

# ASA の設定 : SSL デジタル証明書のインストールと更新

## 内容

---

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[CSR の生成](#)

[1. ASDM による設定](#)

[2. ASACLI を使用した設定](#)

[3. OpenSSL を使用した CSR の生成](#)

[CA での SSL 証明書の生成](#)

[GoDaddy CA での SSL 証明書生成の例](#)

[ASA での SSL 証明書のインストール](#)

[1.1 ASDM を使用した PEM 形式でのアイデンティティ証明書のインストール](#)

[1.2. CLI を使用した PEM 証明書のインストール](#)

[2.1 ASDM を使用した PKCS12 証明書のインストール](#)

[2.2 CLI を使用した PKCS12 証明書のインストール](#)

[確認](#)

[ASDM を使用してインストールされた証明書の表示](#)

[CLI を使用してインストールされた証明書の表示](#)

[Web ブラウザによる WebVPN 用にインストールされた証明書の確認](#)

[ASA での SSL 証明書の更新](#)

[よく寄せられる質問 \(FAQ\)](#)

[1. アイデンティティ証明書のある ASA から別の ASA に転送する最善の方法は何ですか。](#)

[2. VPN ロード バランシング ASA で使用する SSL 証明書を生成するにはどうすればよいですか](#)

[3. 証明書を ASA フェールオーバー ペアのプライマリ ASA からセカンダリ ASA にコピーする必要がありますか。](#)

[4. ECDSA キーが使用されている場合、SSL 証明書の生成プロセスは異なりますか。](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[一般的な問題](#)

[付録](#)

[付録 A : ECDSA または RSA](#)

[付録 B : OpenSSL を使用して、アイデンティティ証明書、CA 証明書、および秘密キーから PKCS12 証明書を生成する](#)

[関連情報](#)

---

# はじめに

このドキュメントでは、クライアントレス SSLVPN および AnyConnect 接続に使用する、信頼できるサードパーティの SSL デジタル証明書を ASA にインストールする方法について説明します。

## 背景説明

この例では、GoDaddy 証明書が使用されます。各ステップには、Adaptive Security Device Manager ( ASDM ) の手順と、同等の CLI が含まれています。

## 前提条件

### 要件

このドキュメントでは、証明書を登録するために信頼できる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、Baltimore、Cisco、Entrust、Geotrust、G、Microsoft、RSA、Thawte、VeriSign などがありますが、他にも存在します。

開始する前に、ASA 上のクロック時間、日付、およびタイムゾーンが正しいことを確認してください。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。『[Cisco ASA シリーズ CLI コンフィギュレーション ガイド \( 一般的な操作 \)、9.1](#)』では、[ASA で時刻と日付を正しく設定するために実行する手順について詳しく説明しています。](#)

### 使用するコンポーネント

このドキュメントでは、ソフトウェア バージョン 9.4.1 および ASDM バージョン 7.4(1) が稼働する ASA 5500-X を使用しています。

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。

## 設定

SSL プロトコルは、クライアントがサーバ認証を実行するために、SSL サーバがクライアントにサーバ証明書を提供することを義務付けています。ユーザが不正なサーバからの証明書を信頼するようにブラウザを誤って設定する可能性があるため、自己署名証明書を使用することは推奨されません。また、ユーザがセキュリティ ゲートウェイに接続するときにセキュリティ警告に回答する必要があるという不便さもあります。この目的のために、信頼できるサードパーティの CA を使用して ASA に SSL 証明書を発行することをお勧めします。

ASA でのサードパーティ証明書のライフサイクルは、基本的に次の手順で行われます。



## CSR の生成


CSR の生成は、x.509 デジタル証明書のライフサイクルの最初のステップです。

プライベート/パブリック Rivest-Shamir-Adleman (RSA) または楕円曲線デジタル署名アルゴリズム (ECDSA) のキーペアが生成されると ([付録 A で、RSA と ECDSA の使用の違いを詳しく説明します](#))、[証明書署名要求 \(CSR\)](#) が作成されます。

CSR は、要求元のホストの公開キーとアイデンティティ情報を含む PKCS10 形式のメッセージです。[PKI のデータ形式](#) ASA および Cisco IOS に適用されるさまざまな証明書形式について説明します。<sup>®</sup>を参照。

### 注：

1. 必要なキーペアのサイズについて、CA に確認します。CA/ブラウザ フォーラムでは、メンバー CA によって生成されたすべての証明書の最小サイズが 2048 ビットであることが義務付けられています。
2. ASA は現在、SSL サーバ認証に 4096 ビット キー (Cisco Bug ID [CSCut53512](#)) をサポートしていません。ただし、IKEv2 は、ASA 5580、5585、および 5500-X プラットフォームでの 4096 ビット サーバ証明書の使用のみサポートしています。
3. 「信頼できない証明書 (Untrusted Certificate)」の警告が出されないようにし、厳密な

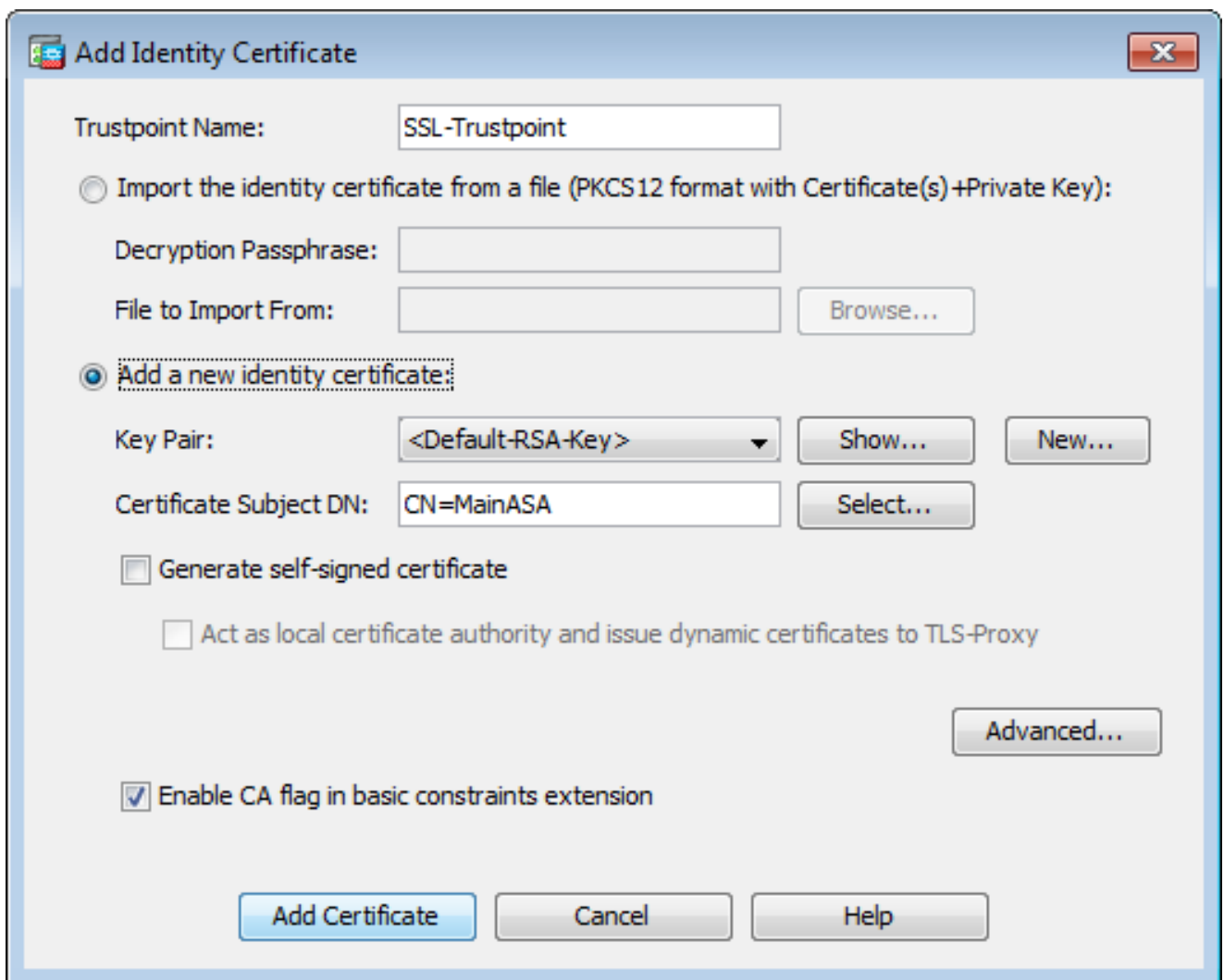
 証明書のチェックに合格するためには、CSR の FQDN フィールドの ASA の DNS 名を使用します。

CSR を生成する方法は 3 つあります。

- ASDM の設定
- ASA CLI による ASA の設定
- OpenSSL を使用した CSR の生成

## 1. ASDM による設定

1. に移動 Configuration > Remote Access VPN > Certificate Management し、 を選択し Identity Certificates ます。
2. をクリックします。Add



3. [トラストポイント名 ( Trustpoint Name ) ] 入力フィールドでトラストポイント名を定義します。
4. [Add a new identity certificate ラジオ] ボタンをクリックします。
5. Key Pair では、 をクリックします New。


The screenshot shows a dialog box titled "Add Key Pair". It has a close button (X) in the top right corner. The "Key Type" section has two radio buttons: "RSA" (selected) and "ECDSA". The "Name" section has two radio buttons: "Use default key pair name" and "Enter new key pair name:" (selected). The text "SSL-Keypair" is entered in the adjacent text box. The "Size" section has a dropdown menu showing "2048". The "Usage" section has two radio buttons: "General purpose" (selected) and "Special". At the bottom, there are three buttons: "Generate Now" (highlighted in blue), "Cancel", and "Help".

6. [キータイプ ( Key Type ) ] に RSA または ECDSA を選択します。 ( これらの違いについては、[「付録 A」](#) を参照してください )。
7. [Enter new key pair name ラジオ] ボタンをクリックします。認識できるように、キーペアの名前を特定します。
8. を選択します Key Size。RSA を使用して選択 General Purpose for Usage 。
9. をクリックします。Generate Now キーペアが作成されます。
10. Certificate Subject DN を定義するには、 をクリックし Select、次の表に示す属性を設定します。

Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

これらの値を設定するには、[属性 ( Attribute ) ] ドロップダウンリストから値を選択し、値を入力して [追加 ( Add ) ] をクリックします。

Attribute	Value
Common Name (CN)	vpn.remoteasa.com
Company Name (O)	Company Inc
Country (C)	US
State (St)	California
Location (L)	San Jose

 注：一部のサードパーティベンダーでは、アイデンティティ証明書を発行する前に、特定の属性を追加する必要があります。必要な属性が明確でない場合は、ベンダーに詳細を問い合せてください。

- 適切な値を追加したら、をクリックしますOK。Add Identity Certificateダイアログボックスが表示され、証明書が表示されますSubject DN field populated.
- [Advanced] をクリックします。

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

Certificate Parameters Enrollment Mode SCEP Challenge Password

FQDN: vpn.remoteasa.com

E-mail:

