ASDMで管理されるASAでの証明書のインストールと更新

内容

よく寄せられる質問（FAQ）

概要

このドキュメントでは、ASDMで管理されているCisco ASAソフトウェアで特定の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

- 開始する前に、適応型セキュリティアプライアンス(ASA)のクロック時刻、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、ネットワークタイムプロトコル(NTP)サーバを使用してASAの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)にアクセスできる必要があります。サードパーティCAベンダーの例としては、Entrust、Geotrust、GoDaddy、Thawte、VeriSignなどがあります。

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種類は次のとおりです。

- 自己署名証明書
- サードパーティ認証局または内部CAによって署名された証明書

EAP認証プロトコル用のSecure Socket Layer(SSL)、Transport Layer Security(TLS)、およびIKEv2 rfc7296では、SSL/TLS/IKEv2サーバが、クライアントがサーバ認証を実行するためのサーバ証明書をクライアントに提供する必要があります。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。

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応答する必要があるという不便さもあります。

ASDMを使用した新しいID証明書の要求とインストール

証明書は、認証局(CA)から要求し、次の2つの方法でASAにインストールできます。

- 証明書署名要求(CSR)を使用します。キーペアを生成し、CSRを使用してCAからID証明書を要求し、CAから取得した署名付きID証明書をインストールします。
- CAから取得した、または別のデバイスからエクスポートしたPKCS12ファイルを使用します。PKCS12ファイルには、キーペア、ID証明書、CA証明書が含まれています。

証明書署名要求(CSR)を使用した新しいID証明書の要求とインストール

ID証明書を必要とするデバイス上にCSRが作成されます。デバイス上に作成されたキーペアを使用します。

CSRには次のものが含まれます。

- 証明書要求情報：要求されたサブジェクトおよびその他の属性、キーペアからの公開キー、
- シグニチャアルゴリズム情報、
- キーペアからの秘密キーで署名された、証明書要求情報のデジタル署名。

