

قرا دمل ASA ىل ع تاداهشل دي دجت و تي ب ث ت (رم او ال رطس ة ه جاو) CLI ة ط ساوب

تايوت حمل

[قمدق م ل ا](#)

[قيس اساس ال ا تابل ط ت م ل ا](#)

[تابل ط ت م ل ا](#)

[قمدخت س م ل ا تانوك م ل ا](#)

[قيس اساس ا تامول عم](#)

[قداهش ل ا تي ب ث ت](#)

[ايتاذ عفوم ل ا قداهش ل ا لي ج س ت](#)

[\(CSR\) قداهش ل ا قط ساوب لي ج س ت ل ا عي قوت ب ل ط](#)

[PKCS12 لي ج س ت](#)

[قداهش ل ا دي دجت](#)

[ايتاذ عفوم ل ا قداهش ل ا دي دجت](#)

[\(CSR\) قداهش ل ا عي قوت ب ل ط عم ق ل ج س م ل ا قداهش ل ا دي دجت](#)

[PKCS12 دي دجت](#)

[ق ل ص ت ا ذ تامول عم](#)

قمدق م ل ا

رادمل Cisco ASA جم ان رب ىل ع تاداهشل نم ة ني عم عاون ا ب ل ط ة ي في ك دن ت س م ل ا اذ ه حضوي
اه دي دجت و اه قي ثوت و اه تي ب ث ت و (رم او ال رطس ة ه جاو) CLI مادخت ساوب

قيس اساس ال ا تابل ط ت م ل ا

تابل ط ت م ل ا

- خيرات ل او ع اس ل ا تقو و هي ل ع رفوت ي (ASA) في ك ت ل ل ل باق ل ا نام ال ا زا ه ن ا نم ق ق ح ت
لوكوت و رب م داخ مادخت ساوب ى صوي ، قداهش ل ا قداص م عم . قح ي ح ص ل ا ة ي نم ز ل ا قطن م ل ا و
ع ج ر م ل ل ق ل ص ل ا ت ا ذ تامول عم ل ا نم ق ق ح ت . ASA ىل ع تقو ل ا ة نم ا زم ل (NTP) ة ك ب ش ل ا تقو
ع ج ر م ىل ا ل و ص و ل ا ب ل ط ت ت اه ن ا ف ، (CSR) قداهش ل ا عي قوت ب ل ط م د خ ت س ت قداهش ب ل ط ل
، ة ي ج ر ا خ ة ه ج ل ني ع ب ا ت ل ا CA عي ئ ا ب ق ل ث م ا ل م ش ت . اه ب قو ث و م ة ي ج ر ا خ ة ه ج و ا ي ل خ ا د ق د ص م
، VeriSign و Thawte و GoDaddy و Geotrust و Entrust ، ر ص ح ل ا ل ل ا ث م ل ا ل ي ب س ىل ع

قمدخت س م ل ا تانوك م ل ا

قيل ل ا ل ا ق ي د ا م ل ا تانوك م ل ا و جم ا ر ب ل ا ت ا ر ا د ص ا ىل ا دن ت س م ل ا اذ ه ي ف ة د ر ا و ل ا تامول عم ل ا دن ت س ت

- ASA v 9.18.1
- OpenSSL مادخت ساوب م تي ، PKCS12 ء ا ش ن ا ل

ةصاخ ةي لم عم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراوللا تامولعمللا ءاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رمأ يأل لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش


ةيساسا تامولعمل

تاداهش وأ ايتاذ ةعقوم تاداهش يه دنتسملا اذه نيوانع اهيلع يوتحت يتلا تاداهشلا عون فيكتلل لباقللا نامألا زاهج حمانرب يف يلخاد قيصدت عجرم وأ يجرأخ قيصدت عجرم نم ةعقوم (رمأوالا رطس ةهجاوب رادملا Cisco). (CLI).

ةداهشلا تيبثت

ايتاذ ةعقوملا ةداهشلا ليحست

1. ددحم حاتفم مچحب يمس م حيتافم جوز ءاشنإب مق (يراي تخا).