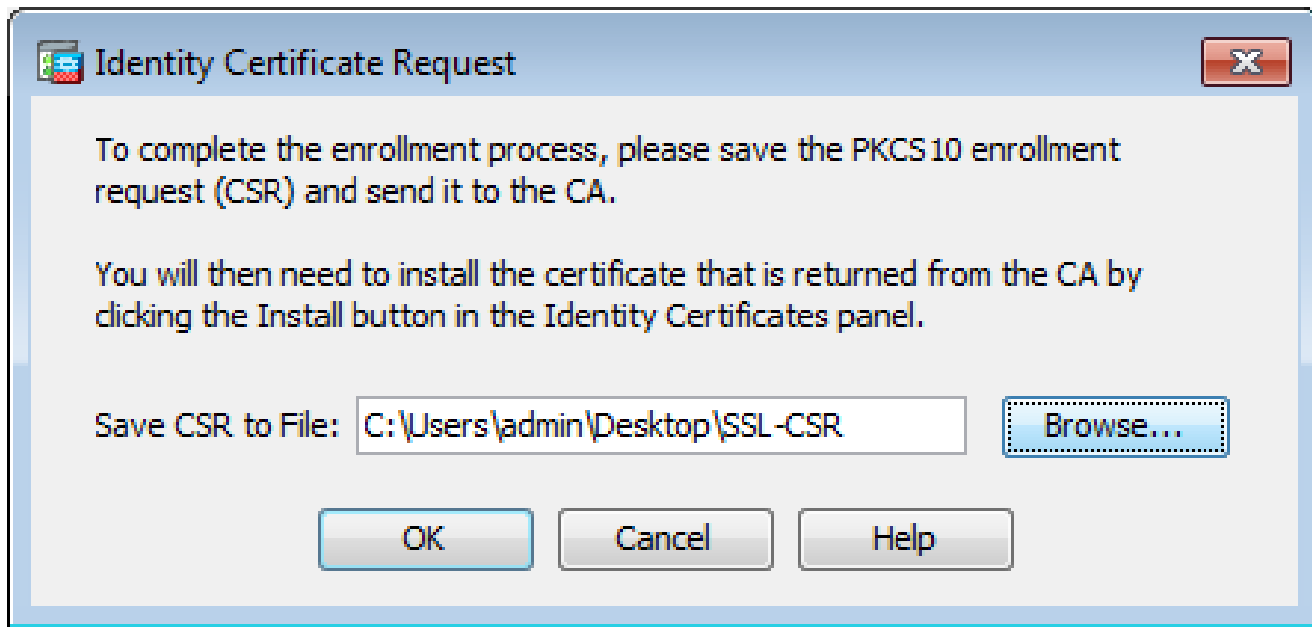
IP Address:

Include serial number of the device


- ファイQDNールドに、インターネットからデバイスにアクセスするために使用されるFQDNを

入力します。をクリックします。OK

14. [基本制約の拡張でCAフラグを有効にする ( Enable CA flag in basic constraints extension ) ] オプションをオンのままにします。デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。オプションをオフにすることで、この要件をバイパスできます。
15. をクリックしOK、次にAdd Certificate. 「A prompt displayed to save the CSR to a file on the local machine.」 をクリックします。



16. をクリックしBrowse、CSRを保存する場所を選択し、.txt拡張子を付けてファイルを保存します。

 注：.txt 拡張子を付けてファイルを保存すると、テキストエディタ (メモ帳など) を使用して PKCS#10 要求を開き、表示することができます。

## 2. ASA CLI による ASA の設定

ASDM では、CSR が生成された時点、または CA 証明書がインストールされた時点でトラストポイントが自動的に作成されます。CLI では、トラストポイントを手動で作成する必要があります。

```
<#root>
```

```
! Generates 2048 bit RSA key pair with label SSL-Keypair.
```

```
MainASA(config)#
```

```
crypto key generate rsa label SSL-Keypair modulus 2048
```

```
INFO: The name for the keys are: SSL-Keypair  
Keypair generation process begin. Please wait...
```

! Define trustpoint with attributes to be used on the SSL certificate

```
MainASA(config)#
crypto ca trustpoint SSL-Trustpoint
MainASA(config-ca-trustpoint)#
enrollment terminal
MainASA(config-ca-trustpoint)#
fqdn (remoteasavpn.url)
MainASA(config-ca-trustpoint)#
subject-name CN=(asa.remotevpn.url),O=Company Inc,C=US,
St=California,L=San Jose
MainASA(config-ca-trustpoint)#
keypair SSL-Keypair
MainASA(config-ca-trustpoint)#
exit
```

! Initiates certificate signing request. This is the request to be submitted via Web or Email to the third party vendor.

```
MainASA(config)#
crypto ca enroll SSL-Trustpoint
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate is 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 is: subject-name CN=

(remoteasavpn.url)

,  
O=Company Inc,C=US,St=California,L=San Jose

% The fully-qualified domain name in the certificate will be:

(remoteasavpn.url)

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

no

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

yes



Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAFYCAQAwYkxETAPBgNVBACTCFNhbiBkb3NlMRMwEQYDVQIQIEwpDYWxp
Zm9ybm1hMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBjbMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9kt1K
uR3Q4TmkysuRMqJNrb9KXpvA6H200PuBfQvSF4rVnSwK0mu3c8nweEvYcdVwV6Bz
BhjXeovTVi17F1NTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv60i8ylhco9Fz7bWvRWvt03NDDbyo1C9b/VgXMuBitcc
rzfUbVnm7VZD0f4jr9EXgUwXxcQidWEAB1FrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytI0zVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAaA/MD0GCSqGSIb3DQEJJDjEwMC4wDgYDVROPAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSKKEHEspu9oohjCYuNnp5qa91SPrZNEjTWw0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxYcny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoL1Cr9+hx74XsTHGBmI1s/9T5oAX26Ym+B21/i/DP5BktIUA
8GvIY1/ypj9K049fP5ap8a10qvLtYycCcfwrCt+0oj0rZ1YyJb3dFuMNRdAX37t
DuHN12EYNpYkjVklwI53/5w3
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]:


no

! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal to a text file to submit to the third party CA.

### 3. OpenSSL を使用した CSR の生成

OpenSSLでは、`OpenSSL config`ファイルを使用して、CSR生成で使用される属性を取得します。このプロセスにより、CSR と秘密キーが生成されます。

---

 **注意**：生成された秘密キーが他のユーザーと共有されていないことを確認します。これは、証明書の整合性が損なわれる可能性があるためです。

---

1. このプロセスが実行されているシステムに OpenSSL がインストールされていることを確認します。Mac OSX および GNU/Linux ユーザーの場合、これはデフォルトでインストールされます。
2. 機能ディレクトリに切り替えます。

Windowsの場合：デフォルトでは、ユーティリティはでインストールされC:\Openssl\binます。この場所でコマンドプロンプトを開きます。

Mac OSX/Linux の場合：CSR を作成するために必要なディレクトリで、ターミナルウィンドウを開きます。

3. テキストエディタを使用して、OpenSSL 構成ファイルを指定された属性で作成します。完了したら、前のステップで説明した場所にファイルをopenssl.cnfとして保存します(バージョン0.9.8h以降の場合、ファイルはopenssl.cfg)。

<#root>

```
[req]
default_bits = 2048
default_keyfile = privatekey.key
distinguished_name = req_distinguished_name
req_extensions = req_ext

[req_distinguished_name]
commonName = Common Name (eg, YOUR name)
commonName_default = (asa.remotevpn.url)

countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California

localityName = Locality Name (eg, city)
localityName_default = San Jose

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Company Inc
```

```
[req_ext]
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1 = *.remotearsa.com
```

4. 次のコマンドを使用して、CSR と秘密キーを生成します。

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
<#root>
```

```
# Sample CSR Generation:
```

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
Generate a 2048 bit RSA private key
```

```
.....+++
.....+++
writing new private key to 'privatekey.key'
-----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

If you enter '.', the field will be left blank.

-----  
Common Name (eg, YOUR name) [(asa.remotevpn.url)]:  
Country Name (2 letter code) [US]:  
State or Province Name (full name) [California]:  
Locality Name (eg, city) [San Jose]:  
Organization Name (eg, company) [Company Inc]:

保存した CSR をサードパーティ ベンダーに送信します。証明書が発行されると、CA は ASA にインストールされるアイデンティティ証明書と CA 証明書を提供します。

## CA での SSL 証明書の生成

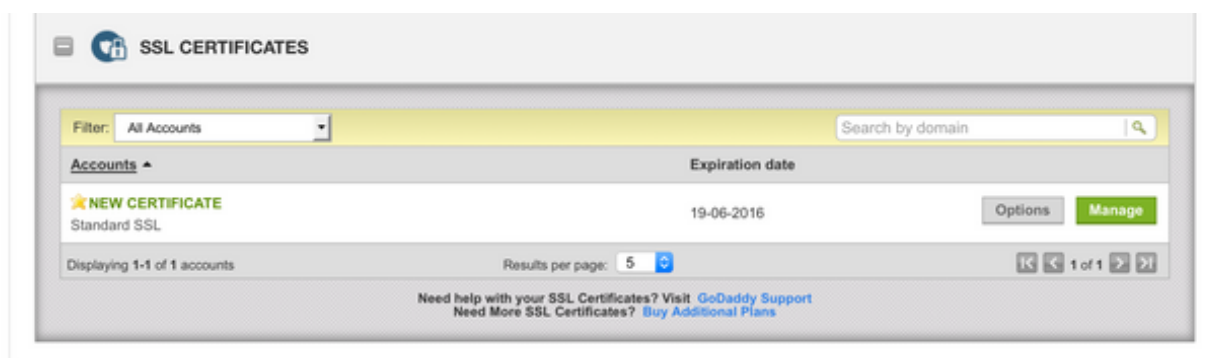
次の手順は、CA から署名された CSR を取得することです。CA は、新しく生成された PEM でエンコードされたアイデンティティ証明書、または PKCS12 証明書を CA 証明書バンドルとともに提供します。

CSR が ( OpenSSL または CA 自体のいずれかによって ) ASA の外部で生成される場合、秘密キーと CA 証明書を含む PEM でエンコードされたアイデンティティ証明書は個別のファイルとして使用できます。[付録 B には、これらの要素を 1 つの PKCS12 ファイル \(.p12 または .pfx 形式\) にまとめてバンドルする手順が記載されています。](#)

このドキュメントでは、ASA にアイデンティティ証明書を発行する例として、GoDaddy CA が使用されています。このプロセスは他の CA ベンダーでは異なります。続行する前に CA のドキュメントを注意深くお読みください。

### GoDaddy CA での SSL 証明書生成の例

SSL 証明書の購入および初期設定フェーズで、GoDaddy アカウントに移動し、SSL 証明書を表示します。新しい証明書が存在するはずです。クリックして Manage、次に進みます。



これにより、次の図に示すように、CSR を提供するためのページが表示されます。

CA は、入力された CSR に基づいて、証明書の発行先となるドメイン名を決定します。

これが ASA の FQDN と一致していることを確認します。

## Choose website

Select a domain hosted with us

Provide a certificate signing request (CSR)

