب ةحصللا نم ققحتلا دنع :رادصلا ةداهش ليمعلا

FTD ACME Client

ACME Server



ACME ليجستلة HTTP-01 ةقداصم قفدت

FTD لعل TLS تاداهش ليجستلة ACME لوكوتورب مادختسال ةيسيئرلا تازيملا نمضت

يولي ام ن مآلة ايمحلا راجل:

- ايم نبلل لوصول ايف مكحتلا ازم لمعت :تاداهشلا ارااال ائاقلا لئليغشتلا اهب ظافتحالاو TLS لاجم تاداهش لعل لوصول ايمع مئظنت لعل (ACME) ايمساسالا ماملا لئلقت لعل لمعي امم ،ن مآلة ايمحلا راجل FTD جم انربب اصاصلا TLS تاهجالول ريبك لكشب ايمويلا ايمرااالا
- مئتي ،ACME رايعم معدت ايمتلا اقثلا طاقن اوجومو :ااداهشلا لئاقلا لئليغشتلا ايمحلا لخدتللا لعل ايمحلا نم للقي امم ،اهتياحلا صاهتنا بارثقا عم ائاقلا تاداهشلا ايمحلا ريمتسملا ايمرااالا
- نود احولاص تاداهشلا احاقب ائاقلا لئليغشتلا اذم نمضي :ريمتسملا نامالا نامض تالاصتالا لعل ظفاحي و اعمقوتملا ريغ ااداهشلا ايمحلا صاهتنا عنمي امم ،عاطقنا ايم مآلا

جم انرب رشن تاي لمعمل نامالا و ايمليغشتلا اعاقللا نئسحت لعل اعممجم ايازملل اذم لمعت ايم مآلة ايمحلا راجل ربع (FTD) اعرسللا قئاف لاسرالا

نئوكتلا

ايمساسالا تابلطتملا نئوكت

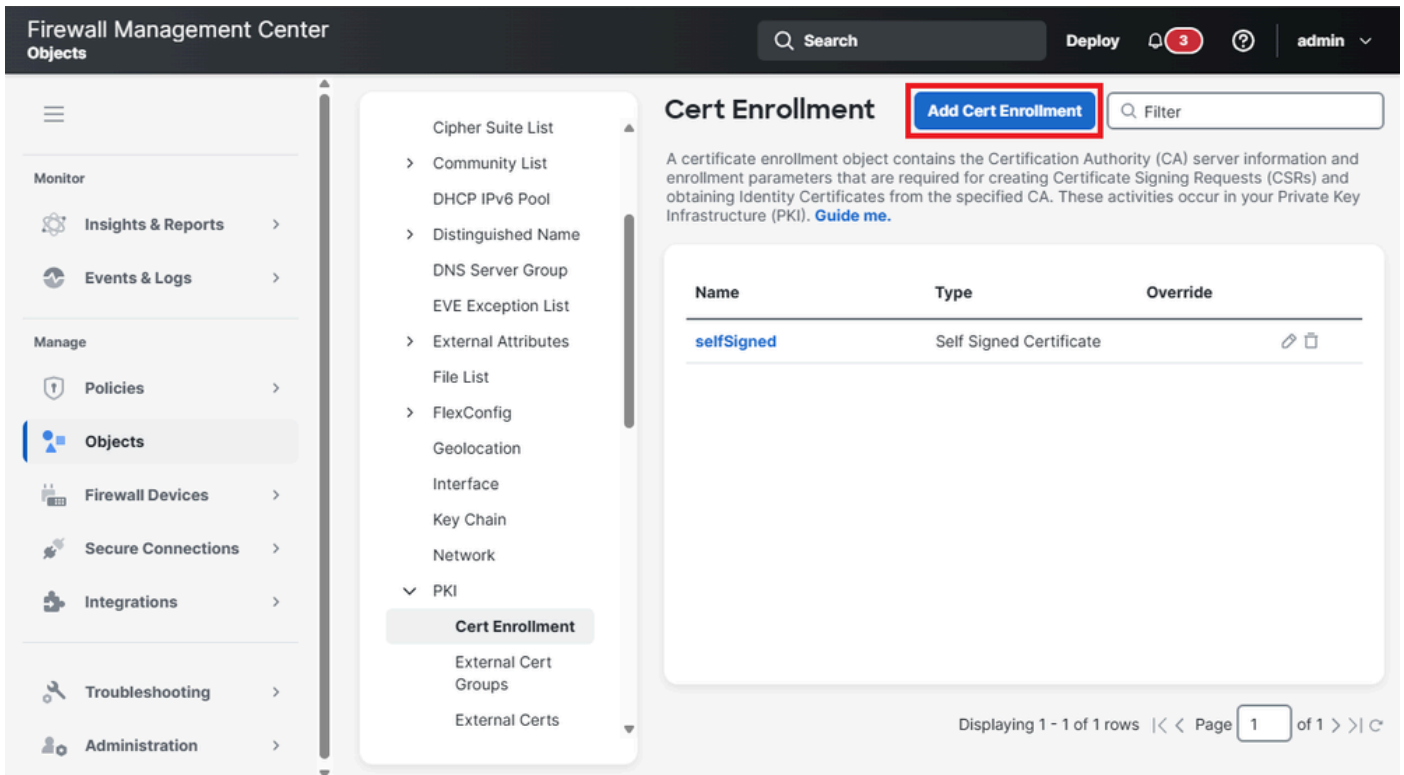
ايملا تال طورشللا اعاقتسا نم اذات ،ACME لئجست ايمع اعب لبق