 مچحو Default-RSA-Key مساب RSA حاتفم مادختسا متي، يضا رتفا لكشب: ةظحال م س فن مدختست ال يتح ةداهش لكل ديرف مسا مادختساب ي صوي، كلذ عمو؛ 2048 ماعلا/صاخلا حيتافم جوز.

```
<#root>
```

```
ASAv(config)#
```

```
crypto key generate rsa label
```

```
SELF-SIGNED-KEYPAIR
```

```
modulus
```

```
2048
```

```
INFO: The name for the keys will be: SELF-SIGNED-KEYPAIR
```

```
Keypair generation process begin. Please wait...
```

show crypto key mypubkey rsa. رمألا مادختساب هؤاشنإ مت يذلا حيتافملا جوز ةيؤر نكمي

```
<#root>
```

```
ASAv#
```

```
show crypto key mypubkey rsa
```

```
(...)
```

```
Key pair was generated at: 14:52:49 CEDT Jul 15 2022
```

```
Key name:
```

```
SELF-SIGNED-KEYPAIR
```

```
Usage: General Purpose Key
```

Key Size

(bits): 2048
Storage: config
Key Data:

```
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. لجس تال عونل تاذل نيوكت . ددحم مساب ةقث ةطقن عاشن |.

```
<#root>

ASAv(config)#

crypto ca trustpoint

    SELF-SIGNED
ASAv(config-ca-trustpoint)#

enrollment self
```

3. عوضومال مس او (FQDN) ل مالاب لهؤمال لاجمال مس نيوكت ب مق .



يتال ASA ةهجاوب صاخلا IP ناونع وأ FQDN FQDN ةملعم قباطت نأ بجي :ريذحت
ليدبلا عوضومال مس نيوكت ب ةملعمال هذه موقت . اهل ةداهشلا مادختسإ متي
ةداهشلل (SAN)

```
<#root>

ASAv(config-ca-trustpoint)#

fqdn

    asavpn.example.com
ASAv(config-ca-trustpoint)#

subject-name

CN=

asavpn.example.com,O=Example Inc,C=US,St=California,L=San Jose
```

4. بولطم ريغ . 1. ةوطخال ي ف هؤاشن | مت يذلا حيتافمال جوز مس نيوكت ب مق (ي راي تخ |).
يضا رتفال حيتافمال جوز مادختسإ ةلاح ي ف

```
<#root>

ASAv(config-ca-trustpoint)#

keypair

    SELF-SIGNED-KEYPAIR
ASAv(config-ca-trustpoint)# exit
```

5. ةءاهشلا ءاشنإ TrustPoint لىج س تب مق .

```
<#root>

ASAv(config)#
crypto ca enroll

SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]:

no

Generate Self-Signed Certificate? [yes/no]:

yes


ASAv(config)#
exit
```

6. show crypto ca certificates رمألا مادختساب ةءىءىل ءىقوتلا ءىءاذ ةءاهشلا ءىؤرن كمى ، اولامتكءا ءرءم بو .

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
start date: 15:00:58 CEDT Jul 15 2022
end date: 15:00:58 CEDT Jul 12 2032
Storage: config
Associated Trustpoints: SELF-SIGNED
```

ةداهش لال عيقوت بل طسة اوب ليجستال (CSR)

1. ددحم حاتفم مجحب ىمسم حيتافم جوز عاشن اب مق (يراي تخا).

 مجحو Default-RSA-Key مساب RSA حاتفم مادختسا متي، يضارتفا لكشب: طهحالم س فن مدختست ال يتح ةداهش لكل ديرف مسا مادختسا اب ىصوي، كلذ عمو؛ 2048 ماعل/صاخلا حيتافم جوز.

```
<#root>
ASAv(config)#
crypto key generate rsa label
    CA-SIGNED-KEYPAIR
modulus
    2048
INFO: The name for the keys will be: CA-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

show crypto key mypubkey rsa. رمألا مادختسا اب هؤاشن ا مت يذلا حيتافم لال جوز ةيؤر نكمي

```
<#root>
ASAv#
show crypto key mypubkey rsa
(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022
Key name:
    CA-SIGNED-KEYPAIR
Usage: General Purpose Key
Key size
    (bits): 2048
Storage: config
Key Data:
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. ليجستال عونل ةيفرطال ةدحولل نيوكت. ددحم مساب ةقث ةطقن عاشن ا.

```
ASAv(config)# crypto ca trustpoint CA-SIGNED
ASAv(config-ca-trustpoint)# enrollment terminal
```