CSRは認証局(CA)に渡され、PKCS#10形式で署名されます。

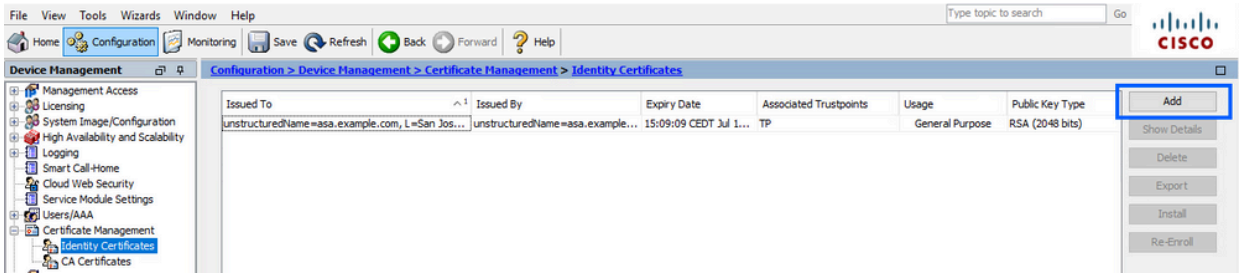
署名付き証明書は、PEM形式でCAから返されます。

注：CAは、CSRに署名して署名付き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。

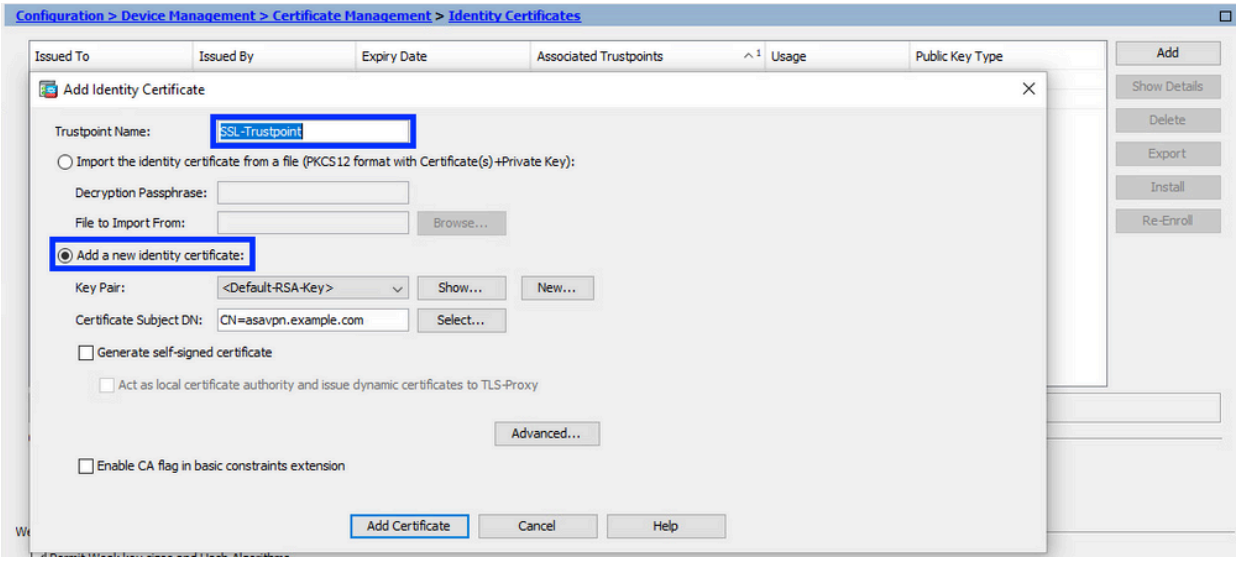
ASDMを使用したCSRの生成

1. 特定の名前を使用したトラストポイントの作成

   a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動します。



   b. [Add] をクリックします。
   c. トラストポイント名を定義します。



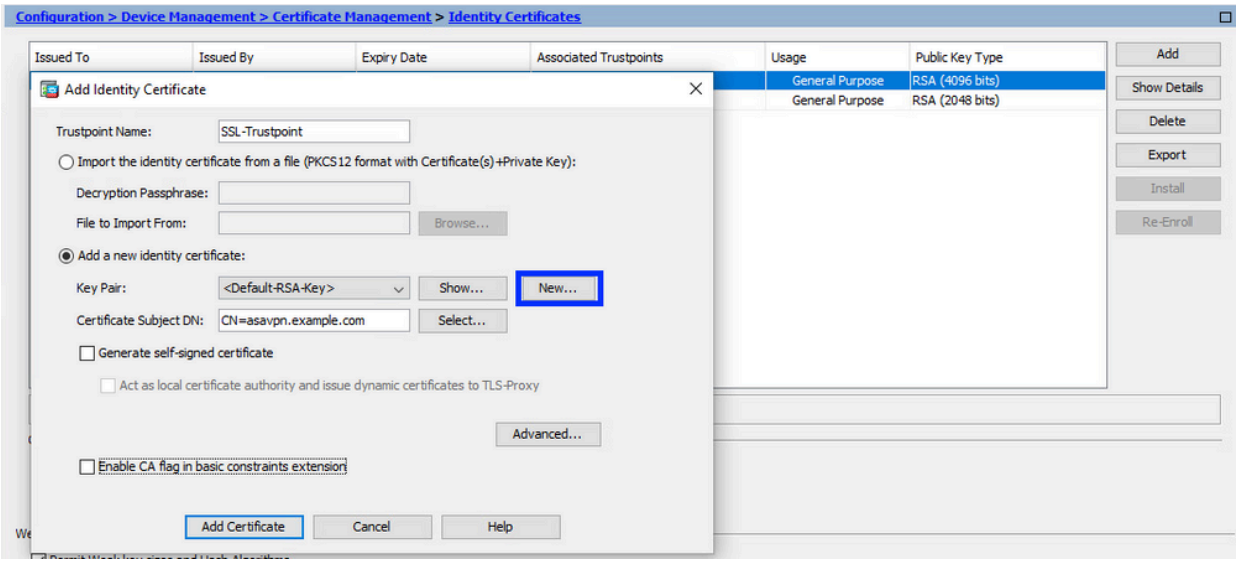
d. [Add a new identity certificate] オプション ボタンをクリックします。

