

CLIで管理されるASAでの証明書のインストールと更新

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[証明書のインストール](#)

[自己署名証明書の登録](#)

[証明書署名要求\(CSR\)による登録](#)

[PKCS12登録](#)

[証明書の更新](#)

[自己署名証明書の更新](#)

[証明書署名要求\(CSR\)に登録されている証明書の更新](#)

[PKCS12更新](#)

[関連情報](#)

はじめに

このドキュメントでは、CLIで管理されるCisco ASAソフトウェアの特定タイプの証明書を要求、インストール、信頼、および更新する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 適応型セキュリティアプライアンス(ASA)のクロックの時刻、日付、およびタイムゾーンが正しいことを確認します。証明書認証では、Network Time Protocol (NTP) サーバを使用して ASA 上で時刻を同期することをお勧めします。「関連情報」を参照してください。
- 証明書署名要求(CSR)を使用する証明書を要求するには、信頼できる内部またはサードパーティの認証局(CA)にアクセスする必要があります。サードパーティCAベンダーの例としては、Entrust、Geotrust、GoDaddy、Thawte、およびVeriSignなどがありますが、これらに限定されるわけではありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASAv 9.18.1
- PKCS12の作成には、OpenSSLが使用されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。


背景説明

このドキュメントで扱う証明書のタイプは、自己署名証明書、コマンドラインインターフェイス (CLI) で管理されるCisco適応型セキュリティアプライアンスソフトウェアのサードパーティ認証局(CA)または内部CAによって署名された証明書です。

証明書のインストール

自己署名証明書の登録

1. (オプション) 特定のキーサイズで名前付きキーペアを作成します。

 注：デフォルトでは、Default-RSA-Keyという名前でサイズが2048のRSAキーが使用されますが、証明書ごとに一意の名前を使用して、それらが同じ秘密キーペアまたは公開キーペアを使用しないようにすることを推奨します。

```
<#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...
```

生成されたキーペアはコマンドで確認できます `show crypto key mypubkey rsa.`

```
<#root>
```

```
ASAv#
```

```
show crypto key mypubkey rsa
```

```
(...)
```

```
Key pair was generated at: 14:52:49 CEST 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
```

- 特定の名称でトラストポイントを作成します。登録タイプselfを設定します。

```
<#root>
```

```
ASAv(config)#
```

```
crypto ca trustpoint
```

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

`enrollment self`

- 完全修飾ドメイン名(FQDN)とサブジェクト名を設定します。



注意: FQDNパラメータは、証明書が使用されるASAインターフェイスのFQDNまたはIPアドレスと一致する必要があります。このパラメータは、証明書のサブジェクト代替名(SAN)を設定します。

<#root>

ASAv(config-ca-trustpoint)#

`fqdn`

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

`subject-name`

`CN=`

asavpn.example.com,0=Example Inc,C=US,St=California,L=San Jose

- (オプション) 手順1で作成したキーペア名を設定します。デフォルトのキーペアを使用する場合は不要です。

<#root>

ASAv(config-ca-trustpoint)#

keypair

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

- トラストポイントを登録し、証明書を生成します。

<#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

- 完了すると、`show crypto ca certificates <truspoint name>`コマンドを使用して、新しい自己署名証明書を表示できます。

```
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
```

証明書署名要求(CSR)による登録

- (オプション) 特定のキーサイズで名前付きキーペアを作成します。



注：デフォルトでは、Default-RSA-Keyという名前でサイズが2048のRSAキーが使用されますが、証明書ごとに一意の名前を使用して、それらが同じ秘密キーペアまたは公開キーペアを使用しないようにすることを推奨します。

<#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...
```

生成されたキーペアはコマンドで確認できます **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
```

- 特定の名称でトラストポイントを作成します。登録タイプ `terminal` を設定します。

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

- 完全修飾ドメイン名とサブジェクト名を設定します。FQDNパラメータとSubject CNパラメータは、証明書が使用されるサービスのFQDNまたはIPアドレスと一致している必要があります。

```
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=
```

- (オプション) 手順1で作成したキーペア名を設定します。

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

- (オプション) 証明書失効チェックメソッドを、証明書失効リスト(CRL)またはオンライン証明書ステータスプロトコル(OCSP)を使用して設定します。デフォルトでは、証明書失効チェックは無効になっています。

