Install and Renew Certificates on ASA Managed by CLI

Contents

Introduction

This document describes how to request, install, trust, and renew, certain types of certificates on Cisco ASA Software managed with CLI.

Prerequisites

Requirements

- Verify that the Adaptive Security Appliance (ASA) has the correct clock time, date, and time zone. With certificate authentication, it is recommended to use a Network Time Protocol (NTP) server to synchronize the time on the ASA. Check Related Information for reference.
- To request a certificate that uses Certificate Signing Request (CSR), it requires access to a trusted internal or third-party Certificate Authority (CA). Examples of third-party CA vendors include, but are not limited to, Entrust, Geotrust, GoDaddy, Thawte, and VeriSign.

Components Used

The information in this document is based on these software and hardware versions:

- ASAv 9.18.1
- For PKCS12 creation, OpenSSL is used.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The type of certificates this document addresses are self-signed certificates, certificates signed by a 3rd party Certificate Authority, or internal CA, on Cisco Adaptive Security Appliance Software managed with Command Line Interface (CLI).

Certificate Installation

Self-Signed Certificate Enrollment

1. (Optional) Create a named keypair with specific key size.

   > **Note:** By default, the RSA key with the name of Default-RSA-Key and a size of 2048 is used; however, it is recommended to use a unique name for each certificate so that they do not use the same private/public keypair.

   ```
   <#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...
   ```

   The generated keypair can be seen with command **show crypto key mypubkey rsa**.

   ```
   <#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. Create a trustpoint with a specific name. Configure enrollment type **self**.
   <#root>

```
ASAv(config)#

crypto ca trustpoint

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

enrollment self
```

3. Configure the Fully Qualified Domain Name (FQDN) and Subject Name.

> **Caution**: The FQDN parameter must match the FQDN or the IP address of the ASA interface that the certificate is used for. This parameter sets the Subject Alternative Name (SAN) for the certificate.

<#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. (Optional) Configure keypair name created in Step 1. Not required if the default keypair is used.
   <#root>

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

keypair

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

5. Enroll the trustpoint and generate the certificate.
   <#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. Once completed, the new self-signed certificate can be seen with command **show crypto ca certificates <truspoint name">.**

   ```
   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
   ```

Enrollment By Certificate Signing Request (CSR)

1. (Optional) Create a named keypair with specific key size.

   > **Note:** By default, the RSA key with the name of Default-RSA-Key and a size of 2048 is used; however, it is recommended to use a unique name for each certificate so that they do not use the same private/public keypair.

   <#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...
```

The generated keypair can be seen with command **show crypto key mypubkey rsa**.

<#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. Create a trustpoint with a specific name. Configure enrollment type **terminal**.

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

3. Configure the Fully Qualified Domain Name and Subject Name. The FQDN and the Subject CN parameters must match the FQDN or IP address of the service for which the certificate is used.

   ```
   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. (Optional) Configure keypair name created in step 1.

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

5. (Optional) Configure certificate revocation check method - with Certificate Revocation List (CRL) or with Online Certificate Status Protocol (OCSP). By default, certificate revocation check is disabled.

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

6. (Optional) Authenticate the trustpoint and install the CA certificate that is going to sign the identity

certificate as trusted. If not installed at this step, the CA certificate can be installed later together with identity certificate.

```
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-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTAlBMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29LynOg9/CTiOGYa+WFTcZXSLHZA6WTUzLYM19IbSFHWa6
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QGO+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
OjRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8odlBvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvMO8svyTXSLlJf0UCdmAY+lGOgqhUlSlkFBtLRt6Z2uCot0ONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----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. Enroll the certificate and generate a CSR that can be copied and sent to a CA for signing. The CSR includes the public key from the keypair used by trustpoint. The signed certificate can only be used by devices that have that keypair.

> **Note:** CA can alter the FQDN and Subject Name parameters defined in the trustpoint when signing the CSR and creating signed identity certificate.

```
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-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x12Oss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
OPFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2BgOKOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkirO62VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmAOpDWL9z
Duu8BQnBGuN08T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

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

8. Import the identity certificate. Once the CSR has been signed, an identity certificate is provided.

```
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-----
MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmVO9l6iSF/ULGlzXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgM0BosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

9. Verify the certificate chain. Once completed, the new identity certificate and the CA certificate can be seen with command **show crypto ca certificates <trustpoint name>.**

```
ASAv# show crypto ca certificates CA-SIGNED
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: CA-SIGNED

Certificate
Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
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: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

PKCS12 Enrollment

Enroll with the PKCS12 file that contains keypair, identity certificate, and optionally CA certificate(s) chain, received from your CA.

1. Create a trustpoint with a specific name.

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

Note: The imported keypair is named after the trustpoint name.

2. (Optional) Configure certificate revocation check method - with Certificate Revocation List (CRL) or with Online Certificate Status Protocol (OCSP). By default, certificate revocation check is disabled.

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

3. Import the certificate from a PKCS12 file.

Note: The PKCS12 file needs to be base64 encoded. If printable characters are seen when file is opened in text editor, then it is base64 encoded. To convert a binary file to base64 encoded form openssl can be used.