3. تمام لع قباطت نأ بجي . عوضومل مساولم الكلاب لهؤملا لاجملا مسانويوكتب مق
ةداهشلا مادختسا متي يتلا ةمدخلاب صاخلا IP ناو نع وأ FQDN عم عوضوملا CN و FQDN
لأل.

```
ASAv(config-ca-trustpoint)# fqdn asavpn.example.com
ASAv(config-ca-trustpoint)# subject-name CN=asavpn.example.com,O=Example Inc,C=US,St=California,L=
```

4. 1. ةوطخلال يف هؤاشنإ مت يذل حيتافملا جوز مسانويوكتب مق (يراي تخإ).

```
ASAv(config-ca-trustpoint)# keypair CA-SIGNED-KEYPAIR
```

5. لاطبإ ةمئاق مادختساب - ةداهشلا لاطبإ نم ققحتلال بولسأ نويوكتب مق (يراي تخإ)،
يضارتفا لكشب . (OCSP) تنرتنإل ربع ةداهشلا ةلاح لوكوتورب وأ (CRL) ةداهشلا،
ةداهشلا لاطبإ نم ققحتلال ليطعت متي.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

6. قوئومك ةيوهلا ةداهش عقوتس يتلا CA ةداهش تيبتتو TrustPoint ةقداصم (يراي تخإ).
قداصملا عجرملا ةداهش تيبتت نكمي ، ةوطخلال هذه يف تيبتتال مدع ةلاح يف . اه.
ةيوهلا ةداهش عم اقحال.

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDXCcAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFMRcwFQYDVQQDEw5j
YS51eGFTcGx1LmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0xMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTA1BMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTi0GYa+WFTcZXSLHZA6WTUzLYM19IbSFHwa6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vkOesJfL2B7pEhGodLh7Gki1T4KoqL/1DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX481s3uxTPH8+B5QG0+d1wa0sbCWk
oK5sEPpHZ3IQuVxGii rp/zmomzx14G/te16eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh11K3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEF55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsX1FwK3j1NBw0sYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqarjixs153jV/YLk8E9oAIatnA/fQfX6V+h74yqucFF1js3d1FjyV14odRPwM
OjRyja1H56BF1ackNc7KRddtVxYB9sFEbFhN8od1BvnUedxGAJFHqxEQKmBE+h4w
gW8YnH0vM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcov0i/PaxnrA1J+Ng2jrwFN3MXWZ04S3CHYMGkwqHkaHCh1qD0x9badgfsyzz
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
```

WARNING: CA certificates can be used to validate VPN connections, by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported

7. عي قوت ل ق دصم ع جرم ى ل ا ه ل اس را و ه خ س ن ن ك م ي CSR ء ا ش ن ا و ء د ا ه ش ل ل ا ل ي ج س ت ب م ق ن ك م ي TrustPoint ل ب ق ن م م د خ ت س م ل ا ح ي ت ا ف م ل ا ج و ز ن م م ا ع ل ا ح ا ت ف م ل ل CSR ن م ض ت ي ا ذ ه ح ي ت ا ف م ل ا ج و ز ى ل ع ي و ت ح ت ي ت ل ا ز ه ج ا ل ل ب ق ن م ط ق ف ء ع ق و م ل ا ء د ا ه ش ل ل ا م ا د خ ت س ا



TrustPoint ي ف ء د د ح م ل ل Subject Name و FQDN ت ا م ل ع م ر ي ي غ ت CA ل ن ك م ي : ء ط ح ا ل م ء ع ق و م ء ي و ه ء د ا ه ش ء ا ش ن ا و CSR ع ي ق و ت د ن ع

```
ASAv(config)# crypto ca enroll CA-SIGNED
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate will be used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes

% Start certificate enrollment ..

% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor

% The fully-qualified domain name in the certificate will be: asavpn.example.com

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes

Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----

```
MIIDHzCCAgcCAQAwYsGZAZBgNVBAMTEUUBIG
A1UECgwLRXhhbXBsZSBjbmMxCzAJBgNVBAYTA1VTMRMwEQYDVQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAS5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/Or8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8It5g4kBdrUSCpr1+VMiTphQgBTAqRPk0vFX4rC8k/T
OPFDE+2gjT1wMn9reb92jYro1GK4MwZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkir062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDADBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUMPENIhHNjQjH
Yh08EOvWyoo9FaL fHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDwL9z
Duu8BQnBGU08T/H3yjdjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAVOAh81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BFGM1
10ApejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
```