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

- (オプション) トラストポイントを認証し、ID証明書に信頼済みとして署名するCA証明書をインストールします。この手順でインストールされていない場合は、CA証明書をID証明書と一緒に後からインストールできます。

```
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
YS5leGFtcG9uLmNvbnR1eS51e390eBMDaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTA1BMMQswDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS51e390eEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTi0GYa+WFTcZXS LHZA6WTUzLYM19IbSFHwa6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
```



```
4noWaXH1boGGD7+5vkOesJfL2B7pEhGodLh7Gki1T4KoqL/1DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX481s3uxTPH8+B5QG0+d1wa0sbCwk
oK5sEPpHZ3IQvXGiirp/zmomzx14G/te16eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh11K3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR00BBYEF55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMAOGCSqGSIb3DQEBCwUAA4IBAQArsX1FwK3j1NBw0sYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqarjjsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
OjRyja1H56BFlackNc7KRddtVxYB9sfEbFhN8od1BvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvM08svyTXSL1Jf0UCdmAY+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

- 証明書を登録し、コピーして署名のためにCAに送信できるCSRを生成します。CSRには、トラストポイントで使用されるキーペアからの公開キーが含まれています。署名付き証明書は、そのキーペアを持つデバイスでのみ使用できます。



注：CAは、CSRに署名し、署名付きID証明書を作成するときに、トラストポイントで定義されているFQDNパラメータとサブジェクト名パラメータを変更できます。

```
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-----
```

```
MIIDH2CCAgcCAQAwYsXgAZBGNVBAEMFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECGRlRXhhbXBsZSBSBmMxMzZlZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
bm1hMREwDwYDVQHDAAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8It5g4kBdrUSCpr1+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpuDms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMiG2EP2Bg0K0T3Fzx0mVuekonQtRhiZt+c
```

```
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyo09FaL fHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAV0Ah81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BfGM1
10ApejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]: no

- ID証明書をインポートします。CSRが署名されると、ID証明書が提供されます。

```
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-----
MIIDoTCCAomgAwIBAgIIBkLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVoQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHT8BcPmV0916iSF/ULG1zXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgMOBosJx65u/n75KnBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

- 証明書チェーンを確認します。完了すると、`show crypto ca certificates <trustpoint name>`コマンドを使用して、新しいID証明書とCA証明書を表示できます。

```
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登録

CAから受け取ったキーペア、ID証明書、およびオプションでCA証明書チェーンを含むPKCS12ファイルに登録します。

- 特定の名称でトラストポイントを作成します。

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



注：インポートされたキーペアの名称は、トラストポイントの名称に基づいています。

- (オプション) 証明書失効チェックメソッドを、証明書失効リスト(CRL)またはオンライン証明書ステータスプロトコル(OCSP)を使用して設定します。デフォルトでは、証明書失効チェックは無効になっています。

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

- PKCS12ファイルから証明書をインポートします。



注：PKCS12ファイルはBase64でエンコードする必要があります。ファイルをテキストエディタで開いたときに印刷可能な文字が表示される場合は、base64エンコードです。バイナリファイルをbase64エンコード形式に変換するには、opensslを使用できます。

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

コマンド：

```
crypto ca import trustpoint pkcs12 passphrase \[ nointeractive \]
```

```
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  
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c  
wqE3Tm0CAggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq  
(...)
```

```
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.
```

- インストールされた証明書を確認します。

```
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
```

前の例では、PKCS12にIDとCA証明書（2つのエントリである証明書とCA証明書）が含まれていました。それ以外の場合は、証明書のみが存在します。

- （オプション）トラストポイントを認証します。

PKCS12にCA証明書が含まれておらず、CA証明書がPEM形式で個別に取得されている場合は、手動でインストールできません。

```
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-----
MIIDXCcCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVoQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcov0i/PAXnrA1J+Ng2jrwFN3MXWZ04S3CHYMGkqWqHkaHCh1qD0x9badgfsyzz
-----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

証明書の更新

自己署名証明書の更新

- 現在の証明書の有効期限を確認します。

```
<#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

- 証明書を再生成します。

```
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
```

- 新しい証明書を確認します。

<#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 CEST Jul 20 2022

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

Storage: config
Associated Trustpoints: SELF-SIGNED

証明書署名要求(CSR)に登録されている証明書の更新

 注：新しい証明書の新しい証明書要素(subject/fqdn、keypair)を変更する必要がある場合は、新しい証明書を作成します。「証明書署名要求(CSR)を使用した登録」セクションを参照してください。次の手順では、証明書の有効期限を更新するだけです。