Certificate Signing Request (CSR) [Learn more](#)

```
/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRRedAX37t
DuHNI2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):

**vpn.remoteasa.com**

## Domain ownership

We'll send an email with a unique code to your address on file. Follow its instructions to verify you have website or DNS control over the selected domain. [More info](#)

### AND

We can send domain ownership instructional emails to one or both of the following:


- Contacts listed in the domain's public WHOIS database record
- Email addresses: admin@[domain], administrator@[domain], hostmaster@[domain], postmaster@[domain], and webmaster@[domain]

[Hide advanced options](#)

Signature Algorithm [Learn more](#)

GoDaddy SHA-2

I agree to the terms and conditions of the [Subscriber Agreement](#).

 注：GoDaddy および他のほとんどの CA は、デフォルトの証明書の署名アルゴリズムとして SHA-2 または SHA256 を使用します。ASA は、8.2(5) [8.3 より前のリリース] および 8.4(1) [8.3 より後のリリース] 以降 ( Cisco Bug ID [CSCti30937](#) ) の SHA-2 署名アルゴリズムをサポートします。8.2(5) または 8.4(1) より古いバージョンが使用されている場合は、SHA-1 署名アルゴリズムを選択します。

要求が送信されると、GoDaddy は証明書を発行する前に要求を検証します。

証明書要求が検証されると、GoDaddy はそのアカウントに証明書を発行します。

その後、ASA にインストールするために証明書をダウンロードできます。ページをクリックして Download、次に進みます。

The screenshot shows the GoDaddy SSL Certificate Management page for the domain `vpn.remoteasa.com`. The page has a green header with navigation links: Certificates, Repository, Help, and Report EV Abuse. Below the header, the domain name and "Standard SSL Certificate" are displayed. The main content area is divided into two sections: "Certificate Management Options" and "Certificate Details".

**Certificate Management Options:** Three buttons are visible: "Download" (with a download icon), "Revoke" (with a revoke icon), and "Manage" (with a gear icon).

**Certificate Details:** A table lists the following information:

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

**Display your SSL Certificate security seal:** This section allows users to customize their security seal. It includes a "Color" dropdown menu set to "Light" and a "Language" dropdown menu set to "English". Below these is a "Preview" section showing a sample seal with the text "GO DADDY VERIFIED & SECURED VERIFY SECURITY". At the bottom, there is a "Code" section with a text area containing the following JavaScript code:

```
<script id="siteSeal"><script
type="text/javascript"
src="http://seal.godaddy.com
/getSeal?sealID=bpFzbxp4KmsyEfxwkdP4Ztd
&sealID=bpFzbxp4KmsyEfxwkdP4Ztd"
></script>
```

A "Ctrl+C to copy" instruction is provided below the code.

Server Typeとしてを選択しOther、証明書zipバンドルをダウンロードします。

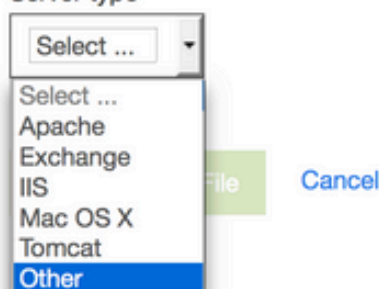
# vpn.remoteasa.com > Download Certificate

Standard SSL Certificate

To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers.

First time installing a certificate? [View Installation Instructions for the selected server.](#)

Server type




.zip ファイルには、アイデンティティ証明書と GoDaddy CA 証明書チェーンバンドルが 2 つの別個の .crt ファイルとして含まれています。SSL 証明書のインストールに進み、これらの証明書を ASA にインストールします。

## ASA での SSL 証明書のインストール

SSL 証明書は、ASDM または CLI を使用して ASA に次の 2 つの方法でインストールできます。

1. PEM 形式で CA およびアイデンティティ証明書を個別にインポートします。
2. または、PKCS12 ファイル ( CLI の場合は base64 エンコード ) をインポートします。このファイルにアイデンティティ証明書、CA 証明書、および秘密キーがバンドルされています。

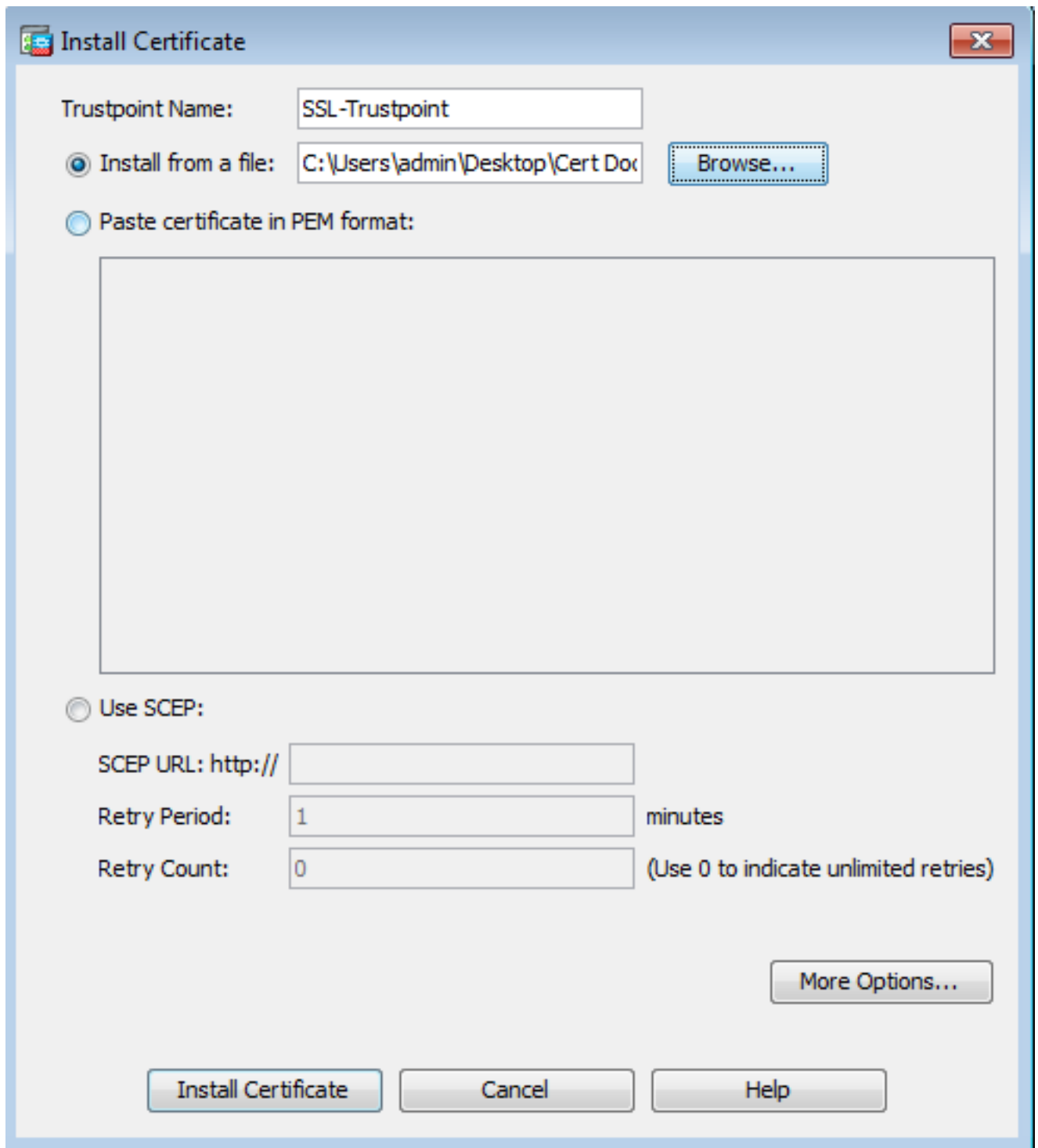
 注 : CA が CA 証明書チェーンを提供している場合は、CSR の生成に使用されたトラストポイントの階層に、即時の中間 CA 証明書のみをインストールします。ルート CA 証明書およびその他の中間 CA 証明書は、新しいトラストポイントにインストールできます。

### 1.1 ASDM を使用した PEM 形式でのアイデンティティ証明書のインストール

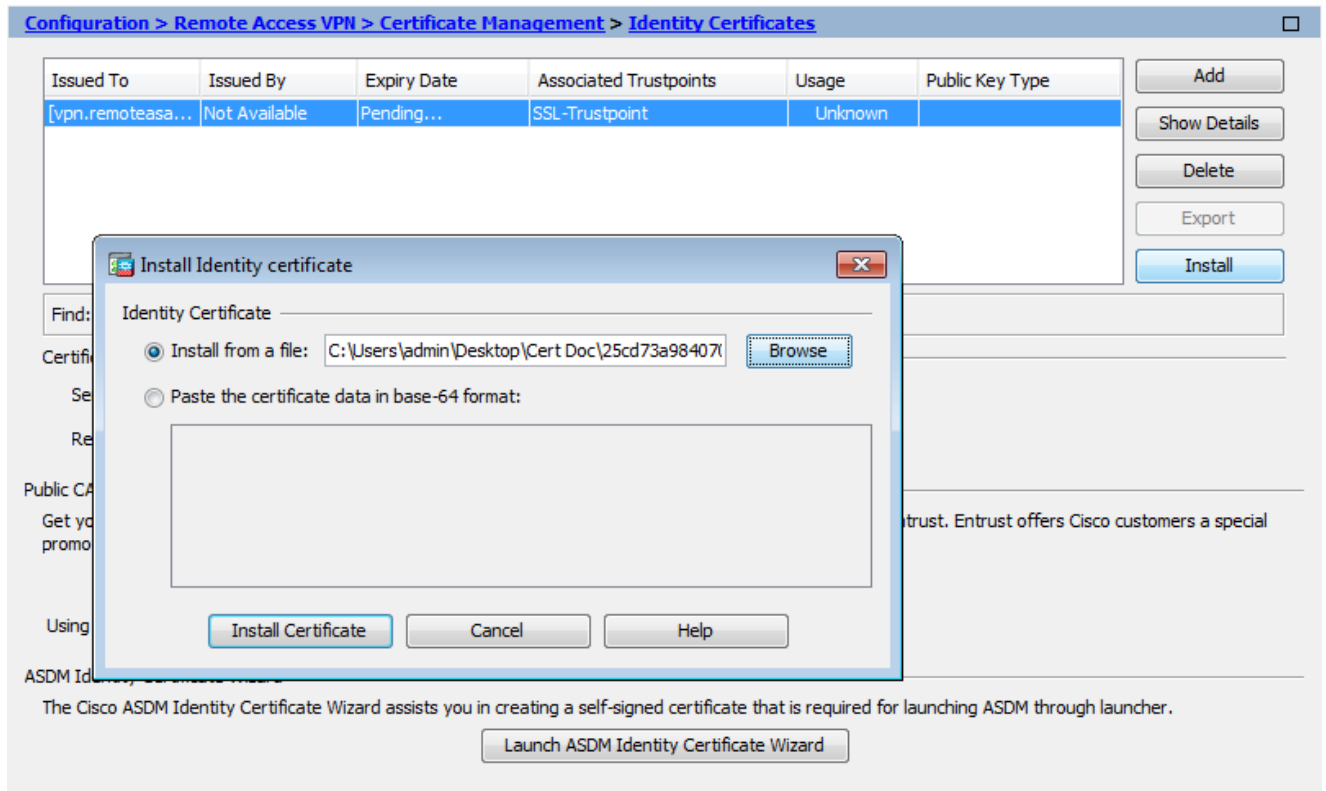
このインストール手順では、CA が PEM でエンコードされた ( pem、.cer、.crt ) アイデンティティ証明書と CA 証明書バンドルを提供していることを前提としています。

1. に移動し **Configuration > Remote Access VPN > Certificate Management**、CA Certificates を選択します。
2. テキスト エディタで PEM でエンコードされた証明書を開き、サードパーティ ベンダーに

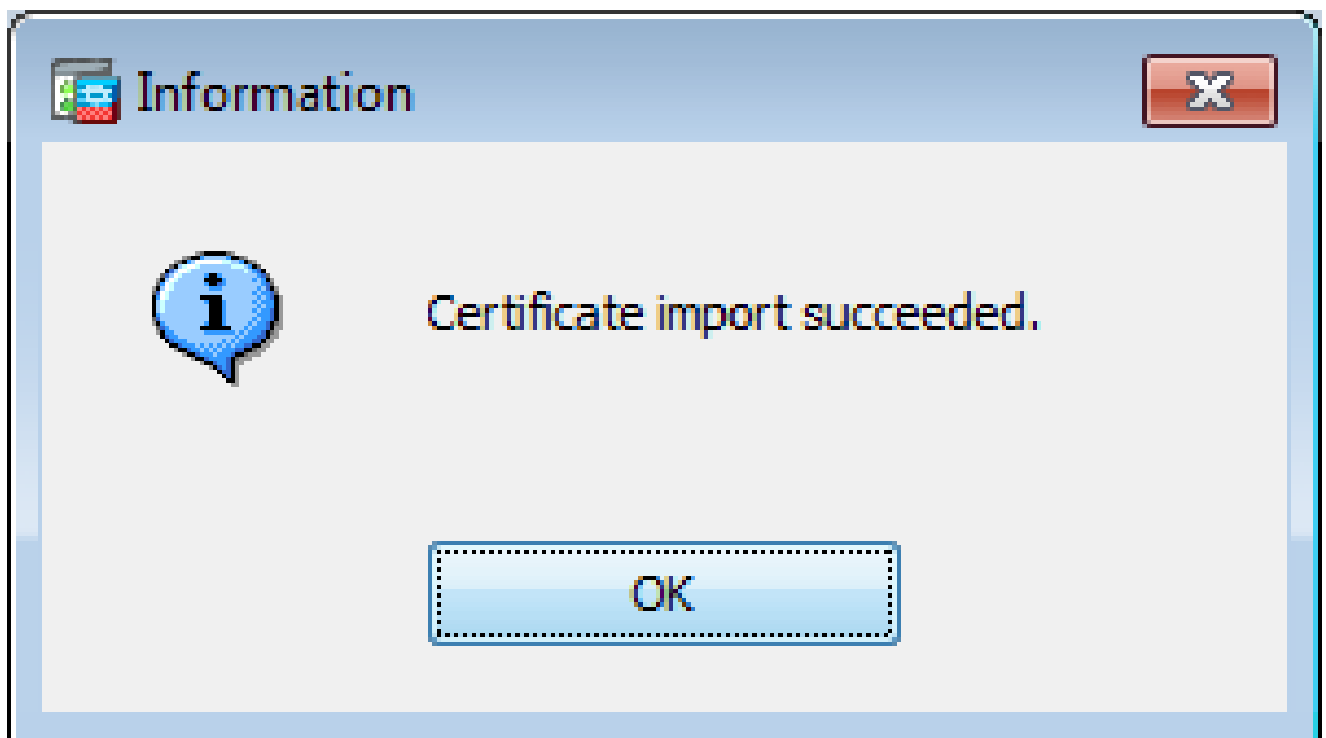
よって提供された base64 CA 証明書をコピーしてテキスト フィールドに貼り付けます。



3. Install Certificate をクリックします。
4. に移動し Configuration > Remote Access VPN > Certificate Management、Identity Certificatesを選択します。
5. 以前に作成したアイデンティティ証明書を選択します。をクリックします。Install
6. オプションボタンをクリックして、PEMでエンコードされたID証明書を選択するか Install from a file、PEMでエンコードされた証明書をテキストエディタで開き、サードパーティベンダーから提供されたBase64のID証明書をテキストフィールドにコピーアンドペーストします。



7. をクリックします。Add Certificate



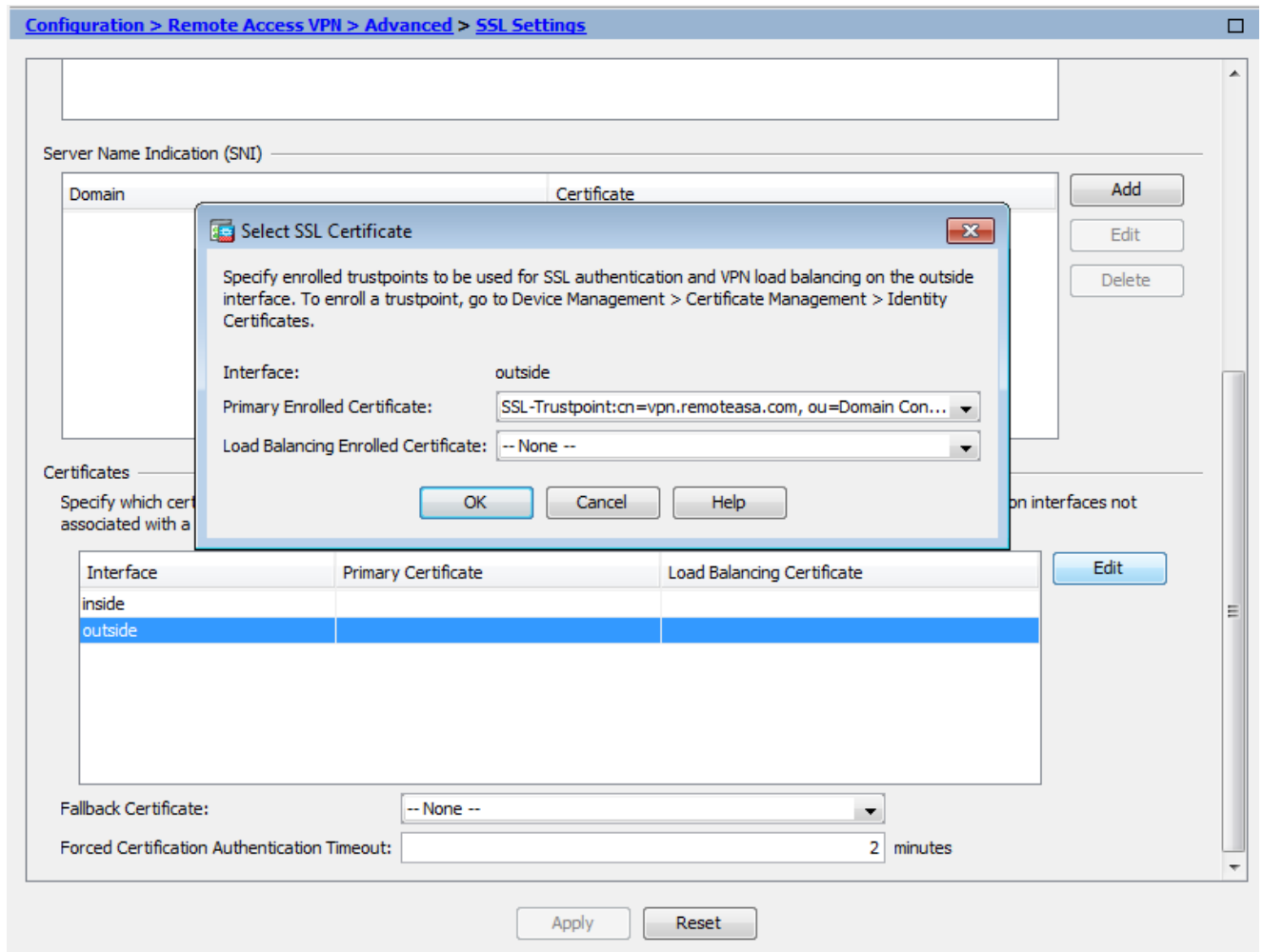
8. に移動します Configuration > Remote Access VPN > Advanced > SSL Settings。

9. [証明書 (Certificates)] で、WebVPN セッションの終端に使用されるインターフェイスを選択します。この例では、外部インターフェイスが使用されています。

10. をクリックします。Edit

11. [証明書 (Certificate)] ドロップダウンリストで、新しくインストールした証明書を選択します。





12. をクリックします。OK

13. をクリックします。Apply新しい証明書が、指定のインターフェイス上で終端するすべてのWebVPNセッションに使用されるようになります。

## 1.2. CLI を使用した PEM 証明書のインストール