2. （オプション）新しいキーペアの作成

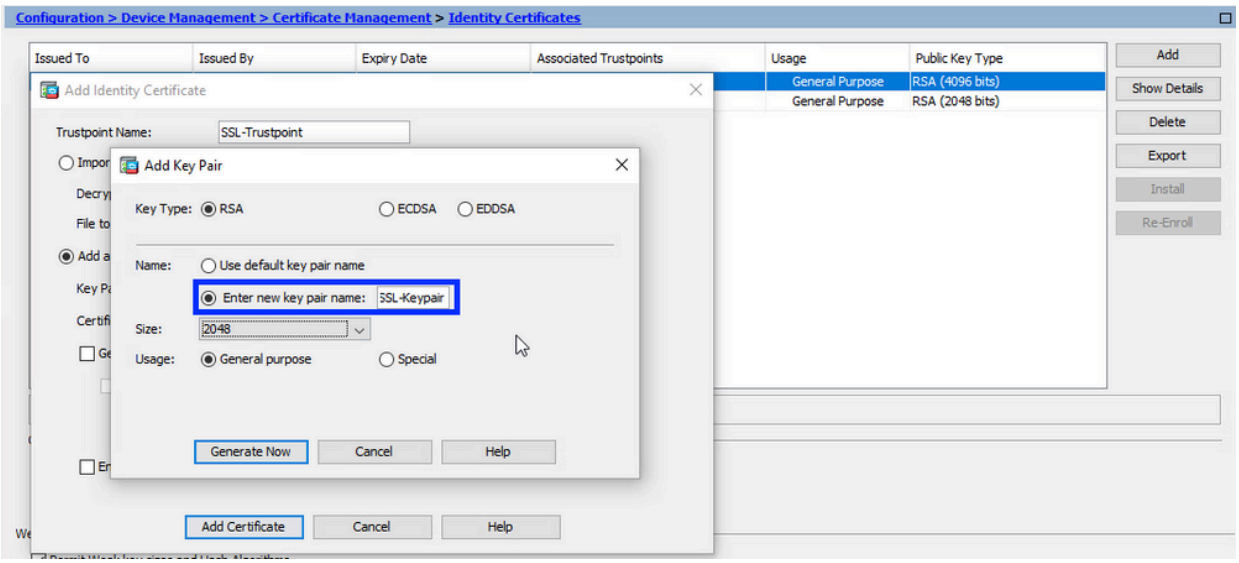
注：デフォルトでは、Default-RSA-Keyという名前とサイズが2048のRSAキーが使用されますが、各ID証明書に一意の秘密キーと公開キーのペアを使用することをお勧めします。

---

a. Newをクリックして、新しいキーペアを生成します。

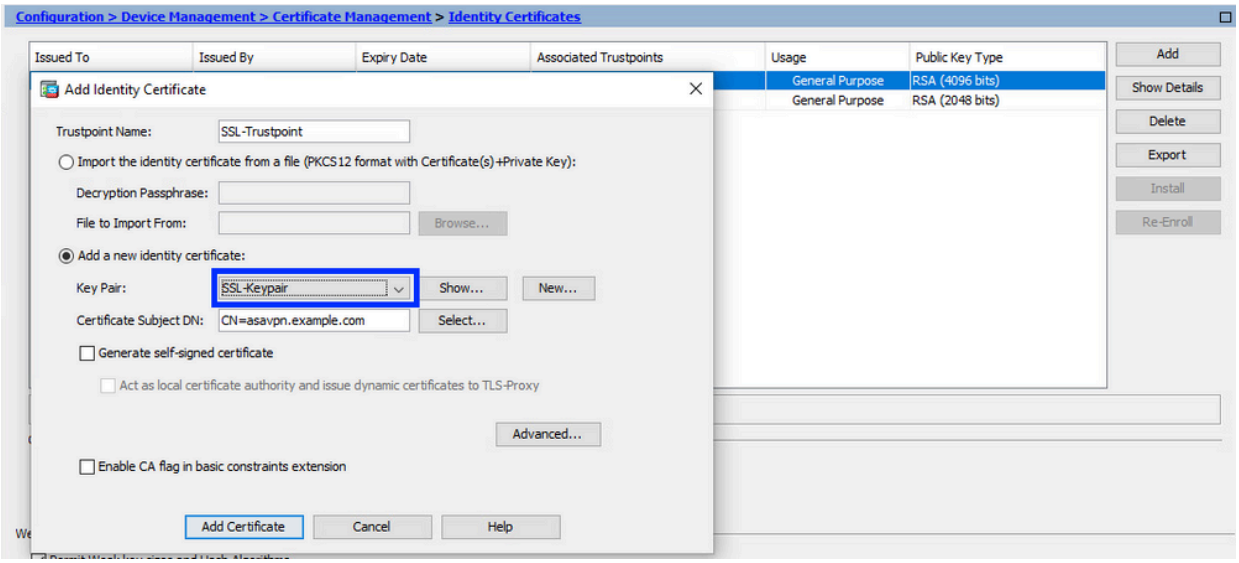


b. Enter new Key Pair nameオプションを選択し、新しいキーペアの名前を入力します。
c. [キータイプ（Key Type）] に RSA または ECDSA を選択します。
d. Key Sizeを選択し、RSAの場合はGeneral purpose for Usageを選択します。
e. [Generate Now] をクリックします。これでキーペアが作成されます。