```
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:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03l0j7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/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. Verify the installed certificate(s).

```
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
```

In the previous example, the PKCS12 contained the identity and CA certificate - the two entries - Certificate and CA Certificate. Otherwise, only Certificate is present.

5. (Optional) Authenticate the trustpoint.

   If the PKCS12 did not contain the CA certificate, and the CA certificate was obtained separately in PEM format, then it can be installed manually.

```
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-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----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
```

Certificate Renewal

Renew Self-Signed Certificate

1. Check the current certificate expiry date.
   <#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 CEDT Jul 15 2022

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

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

2. Regenerate the certificate.

```
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. Verify the new certificate.
   <#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
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:09:09 CEDT Jul 20 2022

end date: 15:09:09 CEDT Jul 17 2032

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

Renew Certificate Enrolled with Certificate Signing Request (CSR)

Note: If any of the new certificate elements (subject/fqdn, keypair) need to be changed for the new certificate, then create a new certificate. Refer to Enrollment using Certificate Signing Request (CSR) section. The next procedure just refreshes the certificate expiry date.

1. Check the current certificate expiry date.
   <#root>

```
ASAv# show crypto ca certificates CA-SIGNED


Certificate

Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
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: 15:33:00 CEDT Jul 15 2022
```

`end date: 15:33:00 CEDT Jul 15 2023`

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

Certificate
Subject Name:
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED
```

2. Enroll the certificate. Generate a CSR that can be copied and sent to a CA for signing. The CSR includes the public key from the keypair used by trustpoint - the signed certificate can only be used by devices that have that keypair.

> **Note:** CA can alter the FQDN and Subject Name parameters defined in the trustpoint when signing the CSR and creating signed identity certificate.

> **Note:** For the same Trustpoint, with no changed subject/fqdn and keypair configuration, subsequent enrollments gives the same CSR as the initial one.

```
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=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-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
```

```
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/Or8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x12Oss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
OPFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3Fzx0mVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkirO62VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
YhO8EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuNO8T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
lOApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

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

3. Import the identity certificate. Once the CSR has been signed, an identity certificate is provided.

```
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
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMzA3MjAxNDA5MDBaMIGL
MRswGQYDVQQDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUg
SW5jMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMEmFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8olf9yvdiCE/9K/HLgFHua0eLIO72l2AksnEm8CnOJGW698ddtL
LPCLXeYOJAXa1Egqa5flTIk6YUIAUwKkT5NLxV+KwvJPO9DxQxPtoIO9cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYNCjk9xc8dJlbnpKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrTlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq9OtlUDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TwweREwMbq8NsJrr8OhsChYby8kwE
LnTkrN7dJBl7u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9rulDVRImd0KYEOx+HYav2INT2udc0G1yDwml/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfN8uR2z5xpzxnEDUBoHOipGlgb1I6G1ARXWO+LwfBl
n1QD5b/RdQOUbLCpfKNPdE/9wNnoXGDlJ7qfZxrO4T7ld2Idug==
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
```

4. Verify the new certificate expiry date.
   <#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 Renewal

It is not possible to renew a certificate in trustpoint enrolled using PKCS12 file. To install a new certificate, a new trustpoint needs to be created.

1. Create a trustpoint with a specific name.

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

2. (Optional) Configure certificate revocation check method - with Certificate Revocation List (CRL) or with Online Certificate Status Protocol (OCSP). By default, certificate revocation check is disabled.

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

3. Import the new certificate from a PKCS12 file.

   > **Note:** The PKCS12 file needs to be base64 encoded. If printable characters are seen when file is opened in text editor, then it is base64 encoded. To convert a binary file to base64 encoded form, openssl can be used.
   >
   > ```
   > openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.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:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/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.
```

> **Note:** If the new PKCS12 file contains an identity certificate with the same keypair that was used with the old certificate, the new trustpoint refers to old keypair name.
> Example:

<#root>

```
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:

MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
...
dnxCNJx6
quit


WARNING: Identical public key already exists as TP-PKCS12


ASAv(config)# show run crypto ca trustpoint

TP-PKCS12-2022

crypto ca trustpoint TP-PKCS12-2022


keypair TP-PKCS12

 no validation-usage crl configure
```

4. Verify the installed certificate(s).
<#root>

```
ASAv# show crypto ca certificates TP-PKCS12-2022
```

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
 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-PKCS12-2022
```

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
```

In the previous example, the PKCS12 contained the identity certificate and the CA certificate, therefore, two entries are seen after the import, Certificate and CA Certificate. Otherwise, only Certificate entry is present.

5. (Optional) Authenticate the trustpoint.

   If the PKCS12 did not contain the CA certificate, and the CA certificate was obtained separately in PEM format, then it can be installed manually.

```
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-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----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. Reconfigure the ASA to use the new trustpoint instead of the old one.

Example:

```
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
```

Note: A trustpoint can be used in different configuration elements. Check your configuration where the old trustpoint is used.

Related Information

How to configure time settings on an ASA.

Check the Cisco ASA Series General Operations CLI Configuration Guide 9.18 for the steps required to set up the time and date correctly on the ASA.
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