```
<#root>
```

```
MainASA(config)#
```

```
crypto ca authenticate SSL-Trustpoint
```

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

```
-----BEGIN CERTIFICATE----- MIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVuzEh MB8GA1UECh
```

```
!!! - Installing Next-level SubCA in the PKI hierarchy
```

```
.
```

```
!!! - Create a separate trustpoint to install the next subCA certificate (if present)  
in the hierarchy leading up to the Root CA (including the Root CA certificate)
```

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

-----BEGIN CERTIFICATE-----

```
MIIEFTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTA1VT
MSEwHwYDVQQKEzhUaGUgR28gRGFkZHKgR3JvdXAsIE1uYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgZELMAkGA1UEBhMCVVMxEDA0BgNVBAGT
B0FyaXpvcjEzARBgNVBACTC1Njb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHKu
Y29tLCBjb29tLWYwYy4xMTAvBgNVBAsTKEdvIERhZGR5IENsYXNzIDIgQ2VydG1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBt0oLTbcJjHMgXBT4H
Tu70+k8vWTAi56sZvmvigaF88xZ1gD1Re+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gE1DtGfDIN8wBmIisiNaW02jBEYt90yHGC00PoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVE1BWEaRIGMLK1D1iPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0A1YnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMvxpRpRgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zA0BgNV
HQ8BAF8EBAMCAQYwHQYDVR00BBYEFdqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCKwJ6A1
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybdBGBGgNVHSAEPzA9
MDsGBFUDIAAwMzAxBggrBgEFBQcCARY1aHR0cHM6Ly9jZXJ0cy5nb2RlZGR5LmNv
bS5yZXBvc210b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XU0Ewf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVn0QowCcWg
0JekxS0TP7QYpgEGRJHj2kntFofzq3Ms3dhP8q0CkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPzfLXs4J1et01UIDyUGAZHHFIYSaRt4bNYC8nY7NmuHDK0
KHAN4v6mF56ED71XcLNa6R+gh10773z/aQvgSM03kwwIC1TErF0UZzdsyqUvMQg3
qm5vjLyb41ddJIGv15echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHCyQFHfjDCm
rw==
```

-----END CERTIFICATE-----

quit

```
INFO: Certificate has the following attributes:
Fingerprint:      81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes
```

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

```
% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n", where n is number thats incremented for every level in the PKI hierarchy) to import the CA certificates leading up to the Root CA certificate.

!!! - Importing identity certificate (import it in the first trustpoint that was created namely "SSL-Trustpoint")

```
MainASA(config)#
```

```
crypto ca import SSL-Trustpoint certificate
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If th

```
yes
```

```
% The fully-qualified domain name in the certificate will be:
```

```
(asa.remotevpn.url)
```

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

```
-----BEGIN CERTIFICATE-----
```

```
MIIFRjCCBC6gAwIBAgIIJc1zqYQHbGwUwDQYJKoZIhvcNAQELBQAwgQxGzAkJBgNV  
BAYTA1VTMRAwDgYDZDQIEwdBcm16b25hMRRMwEQYDQVQHEwPjY290dHNkYWx1MR0w  
GAYDVQQKExFhb0RlZGR5LmNvbSw5jLjEtMCsGA1UECxMkaHR0cDovL2N1cnRz  
LmdvZGFkZHZhY29tL3JlcnRzZXRvcnkMTMwMQYDQDEYpHbyBEYWRkeSBTZWN1  
cmUgQ2VydG1maWwNhdGUGQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN  
MTYwNzIyMTIwNDM4WjA/MSEwHwYDZDQLEXhEb21haW4gQ29udHJvbCBWYXpZGF0  
ZWQxGjAYBgNVBAMTEXzWbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF  
AAOCAQ8AMIIIBCgKAQEArrY2Fv2S2Uq5HdDh0aSzK5Eyok2tv2Rem8DofbTQ+4F9  
C9IXitWdLAo6a7dzyfB4S9hx1VZxOHHMGND6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW  
ITt5GzKdL93ibMxYmau+uwM30kBB8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP  
tta9FZW07c0MNVkiUL1v9WBcy4GK1xyvN9RtWebtVkm5/iOv0ReBTBFFxCJ1YQAG  
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L108cbmbi/u/vnmZ5Xhiqx  
<snip>
```