1. اصاصلا ااداهشلا بلطت اذلا لاجملا مسا نوئي نأ بجي :لحلل لباقللا لاجملا مسا ايمكلم نم ققحتلاب مداخللا مائق ايمناكم نمضي اذم . ACME مداخل اقساوب لحلل الباق لاجملا
2. نامالا ايمحلا راجل نوئي نأ بجي :ACME مداخللا ايمحلا راجل لئليغشتلا لوصوللا اذم مئتي نأ مزلي ال . اصاصلا تاهجالولا ايمحلا لئليغشتلا لوصوللا ايمناكم اهلجا نم ااداهشلا بلطتمئتي ايمتلا ااهجالول ربع لوصوللا
3. ااهجالولا لئليغشتلا ACME CA مداخل نم 80 مقرر TCP اذفملا حامسلا :80 مقرر TCP اذفملا رفوتلا HTTP-01 ايمحلا لئليغشتلا ACME لئليغشتلا اناثا بولطم اذم . لاجملا مسالا اقساوباطملا

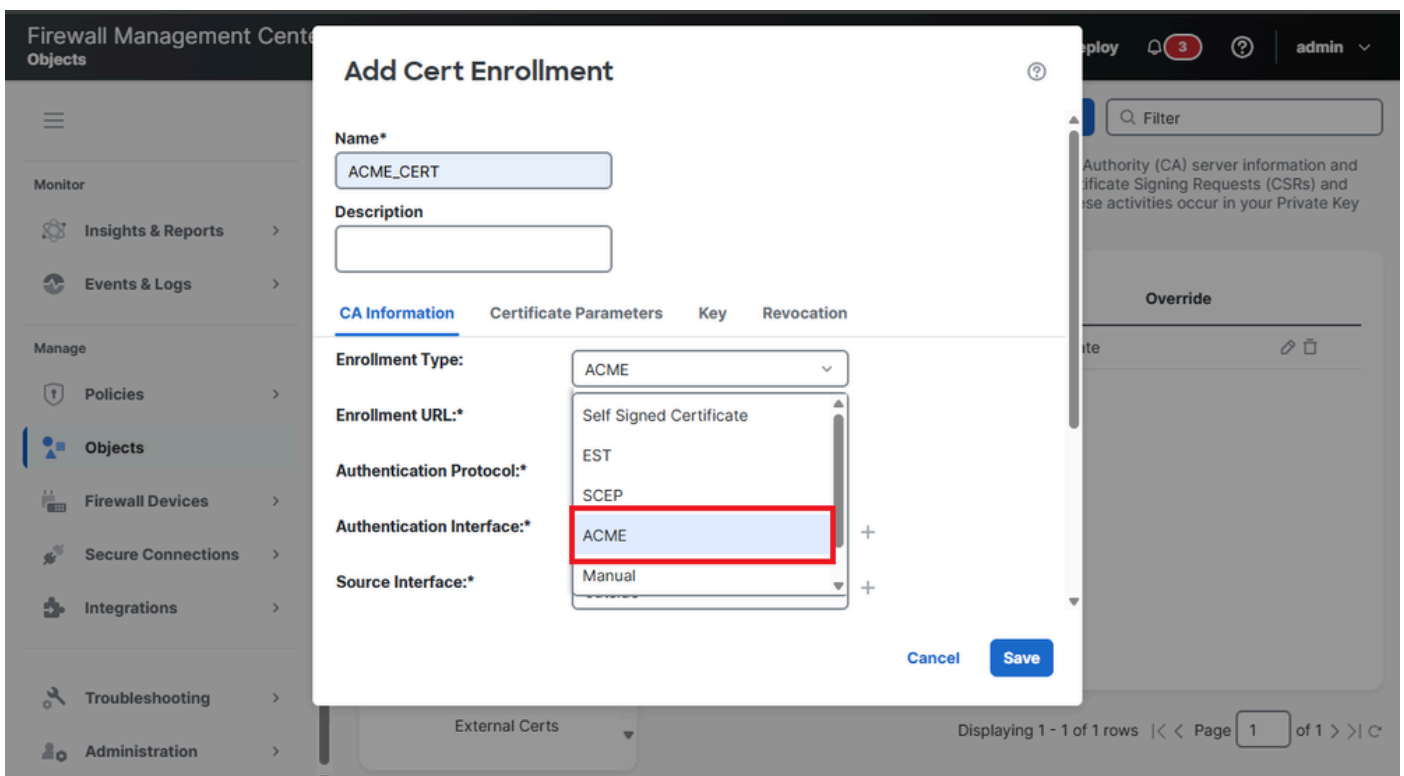
تانايب لئليغشتلا لوصوللا نمئتي ،ااوتفم 80 اذفملا ايمناكم نوئي ايمتلا اهرتفلا اناثا :اظحالم طوق ACME ايمحلا