-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no

8. ء ي و ه ء د ا ه ش ر ي ف و ت م ت ي ، CSR ع ي ق و ت د ر ج م ب . ء ي و ه ل ا ء د ا ه ش ل ل ا د ا ر ي ت س ا

```
ASAv(config)# crypto ca import CA-SIGNED certificate
```



```
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

PKCS12 لي جاست

تاداهش ةلسلسو، ةيوه ةداهش، حيتافم جوز لىل ع يوتحي يذلا PKCS12 فلم ي ف لي جاستلا ك ب صاخلا CA نم ةملتسم، ةيرايتخا (تاداهش) CA

1. ددحم مساب ةقت ةطقن ءاشن ا.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12
ASAv(config-ca-trustpoint)# exit
```



TrustPoint مساب دروتسملا حيتافملا جوز ىمسي : ةظحالم

2. لاطب ا ةمئاق مادختساب - ةداهشلا لاطب ا نم ققحتلا بولسا نيوكتب مق (يرايتخا)، يضارتفا لكشب (OCSP) تنرتن ا ل ربع ةداهشلا ةلاح لوكوتورب وا (CRL) ةداهشلا، ةداهشلا لاطب ا نم ققحتلا لي طعت متي.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. PKCS12 فلم نم ةداهشلا داريتسا ا.



ةعوبطملا فورحلا تناك اذا. رشم base64 نوكي نأ PKCS12 فلم جاتحي : ةظحالم فلم لي وحتل base64 هزيمرت متي هن ا ف، صننلا ررحم ي ف فلملا حتف دن ع ىرت همادختسا نكمي OpenSSL جذومن زمرم Base64 لىل ا يئانث.

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3TmOCaggAgIIHONjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqoKcwECD05
dnxCNJx6
quit
```

Trustpoint CA certificate accepted.

WARNING: CA certificates can be used to validate VPN connections, by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.

4. ةتبت م ل ا (تاداهش ل ا) ةداهش ل ا نم ق قحت .

```
ASAv# show crypto ca certificates TP-PKCS12
```

```
Certificate
Status: Available
Certificate Serial Number: 2b368f75e1770fd0
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
CN=asavpnpkcs12chain.example.com
O=Example Inc
L=San Jose
ST=California
C=US
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: TP-PKCS12
```

```
CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
```

start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12

عداهشال - نيمسقلال - CA عداهشو ويوهلال ىلع يوتحي PKCS12 ناك، قباسلال لاثملا ي
عداهشال. ةدوجوم طقف عداهشال نإف، الإو. CA عداهشو.

5. TrustPoint ةقداصم (يرايخا).

لكشب CA عداهش ىلع لوصحلال متو، CA عداهش ىلع يوتحي PKCS12 نكي مل اذا
ايودي اهتيبثت نكمي، PEM قيسنتب لصفنم.

```
ASAv(config)# crypto ca authenticate TP-PKCS12  
Enter the base 64 encoded CA certificate.  
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----  
MIIDXCcAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE  
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j  
(...)  
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5  
dcVcovOi/PaxnrA1J+Ng2jrwFN3MXWZ04S3CHYMGkqHkaHCh1qD0x9badgfsyzz  
-----END CERTIFICATE-----  
quit
```

```
INFO: Certificate has the following attributes:  
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02  
Do you accept this certificate? [yes/no]: yes
```

```
WARNING: CA certificates can be used to validate VPN connections,  
by default. Please adjust the validation-usage of this  
trustpoint to limit the validation scope, if necessary.
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

عداهشال دي دجت

ايتاذ ةعقومال عداهشال دي دجت

1. ةيلالال عداهشال ةيخالص ءاهتنا خيرات نم ققحت.
<#root>

```
# show crypto ca certificates SELF-SIGNED  
Certificate  
Status: Available  
Certificate Serial Number: 62d16084  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)
```

```
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:00:58 CEST Jul 15 2022

end date: 15:00:58 CEST Jul 12 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

2. إعدادات إنشاء شهادة.

```
ASAv# conf t
ASAv(config)# crypto ca enroll SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

WARNING: Trustpoint TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the current certificate will be replaced.
Do you want to continue with re-enrollment? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]: no
Generate Self-Signed Certificate? [yes/no]: yes
ASAv(config)# exit
```


3. عرض إعدادات إنشاء شهادة.