```
CCsGAQUBwIBFitodHRwOi8vY2VydG1maWwNhdGVzLmdvZGFkZHZhY29tL3JlcnRz  
aXRvcnkVMHYGCCsGAQUBwEBBGowaDAKBggrBgEFBQcwAYYYaHR0cDovL29jc3Au  
Z29kYWRkeS5jb20vMEAGCCsGAQUBzAChjRodHRwOi8vY2VydG1maWwNhdGVzLmdv  
ZGFkZHZhY29tL3JlcnRzZXRvcnkVZ2RpZzIuY3JOMB8GA1UdIwQYMBaAFEDCvSe0  
zDSDMKIz1/tss/COLIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3  
d3cudnBuLnJlbW90ZWZzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW  
BBT7en7YS3PH+s4z+wTR1pHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEA09H8TLN  
x2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVkra9azdrNUAN  
1hjBJ7kKQScLC4sZLONDqG1uTP5rbWR0yikF5wSzyMwd03kOR+vM8q6T57vRst5  
69vzBUUJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt10q  
xkGNys3GgYuCUy6yRP2cAUV11c2tYtaxoCL8yo72YUDDgZ3a4Py01EvC1F0aUtgv  
6QNEOYwmbJkyumdPUwko6wGOCOWLumzv5gHnhil68HYSZ/4XI1p3B9Y8yfg5pwb  
n7puhazH+xgQRdg==
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate successfully imported
```

```
! Apply the newly installed SSL certificate to the interface accepting SSL connections
```

```
MainASA(config)#
```

```
ssl trust-point SSL-Trustpoint outside
```

## 2.1 ASDM を使用した PKCS12 証明書のインストール

ワイルドカード証明書の場合や UC 証明書が生成された場合など、ASA 上で CSR が生成されない場合は、秘密キーとともにアイデンティティ証明書を個別のファイルとして、またはバンドルされた 1 つの PKCS12 ファイル (.p12 または pfx 形式) として受信します。このようなタイプの証明書をインストールするには、次の手順を実行します。

1. アイデンティティ証明書、CA 証明書、および秘密キーは、1 つの PKCS12 ファイルにバン

ドルします。 [付録 B では、OpenSSL でこれを実行する手順について説明します。](#)すでに CA によってバンドルされている場合は、次のステップに進みます。

2. 移動して Configuration > Remote Access VPN > Certificate Management、 Identity Certificates.
3. をクリックします。 Add
4. トラストポイント名を指定します。
5. オブ Import the identity certificate from a file ションボタンをクリックします。
6. PKCS12 ファイルの作成に使用するパスフレーズを入力します。PKCS12 ファイルを参照して選択します。証明書ファイルのパスフレーズを入力します。

**Add Identity Certificate**

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

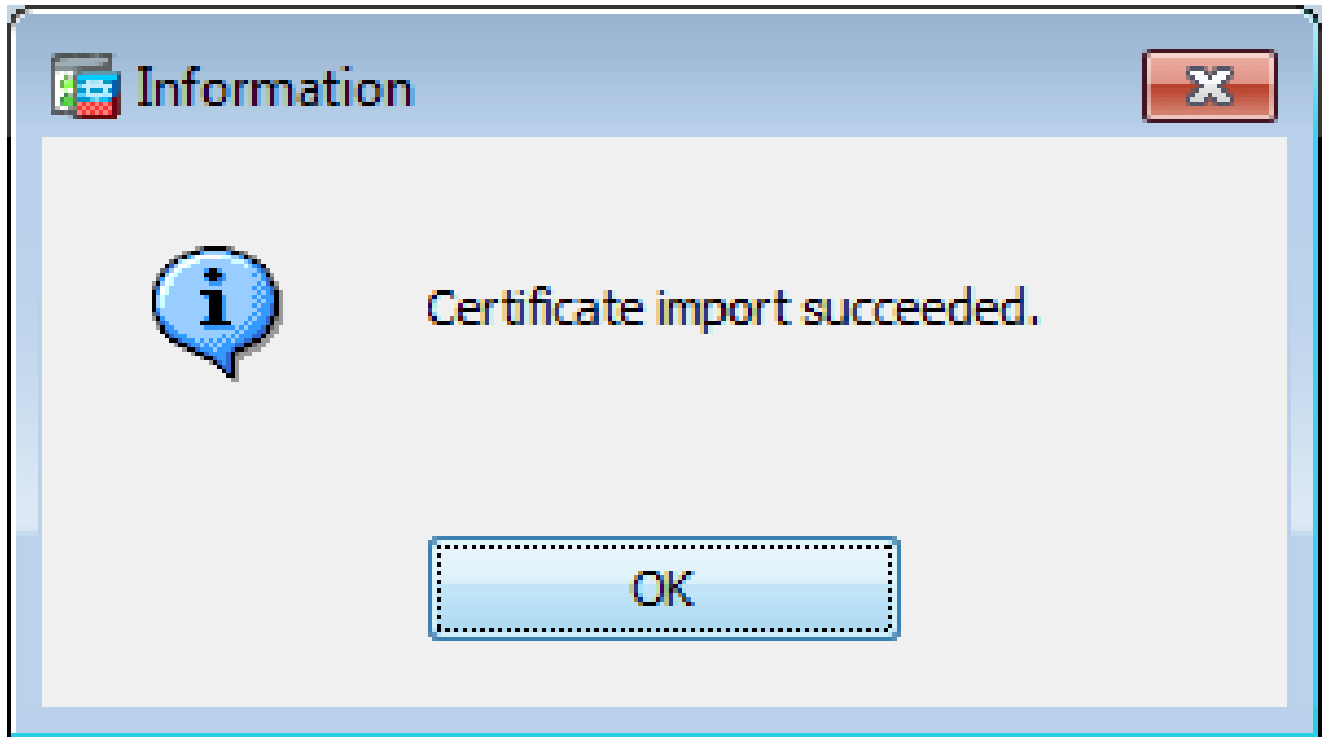
Certificate Subject DN:

Generate self-signed certificate

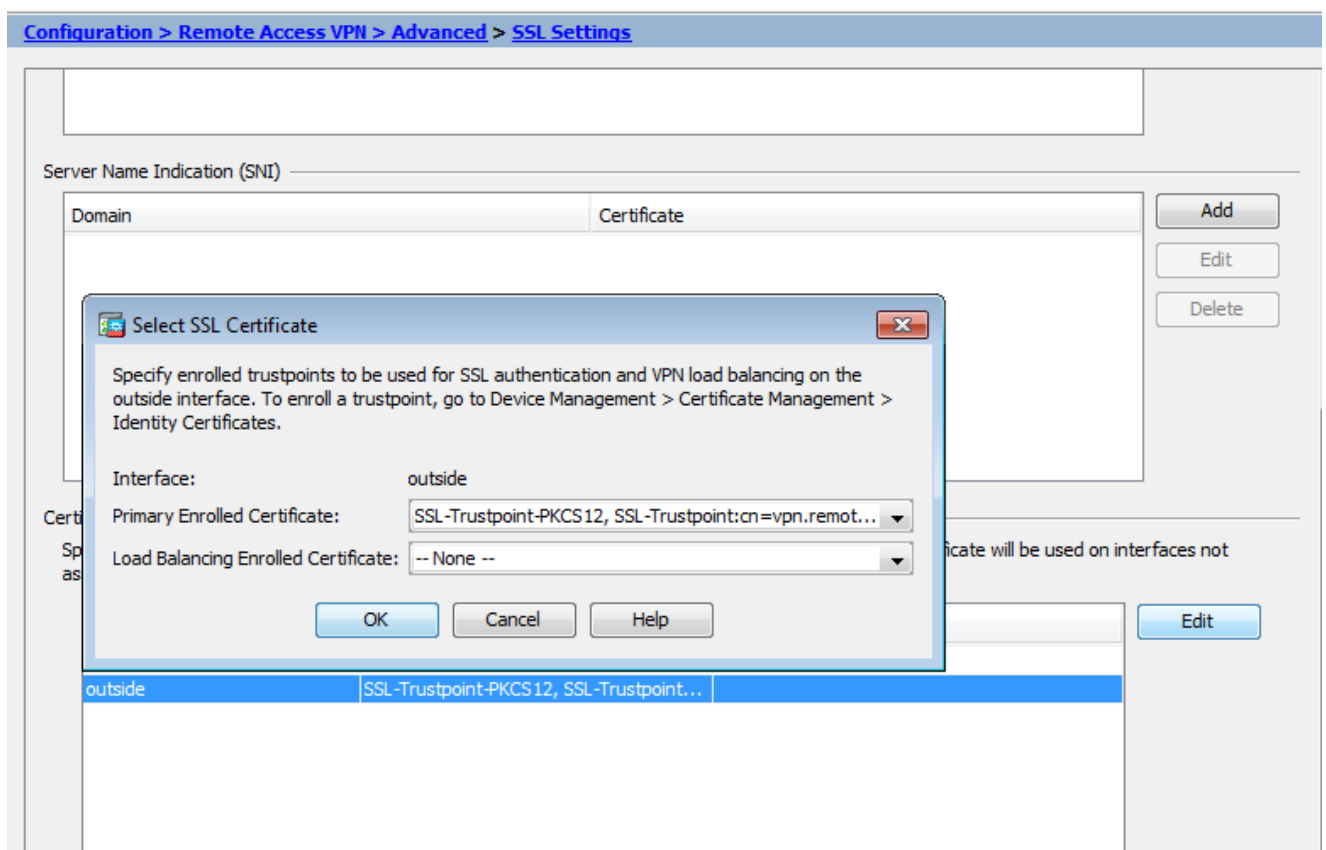
Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

7. [証明書の追加 ( Add Certificate ) ] をクリックします。



8. に移動し **Configuration > Remote Access VPN > Advanced**、 を選択します **SSL Settings**.
9. [証明書 ( Certificates ) ] で、WebVPN セッションの終端に使用されるインターフェイスを選択します。この例では、外部インターフェイスが使用されています。
10. をクリックします。 **Edit**
11. [証明書 ( Certificate ) ] ドロップダウン リストで、新しくインストールした証明書を選択します。



12. をクリックします。OK

13. をクリックします。Apply新しい証明書が、指定のインターフェイス上で終端するすべてのWebVPN セッションに使用されるようになります。

## 2.2 CLI を使用した PKCS12 証明書のインストール

```
<#root>
```

```
MainASA(config)#
```

```
crypto ca trustpoint SSL-Trustpoint-PKCS12
```

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

```
enrollment terminal
```

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

```
exit
```

```
MainASA(config)#
```

```
crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.