ACME ااداهش لئليغشت نئياك اناشلا

1. عدب CERT ليچست ةفاضل قوف رقن او CERT ليچست > PKI > تانئال ال ةل لقتنا .
ن.نيوكت ال ةل عم



2. دح ACME ليچست ال قرط عم ةلدسنم ال ةمئال ال في ACME ليچست رايخ درس متي .
ةعباتم لل ليچست ال عون ةلدسنم ال ةمئال ال نم



3. ةبسانم لآ تامولعملاب لوقحلا لامك إو ،ةداهشلا تاملعم نيوكت تاراخي ضرع م تي .

- بلطل مدختسملا (Let'Encrypt لثم) ACME مداخ ناوع وه اذه :ليجستلل URL ناوع اهاع اچرتساو تاداهشلا .
- لاجملا ةيكلم نم ققحتلل مدختسملا بولسأل اذه ددحي :ةقداصملا لوكوتورب HTTP-01 وه ACME تايدحتل موعدملا لوكوتوربلاو .
- مداخ نم HTTP-01 يدحت لبقتسي يذلا FTD زاهج يل عةكبشلا هجاو :ةقداصملا هجاو ACME .
- ACME مداخ يف ةقتلل (CA) قدصم عجرم نم ةداهش رايتخا بجي :طقف CA ةداهش .

ةماعلا ريفشتلا ةمدخب صاخلا URL ناوع يل ريشي ،يضارتفا لكشب :ةظحالم
<https://acme-v02.api.letsencrypt.org/directory>.

4. مداخل CA ةداهش ةفاضل يل ةجاحب تنأف ،ايج فورعم ريغ ACME مداخ مدختست تنك اذا .
نارتقالا ليجست ةفاضل رزلا قوف رقناو نارتقالا ليجست > تانئاللا يل لقتنا ACME .



Firewall Management Center
Objects

Search Deploy 1 admin

Cert Enrollment

[Add Cert Enrollment](#) Filter

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI). [Guide me.](#)

Name	Type	Override
selfSigned	Self Signed Certificate	 

Displaying 1 - 1 of 1 rows | Page 1 of 1

- CA راڤخلا نم ققحت، كلذ دعب. Manual ك ليچستلا عون ددحو TrustPoint ةي مس تب مق. طافح قوف رقن او ACME Server CA ةداهش قصللا، اريخأ. طقف

Add Cert Enrollment



Enrollment Type:

Manual

CA Only

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

CA Certificate:

```
AQIi7AgEAMBOCA10dbgqWB  
BQK2IfhUvR3bCj3JIG9uyYIDf  
vpSjAfBgNVHSMEGDAW  
gBQTGOy4/RYYKsq+gWZrpp  
51e/TIdTAKBggqhkJOPQQDAg  
NIADBFAiEAqJuhxPuT  
+CRcqBjLTHcf0XDswHUQEnk  
V5ZOSDbwUI7ECIEPkLo0n2m  
DSGJIJrbeCM9jB5jet  
hKIfVaFOh77A7aZH  
-----END CERTIFICATE-----
```

Validation Usage:

IPsec Client

SSL Client

SSL Server

Cancel

Save

- طوقف CA صيخرت مسق يف ACME CA مداخل صاخلا TrustPoint ددح، اريخأ

Edit Cert Enrollment



Name*

ACME_CERT

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

ACME

Enrollment URL:*

https://10.31.124.58:4443/acme/...

Authentication Protocol:*

HTTP-01

Authentication Interface:*

outside



Source Interface:*

outside



CA only Certificate:

ACME_CA

Auto Enroll

Lifetime(10-99):

70

Regenerate Key

Validation Usage:

IPsec Client

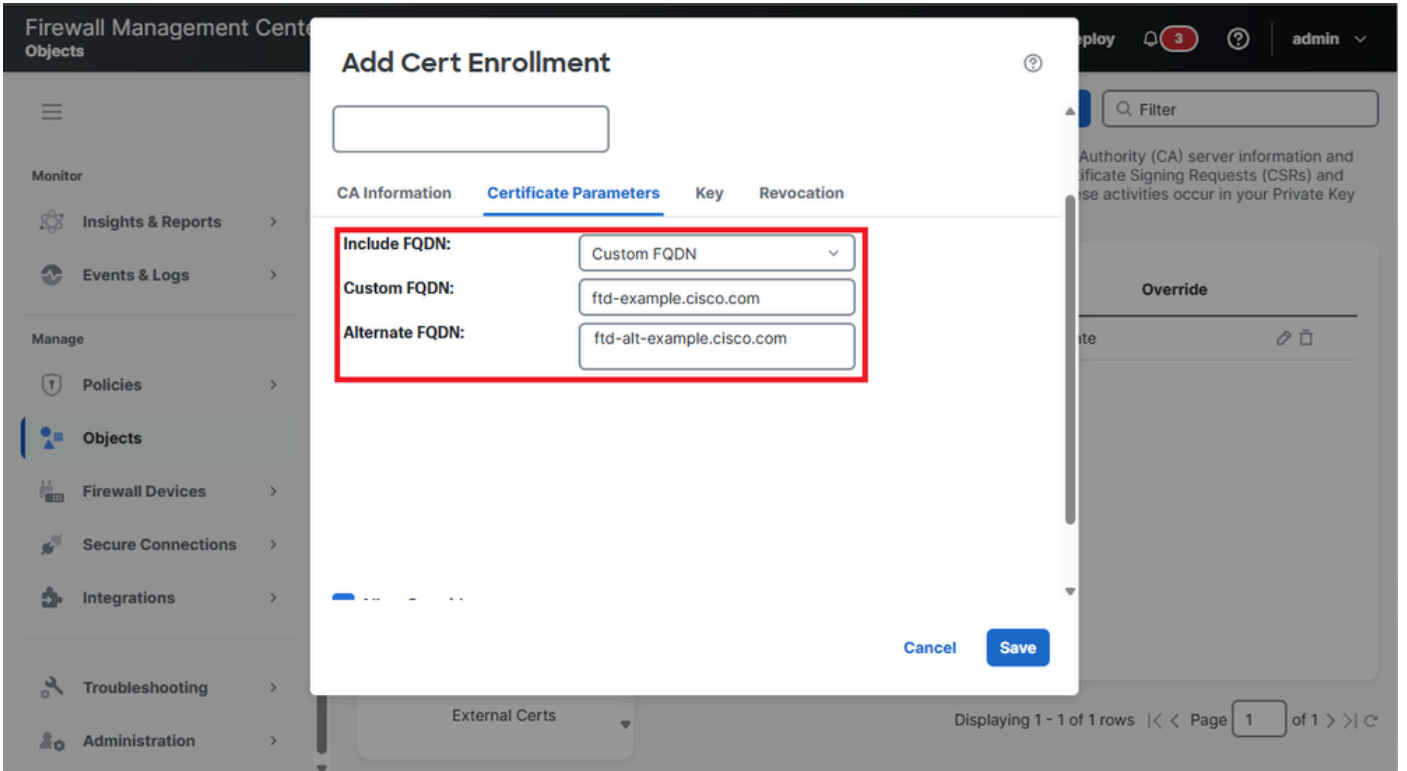
SSL Client

SSL Server

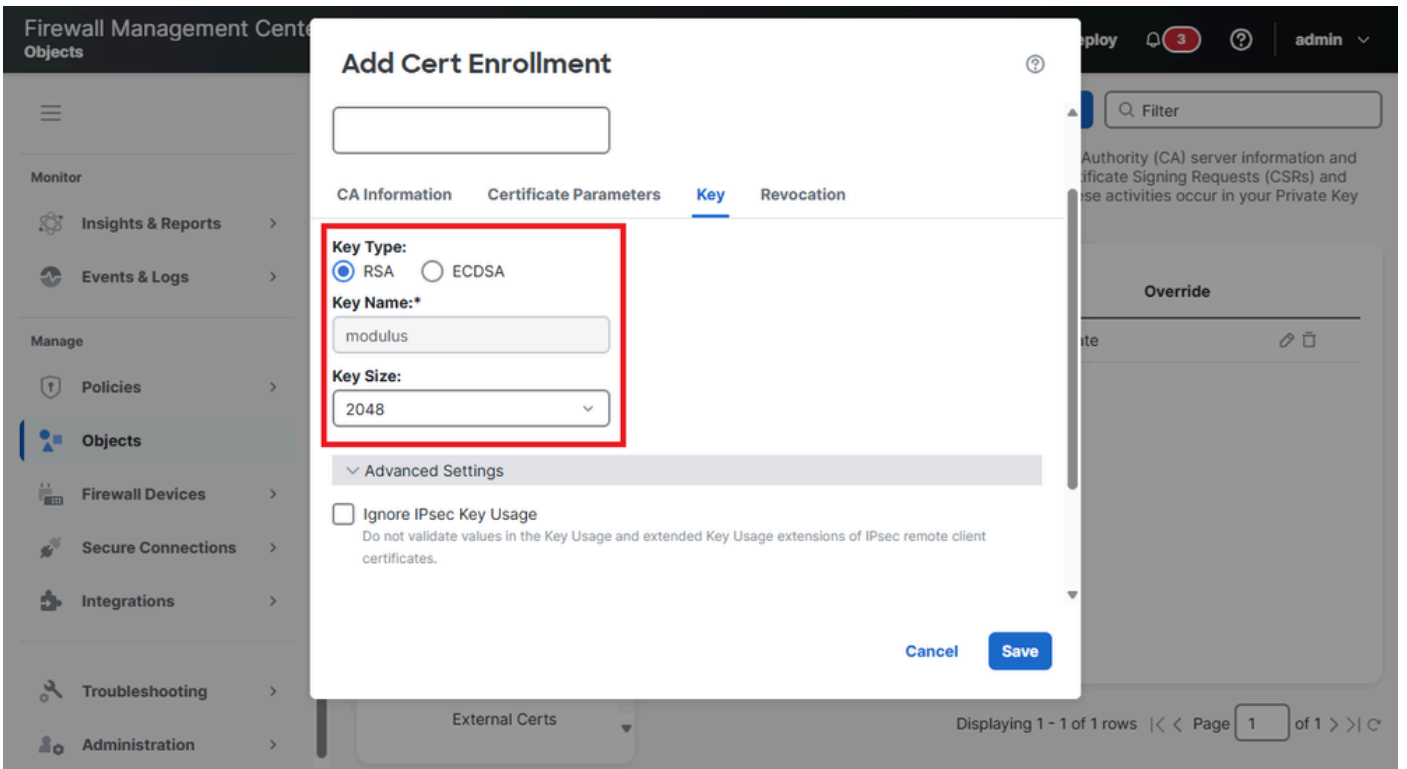
Cancel

Save

مقو FQDN نيمضت ع برم في صصخم ال FQDN راخ دحو، ةداهش ال تامل عم ال لقتنا 5. ةل دب تالاجم ءامسأ ي أو يساس ال FQDN عم لي دب ال FQDN و صصخم ال FQDN في ل قح ةئبعتب ةداهش ال في انه نيمضتل



6. حاات فملا مچوح حاات فملا عون تا اداعا لي دع تل حاات فملا ىل لقا تنا .