```
<#root>

ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16085
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
```


Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED

2. عي قوت لل CA لى لى هلا س راو هخسن نكمي يذلا CSR ءاشن اب مق . ءءاهش لا لي ج ست نكمي - TrustPoint لبق نم مدخت سمل احيات فملا جوز نم ماعلا احيات فملا CSR نمضتي اذ ه احيات فملا جوز لى ع يوتحت يتلا ءزهجال لبق نم طقف ءعقوملا ءءاهش لا مادختسا

 TrustPoint في ءءءملا Subject Name و FQDN تامل عم ريغيغ ت CA ل نكمي : ءظالم ءعقوم ءي وه ءءاهش ءاشن ا CSR عي قوت دن

 جاوزو fqdn/عوضوملا نيوكت ريغيغ مدع عم ، TrustPoint س فنل ءبس نلاب : ءظالم لال يه امك CSR ءبس ن س فن ءقحال ل لي ج ست لا تايل م ح نم ت ، احيات فملا ي ل و ال ل اءءال ءبس نلاب

```
ASAv# conf t
ASAv(config)# crypto ca enroll CA-SIGNED
```

```
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes
```

```
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=California
% The fully-qualified domain name in the certificate will be: asavpn.example.com
% Include the device serial number in the subject name? [yes/no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwYsGzAZBgNVBAMEMFZlYXZwbi5leGFtcGx1LmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhbnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA5cvZvr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/Or8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8ItD5g4kBdrUSCpr1+VMiTphQgBTAqRPk0vFX4rC8k/T
OPFDE+2gjT1wMn9reb92jYro1GK4MwZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMiG2EP2BgOKOT3Fzx0mVuekonQtRhizt+c
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BggqhkiG9w0BCQ4x
LjAsMASGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyo09FaLfhKVdLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3yjdjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAVOAh81xVUF0vuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGM1
10ApgejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

```
Redisplay enrollment request? [yes/no]: no
```

3. ءي وه ءءاهش ري فون متي ، CSR عي قوت درءمب . ءي وه لا ءءاهش ءاري ت سا

```
ASAv(config)# crypto ca import CA-SIGNED certificate
```

```
WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate will be used for VPN authentication this may cause connection problems. Would you like to continue with this enrollment? [yes/no]: yes
```

```
% The fully-qualified domain name in the certificate will be: asavpn.example.com
```

```
Enter the base 64 encoded certificate.  
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----  
MIIDgTCCAmmgAwIBAgIIMA+aIxCTntMwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE  
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFfMRcwFQYDVQDEw5j  
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMI  
MRswGQYDVQQDBHJhc2F2cG4uZXhhbXBsZS5jb20xZDAsBgNVBAoMCOV4YW1w  
bGUgSW5jMQswCQYDVQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTERMA8GA1  
UEBwwIU2FuIEpvc2UxITAFBgkqhkiG9w0BCQIMEFzYXZwbi5leGFtcGxlLmNvb  
TCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAA0XL2Va9YzHvDM+E974  
E9WfAwAEdGr7P0wXWlqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn  
OJGW698ddtLLPCLXeY0JAXa1Egqa5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxP  
toI09cDJ/a3m/do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0d  
Tjg5nsr+LhDGC0v56D8WV2fGIkDIhthD9gYncjk9xc8dJ1bnPKJ0LUYYmbfnM8  
sn0kaKsgUmpBGQcAAaHfKtRiOsf6R9d9CZyRt1CRMiJRaFR6r94y+83wPYpSJ7  
jWh5Iq90t1UDV8CAwEA AaMuMCwwCwYDVR0PBAQDAgWgMBOGA1UdEQQWMBSC  
EmFzYXZwbi5leGFtcGxlLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAFQUchY4U  
jhjkySMJAh7NT3TT5JJ4NzqW8qHawNq+YyHR+sQ6G3vn+6cYCU87tqW1Y3  
fXC27TwwREwMbg8NsJrr80hsChYby8kwELnTkrN7dJB17u50VQ3DRjfmFr  
J9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEMp7cB6veTcF9ru1DVRImd  
0KYE0x+HYav2INT2udcOG1yDwm1/mqdf0/ON2SpBBpnEgtiKshtsST/NAw25  
WjkrDIfn8uR2z5xpzxnEDUBoHOipG1gb1I6G1ARXW0+LwfB1n1QD5b/RdQ0U  
bLCPfKNPde/9wNnoXGD1J7qfZxr04T71d2Idug==  
-----END CERTIFICATE-----  
quit
```

```
INFO: Certificate successfully imported
```