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

```
-----BEGIN PKCS12-----
```

```
MIISNwIBAzCCEfEGCSqGSIB3DQEHAaCCEeIEghHeMIIR2jCCEdYGCsQGSIB3DQEH  
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIB3DQEMAQMwDQQIW03D  
hDtI/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG  
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWi0S7npgaUq0eoqiJRK+Yc7  
LN0nbho6I5WfL56/JiceAM1XDLr/IqqLg2QAAPGdN+F5vANsHse2GsAATewBDLt7  
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCD1zRSuXcqypEV  
q5e3heio0751E8TDLWm03PMvWIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7  
kIQM8fHb4ga8BYfbgRmG6mkMm01STtbSv1vTa19WTmdQdTycCa+G5PkrryRsy3Ww1  
1kGFmHImmrrnNADF7Hmzbys1VohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJD  
mGDhhESH+s/WuFSV9Z9k1TXpJNZxpTASoWBQRrwm05v8ZwbjbVNJ7sVdbwpU16d+  
NNFGR7LTq08hpupeJnY9eJc2yYqAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3b13A  
xqxGi fanWpNLyG611NKuNjTgbjhnEYI2uZzU0qxn1Ka8zyXw+1zrKuJscDbkAPZ  
wKtW8K+p40zXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa  
16LMana+4QRgSetJhUOLtSmaQfRJGkha4JLq2t+JrCAPz2osAR1TsB0jQBNq6YNj  
OuB+gk2G18Q5N1n6K1fz0XBFZLWEDBLsaBR05ManE7wWt00+4awGYqVdmIF11kf  
XIRKAiQEr1pZ6BVPuvscNjXaaUHzufhYI2ZackasKBZ0T8/7YK3fnAaGoBCz4cHa  
o2EEQhq2aYb6YTv0+wtLEWGHZsbGZEM/u54XmsXAI7g28LGJYdfwi509KyV+Ac1V  
KzHqXZMM2BbUQCNCtF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg  
Z1PXiDbNr1k4e8L4gqumMKWg853PY+oY22rLDC7bu11CKtixIYBCvbn7dAYS14GQ  
16xXhNu3+iye0HgbUQCfTU/mBrAOZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM  
K7YinFLoHwTWbi3MsmqVv+Z4ttVwy7Xmi ko02nMynJMP6/CNV80MxMKdC2qm+c1j  
s4Q1KcAmFsQmNp/7SIP1wnv0c6JbUmC10520U/r8ftTzn8C7WL62W79cLK4H0r7J  
sNsZnOz0J0Z/xdZT+cLTCTtVevKJQOMK3vMsiOuy52FkuF3HnfrmbQDkbR7yZxELG  
RCELOEDdbp8VP0+IhN1yz1q7975SscdxFSL0TvjnHGFwd14ndoqN+bLhWbdPjQWV  
13W2NCI95tmHDLGgp3P001S+rjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS  
/ubyUagdzUKt1ecfb9hMLP65ZnQ93VIw/NJKbIm7b4P/1Zp/1FP5eq7LkQPAXE4/  
bQ4mHcnwrs+JGfkn19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgrvHqpQe  
B7odN10FLAhd01G5BsHExlUeNEsb40Q0pmKXidDB5B001bJsr748fZ6L/LGx8A13
```

```
<snip>
```

```
ijDqxyfQXY4zSyt1jSmWmtYA9hG5I79Sg7pnME1E9xq1D0oRGg8vgxlwiciKtLxp  
LL0ReDY31KRYv00vW0gf+tE71ST/3TKZvh0sQ/BE0V3kHnw1dejMFH+dvYAA9Y1E  
c80+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF41jNvUNV09VtVFR2FTyWpzZFY8A
```

GG5XPIA80WF6wKEPFHICn8scY+Vot8kXxG96hwt2Cm5NQ20nVzxUZQbpKsjs/2jC  
3HVF3UJFBsY9UxTLCXPYBSIG+VeqkI8hWZp6c1TfNDLY2ELDy1Qzp1mBg2FujZa  
YuE0avjCJzBzZUG2umtS5mHQnwPF+Xk0ujEyhGMauhGxHp4nghSzrUZrBeuL91UF  
2mbpsOcgZkzxMS/rjdNXjCmPF1oRBvKkZS1xHFrE/5ZopAhn4i7YtHQNrZ9U4RjQ  
xo9cUuaJ+LnmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P  
X87CXCPtYrPHF57eSo+tHDINCgfYXD6e/7r2ngfiCeUeNDZ4aV12XxvZDaU1BPP  
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdFG1ZIwdTe13CzKqXA5Pmpjt4q9  
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gz0bee2Wz+aRRwzSxu6tEWVZo1PEM  
v0AA7po3vPek1g0nLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU  
1w73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWmOK/op62C9/eqqMwZ8zoCMPt  
ENna7T+70s66SCbMmXCHwyh00tygNKZFFw/AATFyjqPMWPaxGuPN0rnB6uYcN0Hk  
1BU7tF143RNIzaQqEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS  
uhdFEpoDrJH1VmI2tik/iqYwaz+oDqXPHQXnJhw25h9ombR4qnd+FCfwFCGtPFON  
o3Qffz53C95n5jPHVMYr0xuDdpwnvzCQPdj6yQm564TwLAmiz7uD1pqJZJe5QxHD  
no1v+4MdGsfVtBq+ykFoVcaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49E1ndI  
L01DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjPHCwEYms4Wgt/vKKRFsuWJNZf  
efH1dw11tkd5dKwSvDocPT/7mSLtLJa94c6AfgxYy9z0+FTLDQwzXga7xC2krAN1  
yHxR2KHN5YeRL+KDzu+u6dYoKaz+YAgw1W6KbeavALSuH4EYqcvG8hUEhp/ySiSc  
RDhuygxEovIMGfES4FP5V521PyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ  
1ptWYyO8Bdr4Wnwt5xqsZgYR6mmGeAIin7bDunsF1uBHWF4dyK1z1tsdRNMqQ  
+W5q+QjVdrj1dwv/bMF0aqEjxeNwBRqjzccff3BxMnwVxtgqxFvRh+DZxiJoiBG+  
yx7x8np2AQ1r0METSSxbnZzfzKZKvBVMkIC6JsmT2WEVTQvofJ8em+nem0Wgti/  
hHSBzjE7RhAucnHuiFOCX0gvR1SDDqyCQbduc1QjXN0svA8Fqbea9WEH5khOPv3  
pbtsL4gsf12pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVvrdson11/qq+xW0d3tB4/  
zoH9LEMgTy9Ssz7myWrB9E00Z8BIjL1M8oMigEYrTD0c3KbyW1S9dd7QAxIU0BaX1  
8J8q10ydvTBzmqcjesFH4/1NHn5Vnf0ZnNpui4uHP0XBG+K2zJUJXm6dq1AHB1E  
KQFsFzPNNyave0Kk8JzQnLAPd70UU/Iksy0CGQozGBH+HSzVp1RDjrrbC342rkBj  
wnI+j+/1JdWbMhdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC  
FE5FZnMFvhM900LaiUZff8WWC0ferDMttLXb1nuxPF1+1Rk+LN1PLVptWgcxzfSr  
JXrGiWjxybBB9oC0rAcq8fGAtEs8WRxJyDH3Jjmn9i/G16J1mMcuF//LxAH2WQx8  
Ld/qS50M2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CwaKjwOMQ  
5tbbLM1nc7ALIj9LxZ97YiXSTyeM6oBxBfX6Rpk1kDv05m1BghSpVQiMcQ20RIkh  
UVVNBsh019S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXp0  
EqEFuatT11QvCRbcKs3xou4MAixcYUxKwEhbZA/6hd10XSBjwe7jKBV9M6w1iKab  
UfoJCGTaf3sY681qrMPrbt0eewf1C02Sd9Mn+V/jvni17mxYFFUpruRq3r1LeqP  
J5camfTtHwyL8N3Q/Zwp+zQeWziLA8a/iAVu/hYLR1bpF2WCK010tJqkvVmrLVLz  
maZZjbJe0ft5cP/1RxbK1S6Gd5dFEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Lj1  
kXwF+ivox0Q8a+Gg1bVTR0c7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi  
1+0io07Ked4BySwN1Yy9yaJtBTZSCstfP+ApLiDn7pSBvvXf1aHmeNbkPOZJ+c+t  
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGuWMS3NfS25XgcMuvnLqGVO  
RzcrZ1ZIG8G0oLYwOCuzoY0D/m901001ahePyA9tmVB7HRRbytLdaW7gYeikoCv  
7qtBqJFF17ntWJ3EpQHZUCVClbHIKqjNqRbDCY7so4A1IW7kSEUGWMIUDhprE8Ks  
NpvnPH2i9JrYrTeRoYUI0tL/7SATd2P0a21xz/zUwekeqd0bmVCsAgQNbB2XkrR3  
XS0B52o1+63e8KDqS2zL2TZd3daDFidH1B8QB26tfbf0Aca0bJH5/dWP8ddo8UYo  
Y3JqT10malxSjhaMhMqDZIqP49utW3Tcjg11YS4HEmcqtHud0ShaUysC6239j1Q  
K1FwrwXT1BC5vnq5IcOMqx5zyNbfXz28969cwoMCyU6+kRw0TyF6kF7EEv6XWca  
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI  
N34yeI/ORCLyeGs0EiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S  
/n/1ZVUHbUk71xKR2bWZgEC17fIe17w1rbjP3Wbk+Er0kfYcsNRHxeTDpKPsT9s  
u/UsyQJiyNARG4X3iyQ1sTce/06Ycyri6GcLHAu58B02nj4Cxo1Cp1ABZ2N79HtN  
/7Kh5L0pS9MwsDCHuUI8KFRtSEt7TB1tIU99FdB19L64s1/shYAHbccvVWU50WhT  
PdLoaErrX81Tof41IxBSzBI8grUC4KfG2sdPLJKu3HVTeQ8Lfl1bBLxfs8ZBS+Oc  
v8rH1Q012kY6LsFGLehj+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K  
HfSCCbLpKCyEay80dyWkHfgy1qXmb9ud0oM050aFJyqRONjnt6pcxBRy2A6AJR5S  
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ  
Ojcyt1r9qpWdzPnfK8EzizwKiAYtsiEh2pzPt6YUkpsRb6CXTkiZog+Klsv2m3b8  
OHyZ9a8z81/gnxrZ11s5SCTf0SU70pHWh8VAYKVHhk+MwgQrOm/2ocV32dkRBLMy  
2R6P4WfHyI/+9de1x3PtIu0iv2knpXhv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh  
MAKGBSs0AwIaBQAeffTRETzpiSHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd  
qJSzcwh0hgICBAA=  
-----END PKCS12-----

quit

```
INFO: Import PKCS12 operation completed successfully
```

```
!!! Link the SSL trustpoint to the appropriate interface  
MainASA(config)#
```

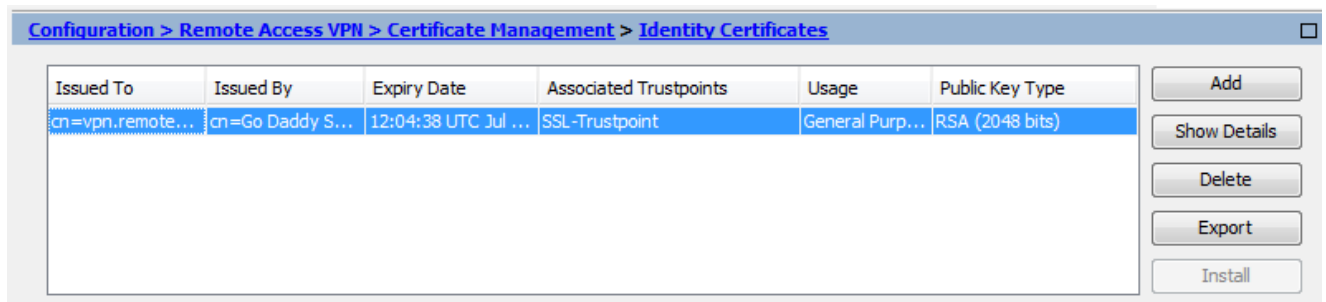
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

## 確認

サードパーティベンダーの証明書のインストールが成功し、SSLVPN 接続に使用されていることを確認するには、次の手順に従います。

### ASDM を使用してインストールされた証明書の表示

1. 移動し Configuration > Remote Access VPN > Certificate Management, て選択 Identity Certificates.
2. サードパーティベンダーにより発行されたアイデンティティ証明書が表示されます。