7. ةي وهلا ةداهشل ىل لقا تل لىج ستلا ني كمتب مق (ىراىخا) .

ىل لقا تل لىج ستلا اقب ةرتفل ةي وئملا ةبسنلا دحو Auto Registration رايخالا ةناخ دحو

ةيؤئلمة بسنللدحت. اهتجالص اهتناللق ايئاقلت ةداهشلل ديدجت ةزيملا هذ نمضت ل بس لىع. ديدجتاللة لمع اهيف أدبت يتلل ةداهشلل ةيجالص اهتنالقبست يتلال ةرتفال ةرتف نم 80% لىل ةداهشلل لصت امدنع ديدجتاللة لمع أدبت، 80% لىع اهنبيعت مت اذا، لالثلل اهتجالص.

Firewall Management Center
Objects

Add Cert Enrollment

CA Information Certificate Parameters Key Revocation

Enrollment Type: ACME

Enrollment URL:* https://acme-v02.api.letsencrypt...

Authentication Protocol:* HTTP-01

Authentication Interface:* Default: Management/Diagnosti... +

Source Interface:* outside +

CA only Certificate: Manual CA Certificate

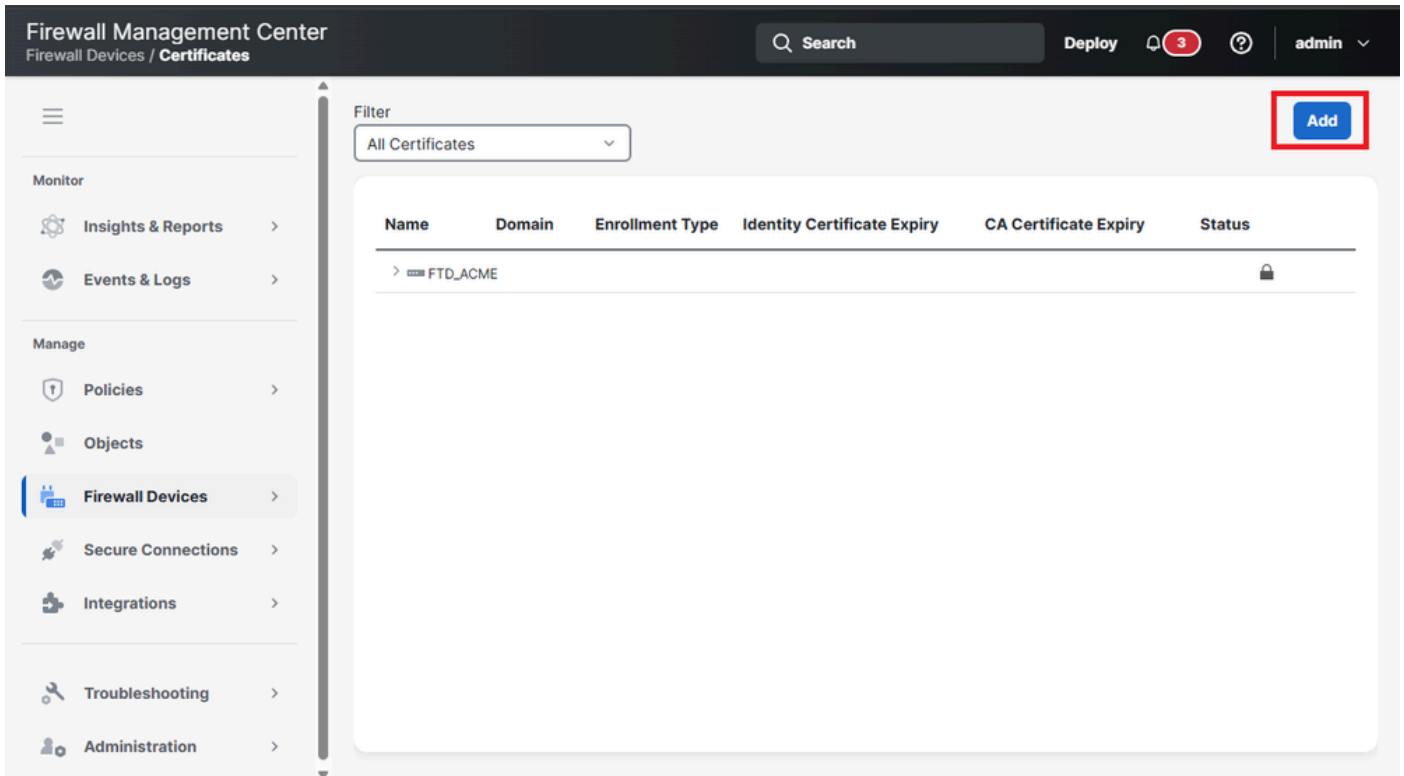
Auto Enroll Lifetime(10-99): 70 Regenerate Key