4. ەدي دجال ەداهش لال ەي حال ص ەات نا خيرات نم ق قحت <#root>

```
ASAv# show crypto ca certificates CA-SIGNED  
Certificate  
Status: Available  
Certificate Serial Number: 300f9a2310ad36d3  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: RSA-SHA256  
Issuer Name:  
CN=ca.example.com  
OU=lab  
O=ww-vpn  
C=PL  
Subject Name:  
unstructuredName=asavpn.example.com  
L=San Jose  
ST=California  
C=US  
O=Example Inc  
CN=asavpn.example.com  
Validity Date:
```

start date: 16:09:00 CEDT Jul 20 2022

end date: 16:09:00 CEDT Jul 20 2023

Storage: config

Associated Trustpoints: CA-SIGNED

PKCS12 ديدجت

ةداهش تيبتتل PKCS12 فلم مادختساب ةلجسم TrustPoint في ةداهش ديدجت نكمي ال ةديدج TrustPoint ءاشن بجي، ةديدج

1. ددجم مساب ةقث ةطقن ءاشن |.


```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12-2022
```

```
ASAv(config-ca-trustpoint)# exit
```

2. لاطب ةمئاق مادختساب - ةداهش لاطب نم ققحتل لبولسأ نيوكتب مق (يرايتخا) ،يضارتفا لكش ب (OCSP) تنرتنإل ربع ةداهش لةلاح لوكوتورب وأ (CRL) ةداهش لةداهش لاطب نم ققحتل ليطعت متي

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. PKCS12 فلم نم ةديدجل ةداهش لداريتس |.

 ةعوبطملا فورحلا تناك اذا . رشم base64 نوكي نأ PKCS12 فلم جاتحي :ةظحالم فلم ليوحتل . base64 هزيمرت متي هنإف ،صننل ررحم في فلملحتف دنع ىرت OpenSSL مادختسإ نكمي ، base64 زمرم جذومن لىل يئانث

```
openssl enc -base64 -in asavnpkcs12chain.example.com.pfx -out asavnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12-2022 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCCBcGCSqGSIb3DQEH  
BqCCCAgwgggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c  
wqE3TmOCAggAgIIHONjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzKKq  
(...)
```

```
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA  
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqKcWECDO5  
dnxCNJx6
```

```
quit
```

Trustpoint CA certificate accepted.

WARNING: CA certificates can be used to validate VPN connections, by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary.

Associated Trustpoints: TP-PKCS12-2022

CA Certificate

Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
Subject Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12-2022

رهظي، كذلك، CA، عدهاشو ةيوهلا عدهاش ىلع يوتحي PKCS12 ناك، قباسلا لاثملا ي
ادوجوم طقف عدهاشلا لادخا نوكي، الاو. CA عدهاشو عدهاشلاو داريتسالا دعب نالادخا

5. TrustPoint ةقداصم (يارياتخا).

لكشب CA عدهاش ىلع لوصحلا متو، CA عدهاش ىلع يوتحي PKCS12 نكي مل اذا
ايودي اهتيبثت نكي، PEM قيسنتب لصفنم.

```
ASAv(config)# crypto ca authenticate TP-PKCS12-2022
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXCCAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYD
VQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcov0i/PAXnrA1J+Ng2jrWfN3MXWZ04S3CHYMGkqHkaHCh1qDOx9badgfsyzz
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
```

```
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.
```


```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

6. ةميدقلا ةطقنلا نم الءب ةديءلا ةقثلا ةطقن مادختسالا ASA نيوكت ةءاعاب مق.

لاثم:

```
ASAv# show running-config ssl trust-point
ssl trust-point TP-PKCS12
ASAv# conf t
ASAv(config)#ssl trust-point TP-PKCS12-2022
ASAv(config)#exit
```

 نيوكتال نم ققحت. ةفلتخم نيوكت رصانع ي ف TrustPoint مادختسإ نكمي: ةظحالم مئدقلا TrustPoint مادختسإ متي شيح كب صاخلا

ةلص تاذا تامولعم

ASA. لعل تقولا تادادعإ نيوكت ةيفيك

عالطال 9.18 ةماعلا Cisco ASA تاي لمعل رماوالا رطس ةهجاو نيوكت ليلد نم ققحت
ASA. لعل يحيص لكشب خيراتلاو تقولا دادعإ ةبولطملا تاوطخلا لعل
<https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/configuration/general/asa-918-general-config/basic-hostname-pw.html#ID-2130-000001bf>

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 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة 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 ة 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