### CLI を使用してインストールされた証明書の表示

```
<#root>
```

```
MainASA(config)#
```

```
show crypto ca certificate
```

#### Certificate

```
Status: Available  
Certificate Serial Number: 25cd73a984070605  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: SHA256 with RSA Encryption  
Issuer Name:  
  cn=Go Daddy Secure Certificate Authority - G2  
  ou=http://certs.godaddy.com/repository/  
  o=GoDaddy.com\, Inc.  
  l=Scottsdale  
  st=Arizona  
  c=US  
Subject Name:
```



cn=(asa.remotevpn.url)  
ou=Domain Control Validated  
OCSP AIA:  
URL: http://ocsp.godaddy.com/  
CRL Distribution Points:  
[1] http://crl.godaddy.com/gdig2s1-96.crl  
Validity Date:  
start date: 12:04:38 UTC Jul 22 2015  
end date: 12:04:38 UTC Jul 22 2016  
Associated Trustpoints:

#### SSL-Trustpoint

#### CA Certificate

Status: Available  
Certificate Serial Number: 07  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: SHA256 with RSA Encryption  
Issuer Name:  
cn=Go Daddy Root Certificate Authority - G2  
o=GoDaddy.com\, Inc.  
l=Scottsdale  
st=Arizona  
c=US  
Subject Name:  
cn=Go Daddy Secure Certificate Authority - G2  
ou=http://certs.godaddy.com/repository/  
o=GoDaddy.com\, Inc.  
l=Scottsdale  
st=Arizona  
c=US  
OCSP AIA:  
URL: http://ocsp.godaddy.com/  
CRL Distribution Points:  
[1] http://crl.godaddy.com/gdroot-g2.crl  
Validity Date:  
start date: 07:00:00 UTC May 3 2011  
end date: 07:00:00 UTC May 3 2031  
Associated Trustpoints:

#### SSL-Trustpoint

#### CA Certificate

Status: Available  
Certificate Serial Number: 1be715  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: SHA256 with RSA Encryption  
Issuer Name:  
ou=Go Daddy Class 2 Certification Authority  
o=The Go Daddy Group\, Inc.  
c=US  
Subject Name:  
cn=Go Daddy Root Certificate Authority - G2  
o=GoDaddy.com\, Inc.

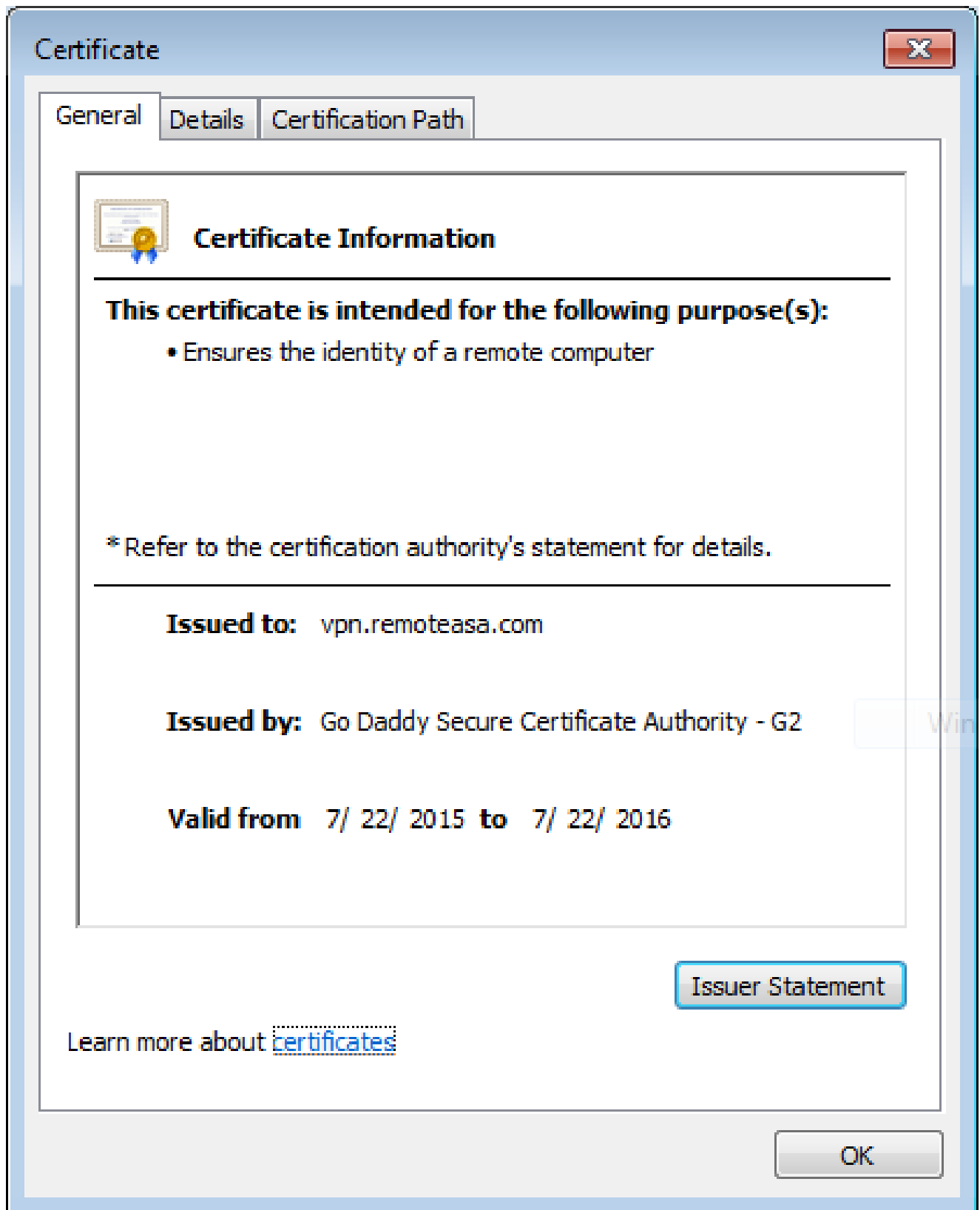
```
l=Scottsdale
st=Arizona
c=US
OCSP AIA:
  URL: http://ocsp.godaddy.com/
CRL Distribution Points:
  [1] http://crl.godaddy.com/gdroot.crl
Validity Date:
  start date: 07:00:00 UTC Jan 1 2014
  end   date: 07:00:00 UTC May 30 2031
Associated Trustpoints:
SSL-Trustpoint-1
```

...(and the rest of the Sub CA certificates till the Root CA)

## Web ブラウザによる WebVPN 用にインストールされた証明書の確認

WebVPN が新しい証明書を使用していることを確認します。

1. Web ブラウザを介して WebVPN インターフェイスに接続します。証明書を要求するために使用した FQDN とともに `https://` を使用します (たとえば、[https://\(vpn.remotearsa.com\)](https://vpn.remotearsa.com) のようにします)。
2. WebVPN login ページの右下隅に表示されているロック アイコンをダブルクリックします。インストールされている証明書の情報が表示されます。
3. 内容を確認し、サードパーティベンダーが発行した証明書に合致することを確認します。

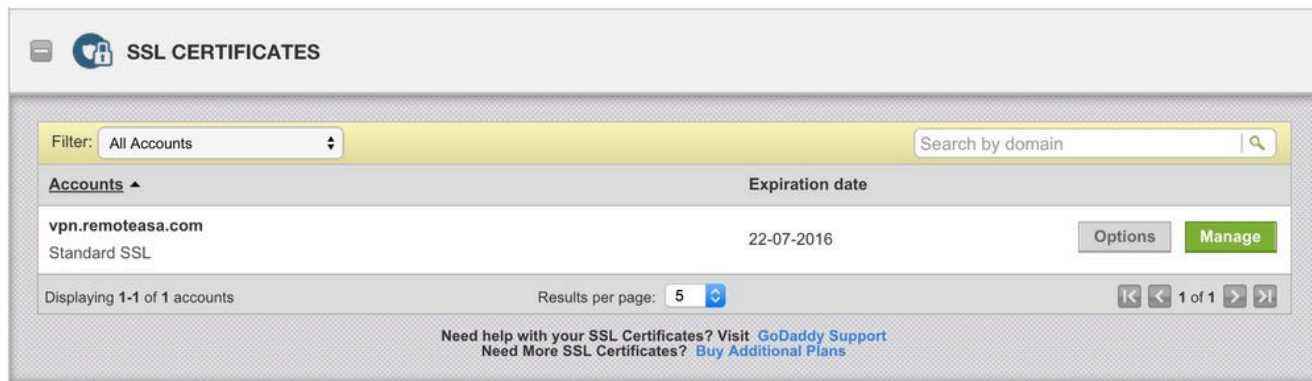


## ASA での SSL 証明書の更新

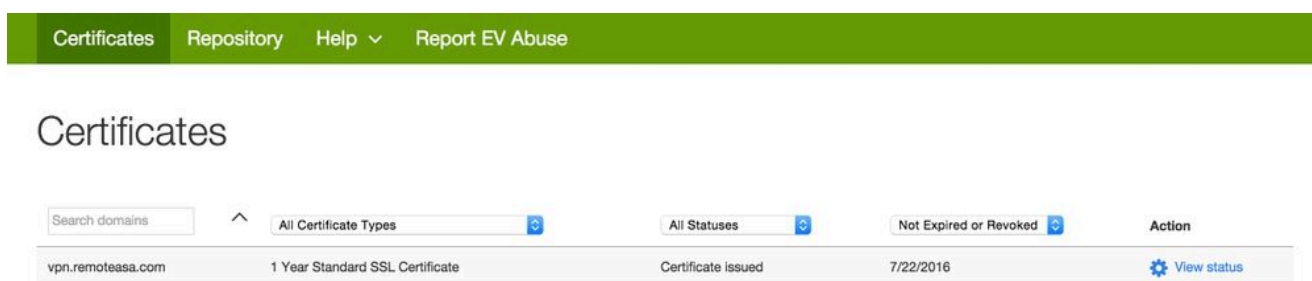
1. ASA で、または古い証明書と同じ属性を使用して OpenSSL が CA で、CSR を再生成します。「[CSR の生成](#)」に記載されている手順を実行します。
2. CA で CSR を送信し、CA 証明書とともに、PEM 形式 ( pem、.cer、.crt ) で新しいアイデンティティ証明書を生成します。PKCS12 証明書の場合は、新しい秘密キーも生成されま

GoDaddy CA の場合、生成された新しい CSR で証明書のキーを再生成できます。

[GoDaddyaccount] に移動し、[SSL証明書 ( SSL Certificates ) ] の下で [管理 ( Manage ) ] をクリックします。



必要なドメイン名の [ステータスの表示 ( View Status ) ] をクリックします。



[管理 ( Manage ) ] をクリックして、証明書のキーを再生成するためのオプションを指定します。

## All &gt; vpn.remoteasa.com

Standard SSL Certificate

## Certificate Management Options

		
Download	Revoke	Manage

## Certificate Details

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

オプションの [証明書のキーの再作成 ( Re-Key certificate ) ] を展開して、新しい CSR を追加します。

## vpn.remoteasa.com > Manage Certificate

Standard SSL Certificate

Use this page to submit your certificate changes for review all at once, not individually. We'll review them together so your changes happen faster.  
Submitting any changes on this form will issue a new certificate and your current certificate will be revoked. You will have 72 hours to install the new certificate on your website.

**Re-Key certificate**

Certificate Signing Request (CSR)

13gHhfenpRd3QX0kDh4P/wKl12bz/zb1v/SI  
 N80GsenQVuZaYzIH3R9EU/3Rz9  
 PcctuZ18yZLZTr6NSxk9m111aCuxlH9FmW

Domain Name (based on CSR):  
vpn.remoteasa.com

*Private key lost, compromised, or stolen? Time to re-key.*

**New Keys, please...**

You can generate a Certificate Signing Request (CSR) by using a certificate signing tool specific to your operating system. Your CSR contains a public key that matches the private key generated at the same time.