Cancel Save

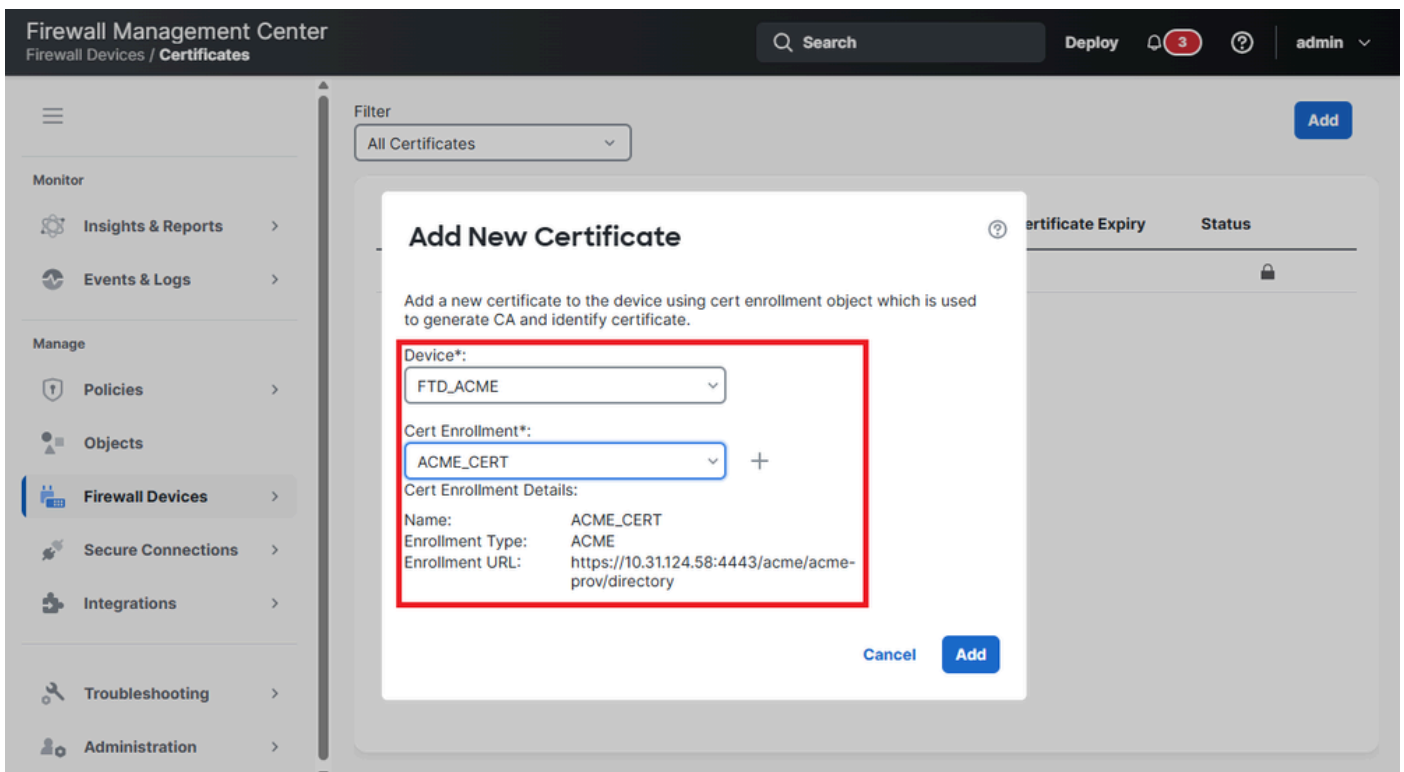
ظفح قوف رقنا 8.