- 現在の証明書の有効期限を確認します。

<#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 CEST Jul 15 2022

end date: 15:33:00 CEST 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

- 証明書を登録する署名のためにコピーしてCAに送信できるCSRを生成します。CSRには、トラストポイントが使用するキーペアの公開キーが含まれています。署名付き証明書は、そのキーペアを持つデバイスでのみ使用できます。



注：CAは、CSRに署名し、署名付きID証明書を作成するときに、トラストポイントで定義されているFQDNパラメータとサブジェクト名パラメータを変更できます。



注：同じトラストポイントに対して、サブジェクト/fqdnおよびキーペアの設定が変更されていない場合、後続の登録では最初のトラストポイントと同じCSRが提供されます。

```
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-----
MIIDHzCCAQcCAQAwYsxCZAZBgNVBAMEMFZlYXZwbi5leGFtcG91LmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBjb2MxMzZlZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
Ym1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/Or8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8It5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+c
```

```
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyo09FaL fHKVDLvFxh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAV0Ah81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BFGM1
10ApgeJACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]: no

- ID証明書をインポートします。CSRが署名されると、ID証明書が提供されます。

```
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-----
MIIDgTCCAmgAwIBAgIIMA+aIxCTntMwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQDEw5j
YS51eGFtcGx1LmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMIIG
MRswGQYDVQDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMCOV4YW1wbGUg
SW5jMjQwFQYDVQDEw5jVUzETMBEGA1UECAwKQ2FsaWZvcj5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAFBgkqhkiG9w0BCQIMFzYXZwbi51eGFtcGx1LmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn0JGW698ddtL
LPCLXeYOJAXa1Egqa5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2FGIkDIhthD9gYncjk9xc8dJ1bnPKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRiOSf6R9d9CZyrT1CRMiJRaFR6r94y+83wPYpSJ7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi51eGFtcGx1LmNv
bTANBgkqhkiG9w0BAQsFAAOCQAQEAfQUchY4UjhjkySMJA7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqw1Y3fXC27TtweREwMbg8NsJrr80hsChYby8kwE
LnTkrN7dJB17u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9ru1DVRImd0KYE0x+HYav2INT2udcOG1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8ur2z5xpzxnEDUBoHOipG1gb1I6G1ARXW0+LwfB1
n1QD5b/RdQ0UblCpfKnpDE/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
```

- 新しい証明書の有効期限を確認します。

```
<#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更新

PKCS12ファイルを使用して登録されたトラストポイントの証明書を更新することはできません。新しい証明書をインストールするには、新しいトラストポイントを作成する必要があります。

- 特定の名前でトラストポイントを作成します。

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

- (オプション) 証明書失効チェックメソッドを、証明書失効リスト(CRL)またはオンライン証明書ステータスプロトコル(OCSP)を使用して設定します。デフォルトでは、証明書失効チェックは無効になっています。

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

- PKCS12ファイルから新しい証明書をインポートします。



注：PKCS12ファイルはBase64でエンコードする必要があります。ファイルをテキストエディタで開いたときに印刷可能な文字が表示される場合は、base64エンコードです。バイナリファイルをbase64エンコード形式に変換するには、opensslを使用できます。

```
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:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgaggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kI10310j7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABSAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQ1jHW7J/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.



注：新しいPKCS12ファイルに、古い証明書で使用されたものと同じキーペアのID証明書が含まれている場合、新しいトラストポイントは古いキーペアの名前を参照します。以下に例を挙げます。

```
<#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

- インストールされた証明書を確認します。

<#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
```

前の例では、PKCS12にID証明書とCA証明書が含まれていたため、インポート後に、証明書とCA証明書の2つのエントリが表示されます。それ以外の場合は、証明書エントリのみが存在します。

- (オプション) トラストポイントを認証します。

PKCS12にCA証明書が含まれておらず、CA証明書がPEM形式で個別に取得されている場合は、手動でインストールできません。

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+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
```

- 古いトラストポイントの代わりに新しいトラストポイントを使用するようにASAを再設定します。

以下に例を挙げます。

```
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
```

 注：トラストポイントはさまざまな設定要素で使用できます。古いトラストポイントが使用されている設定を確認します。

関連情報

ASAでの時刻設定の設定方法

ASAで時刻と日付を正しく設定するために必要な手順については、このリファレンスを参照してください。[CLIブック1: Cisco Secure Firewall ASAシリーズ一般操作CLIコンフィギュレーションガイド9.18](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。