---

**Change the site that your certificate protects**

*If you want to switch your certificate from one site to another, do it [here](#).*

---

**Change encryption algorithm and/or certificate issuer**

*Upgrade your protection or change the company behind your cert.*

保存して、次のステップに進みます。GoDaddy は、提供された CSR に基づいて新しい証明書を発行します。

- 「ASA での SSL 証明書のインストール」のセクションに示されているように、新しい証明書を新しいトラストポイントにインストールします。

## よく寄せられる質問 (FAQ)

- アイデンティティ証明書をある ASA から別の ASA に転送する最善の方法は何ですか。

証明書をキーとともに PKCS12 ファイルにエクスポートします。

元の ASA から署名証明書をエクスポートするには、次のコマンドを使用します。

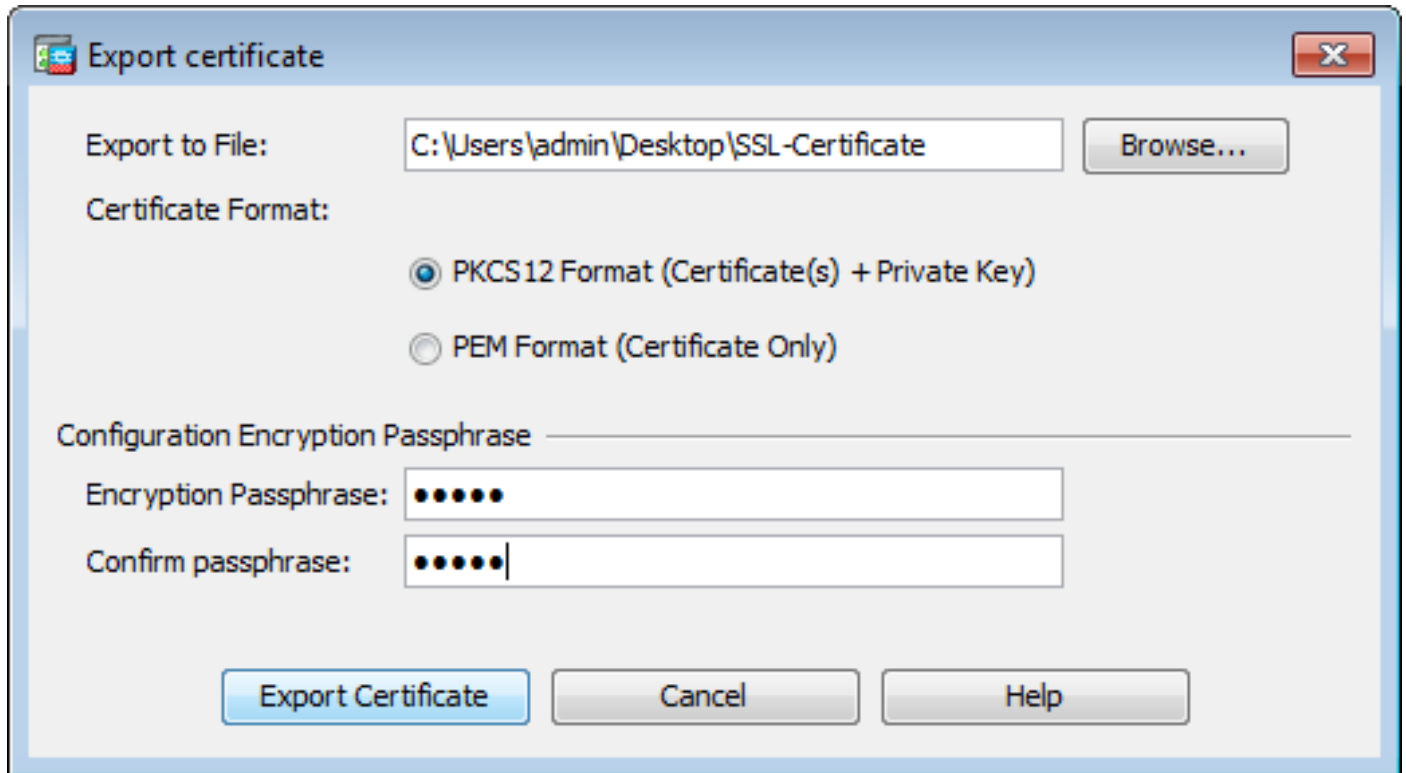
```
<#root>
```

```
ASA(config)#
```

```
crypto ca export
```

```
pkcs12
```

ASDM による設定：



CLI を介してターゲット ASA に証明書をインポートするには、次のコマンドを使用します。

```
<#root>
```

```
ASA(config)#
```

```
crypto ca import
```

```
pkcs12
```

ASDM による設定 :

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

これは、次の手順で ASDM のバックアップ/復元機能を使用して実行することもできます。

1. ASDM経由でASAにログインし、を選択します **Tools > Backup Configuration**。
2. すべての設定をバックアップするか、またはアイデンティティ証明書のみをバックアップします。
3. ターゲットASAでASDMを開き、 **Tools > Restore Configuration**。

2. VPN ロード バランシング ASA で使用する SSL 証明書を生成するにはどうすればよいですか。

VPN ロード バランシング環境用に SSL 証明書を使用して ASA をセットアップするために使用できる方法がいくつかあります。

1. DN としてロード バランシング FQDN を持ち、個別のサブジェクト代替名 (SAN) として各 ASA FQDN を持つ、1つのユニファイド コミュニケーション/複数ドメイン証明書 (UCC) を使用します。GoDaddy、Entrust、Comodo など、そのような証明書をサポートする、広く知られている CA がいくつかあります。この方法を選択する場合は、現在、ASA



では複数の SAN フィールドを持つ CSR の作成がサポートされていないことを覚えておくことが重要です。このことについては、機能拡張 Cisco Bug ID [CSCso70867](#) で説明されています。この場合、CSR を生成するには 2 つのオプションがあります。

- a. CLI または ASDM を使用します。CSR が CA に送信されたら、CA ポータル自体で複数の SAN を追加します。
- b. OpenSSL を使用して、CSR を生成し、複数の SAN を openssl.cnf ファイルに含めます。

CSR が CA および生成された証明書に送信されたら、この PEM 証明書を、CSR を生成した ASA にインポートします。完了したら、この証明書を PKCS12 形式でエクスポートして、他のメンバーの ASA にインポートします。

2. ワイルドカード証明書を使用します。これは UC 証明書と比べて安全性と柔軟性の点で劣っています。CA が UC 証明書をサポートしていない場合、CSR は CA で、または FQDN が \*.domain.com の形式である OpenSSL を使用して生成されます。CSR が CA および生成された証明書に送信されたら、PKCS12 証明書をクラスタ内のすべての ASA にインポートします。
3. メンバー ASA ごとに、およびロード バランシング FQDN に、個別の証明書を使用します。これは、最も効果が低い解決策です。このドキュメントに示すように、個々の ASA について証明書を作成できます。VPN ロードバランシング FQDN の証明書は、ある ASA で作成され、PKCS12 証明書としてエクスポートされて、他の ASA にインポートされます。

### 3. 証明書を ASA フェールオーバー ペアのプライマリ ASA からセカンダリ ASA にコピーする必要がありますか。

ステートフル フェールオーバーが設定されている限り、ASA 間で証明書が同期されるため、プライマリ ASA からセカンダリ ASA に証明書を手動でコピーする必要はありません。フェールオーバーの初期セットアップで、証明書がスタンバイ デバイスに表示されない場合は、コマンド `write standby` を発行して、同期を強制します。

### 4. ECDSA キーが使用されている場合、SSL 証明書の生成プロセスは異なりますか。

構成の唯一の違いは、キーペアの生成手順です。この場合、RSA キーペアの代わりに ECDSA キーペアが生成されます。手順のそれ以外の部分は変わりません。ECDSA キーを生成するための CLI コマンドを次に示します。

```
<#root>
```

```
MainASA(config)#
```

```
cry key generate ecdsa label SSL-Keypair elliptic-curve 256
```

```
INFO: The name for the keys will be: SSL-Keypair  
Keypair generation process begin. Please wait...
```

# トラブルシューティング

## トラブルシューティングのためのコマンド

SSL 証明書のインストールに失敗した場合、次のデバッグ コマンドが CLI で収集されます。

```
debug crypto ca 255
```

```
debug crypto ca messages 255
```

```
debug crypto ca transactions 255
```

## 一般的な問題

9.4(1) 以降を実行している ASA の外部インターフェイスで有効なサードパーティの SSL 証明書を使用する場合、信頼できない証明書に関する警告が出されます。

解決策：この問題は、証明書で RSA キーペアが使用されている場合に発生します。9.4(1) 以降の ASA バージョンでは、すべての ECDSA および RSA 暗号がデフォルトで有効になっており、最も強力な暗号（通常は ECDSA 暗号）がネゴシエーションに使用されます。この場合、ASA は、現在設定されている RSA ベースの証明書の代わりに自己署名証明書を提示します。RSA ベースの証明書がインターフェイスにインストールされ、Cisco bug ID [CSCuu02848](#) によって追跡される場合の動作を変更するための機能拡張が用意されています。

推奨処置：次の CLI コマンドを使用して、ECDSA 暗号を無効にします。

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

または、ASDMで、に移動し **Configuration > Remote Access VPN > Advanced**、を選択します **SSL Settings**。[暗号化 (Encryption)] セクションで、[暗号バージョン (Cipher version)] として **tlsv1.2** を選択し、カスタム文字列 **AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5** を使用してそれを編集します。

## 付録

### 付録 A：ECDSA または RSA

ECDSA アルゴリズムは楕円曲線暗号 (ECC) の一部であり、楕円曲線の式を使用して公開キーを生成します。RSA アルゴリズムでは、2 つの素数と小さい数の積を使用して公開キーを生成します。つまり、ECDSA では RSA と同じレベルのセキュリティを実現できますが、キーは小さくなります。これにより、計算時間が短縮され、ECDSA 証明書を使用するサイトの接続時間が増加します。

[次世代暗号化と ASA に関するドキュメントでは、詳細な情報を提供しています。](#)

## 付録 B : OpenSSL を使用して、アイデンティティ証明書、CA 証明書、および秘密キーから PKCS12 証明書を生成する

1. このプロセスが実行されているシステムに OpenSSL がインストールされていることを確認します。Mac OSX および GNU/Linux ユーザーの場合、これはデフォルトでインストールされます。
2. 有効なディレクトリに切り替えます。

Windows の場合 : デフォルトでは、ユーティリティは C:\Openssl\bin にインストールされます。この場所でコマンドプロンプトを開きます。

Mac OSX/Linux の場合 : PKCS12 証明書を作成するために必要なディレクトリで、ターミナルウィンドウを開きます。

3. 前の手順で説明したディレクトリに、秘密キー ( privatekey.pem )、アイデンティティ証明書 ( certificate.crt )、およびルート CA 証明書チェーン ( CACert.crt ) の各ファイルを保存します。

秘密キー、アイデンティティ証明書、およびルート CA 証明書チェーンを PKCS12 ファイルに結合します。PKCS12 証明書を保護するためのパスフレーズを入力します。

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -cer
```

4. 生成された PKCS12 証明書を Base64 でエンコードされた証明書に変換します。

```
<#root>
```

```
openssl base64 -in certificate.pfx -out certificate.p12
```

次に、最後の手順で生成された証明書を、SSL で使用するためにインポートします。

## 関連情報

- [ASA 9.x コンフィギュレーション ガイド : デジタル証明書の設定](#)
- [ASA で ASDM を使用して Microsoft Windows CA からデジタル証明書を取得する方法](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 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。