زاهجال لىل ACME ةداهش لىجست

ةديدج ةداهش لىجستل ةفاضا رزلال قوف رقنا واداهشلل > ةياملجال رادج ةزهجال لىل لقتنا 1.



في اقبس م هؤاشنإ م ت يذلا ةداهشل نئاك و زاهجلا ةلدسنملا ةمئاقلا نم FTD زاهج ددح .2
جت نملا ليحست



ةفاضإ قوف رقنا .3

فرعملا ةداهش رز ةلاجل دومع ضرعي ،رشنلا لامتكأ درجمب .4

Firewall Management Center
Firewall Devices / Certificates

Search Deploy 3 ? admin

Filter: All Certificates Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD_ACME					
selfSigned	Global	Self-Signed	Jul 14, 2035		CA ID
ACME_CERT	Global	ACME	Jul 22, 2025 <i>Expires in a day</i>		CA ID
ACME_CA	Global	Manual (CA Only)		Jul 19, 2035	CA ID

5. فرع عمل رزى لى رقن لى اب فرع عمل اءءاءش ءامول عم ءءص نم ققءء.

Identity Certificate



- Status : Available
- Serial Number : 058f993097bd56758e 4555193be
- Issued By : acme Intermediate CA
O : acme
- Issued To: ft-examle.cisco.com
- Public Key Type : RSA (2048 bit)
- Signature Algorithm : ecdsa-with-SHA56
- Associated Trustpoints : ACME_CERT
- Valid From: : 11:20:55 UTC July 21 2025
- Valid To : 11:21:55 UTC July 22,2025
- Public Key Hashes : 26b7a0f741436434a53b26114478b245204
SHA1 PublicKey hash :
241256de8674656fc15551717844f651975b562c520a0

Close

ةحصلنا نم ققحتلنا

FTD يف ةتبتملنا ةداهشلنا ضرع

.show crypto ca certificates <trust point name> رمألنا يف ةلجسم ةداهشلنا نأ نم دكأت

<#root>

firepower#

show crypto ca certificates

ACME_CERT

Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a

Syslog ثادحاً

ليجستب عقولعتم الما ثادحاً لال طاق تلال نم آلا ةيامحل رادج ل FTD ي ف ةديج syslogs كانه
لوكوتورب مادختساب ةداهش ل
ACME:

• ACME. ةداهش ليجست أدبي ىتم نع تامولعم رفوي: 717067

%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.>

• ACME. ةداهش ليجست حاجن تقو نع تامولعم رفوي: 717068

%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa

• ACME. ليجست لشف تقو لوح تامولعم رفوي: 717069

%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>

• ةداهش ل دي دجت وأ ةداهش ل ليجستل حيتافم ل جوزب ةقولعت م تامولعم رفوت: 717070

%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>

اهحالصإو ءاطخأل افاشكتسا

ةلكشم ل فيرعتل ةيلالت ل تاوطخل ل في ريكفتلاب مقف، ACME ةداهش ليجستل لشف اذا
اهلحو:

- مداخب ةكبش لاصتا هيدل نمأل ةيامل رادج نأ نم دكأت: مداخلاب لاصتال نم ققحت
عنمت يتل ةيامل رادج دعاوق وأ ةكبشل ل في لكاشم دوجو مدع نم ققحت. ACME
لاصتال
- مت يذل لاجم ل مسا نأ نم دكأت: لجل لباق نمأل ةيامل رادج لاجم مسا نأ نم دكأت
ققحتل اذه دع. ACME مداخ ةطساوب لجل لباق FTD نمأل ةيامل رادج لعل هنيوكت
بلطلا ةحص نم ققحتل مداخلل ةيمهأل غلاب ارمأ ةحص ل نم
- ةكولمم TrustPoint في ةددحمل لالاجم ل ءامسأ ةفاك نأ نم ققحت: لاجم ل ةيكلم ديكأت
ةيكلم ةحص نم ققحتل هنكمي ACME مداخ نأ نمضي اذهو. نمأل ةيامل رادج ل FTD ل
لاجم ل

اهحالصإو ءاطخأل افاشكتسا رماو

ةيلالت ل ءاطخأل حيصت رماو تاجرخم عيمجتب مق، ةيفاضا تامولعم لعل لوصلل

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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 ا 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
ا م ك 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 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 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 (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