3. キーペア名の選択

CSRに署名し、新しい証明書にバインドするキーペアを選択します。

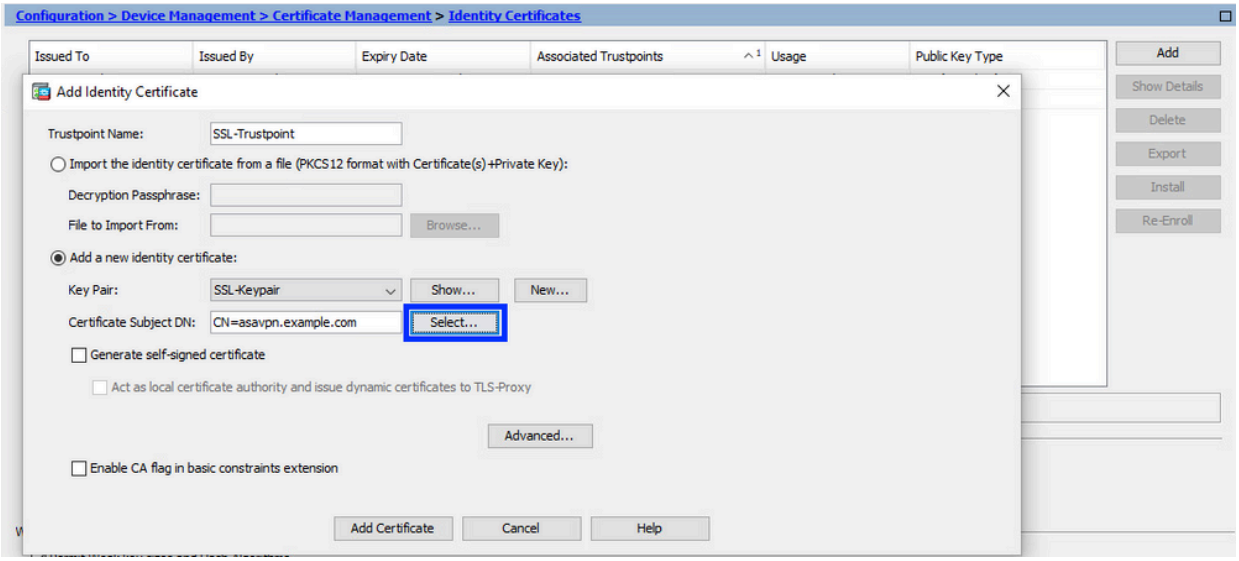


4. 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定

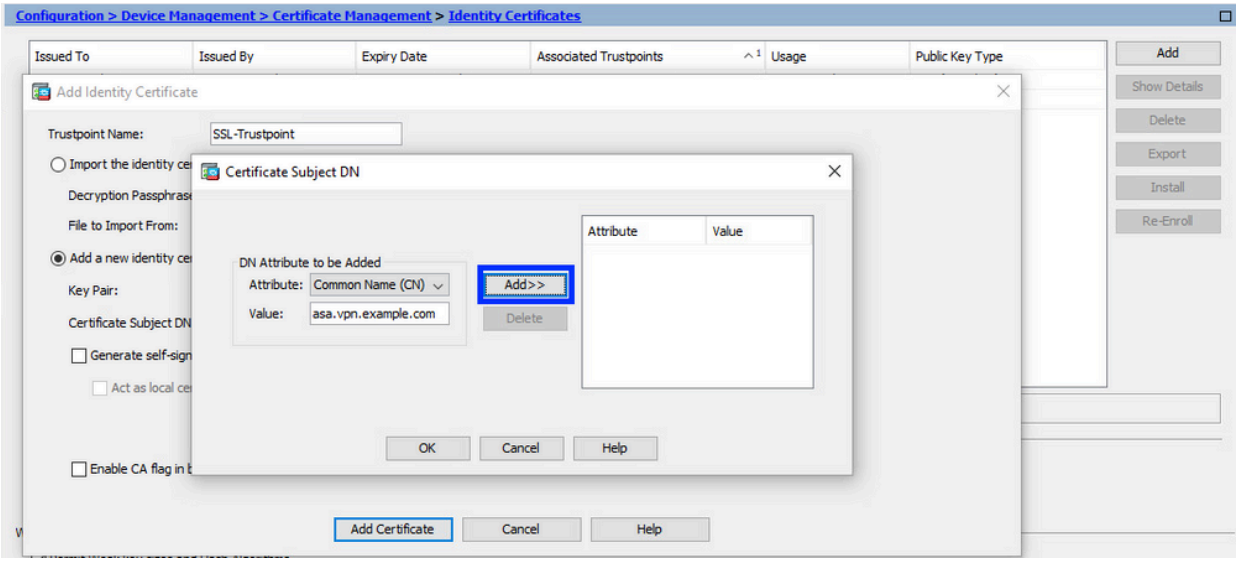
注意:FQDNパラメータは、ID証明書が使用されるASAインターフェイスのFQDNまたはIPアドレスと一致する必要があります。このパラメーターは、ID証明書に対して要求されたサブジェクト代替名(SAN)拡張を設定します。SAN拡張は、証明書が接続先のFQDNと一致するかどうかを確認するためにSSL/TLS/IKEv2クライアントによって使用されます。

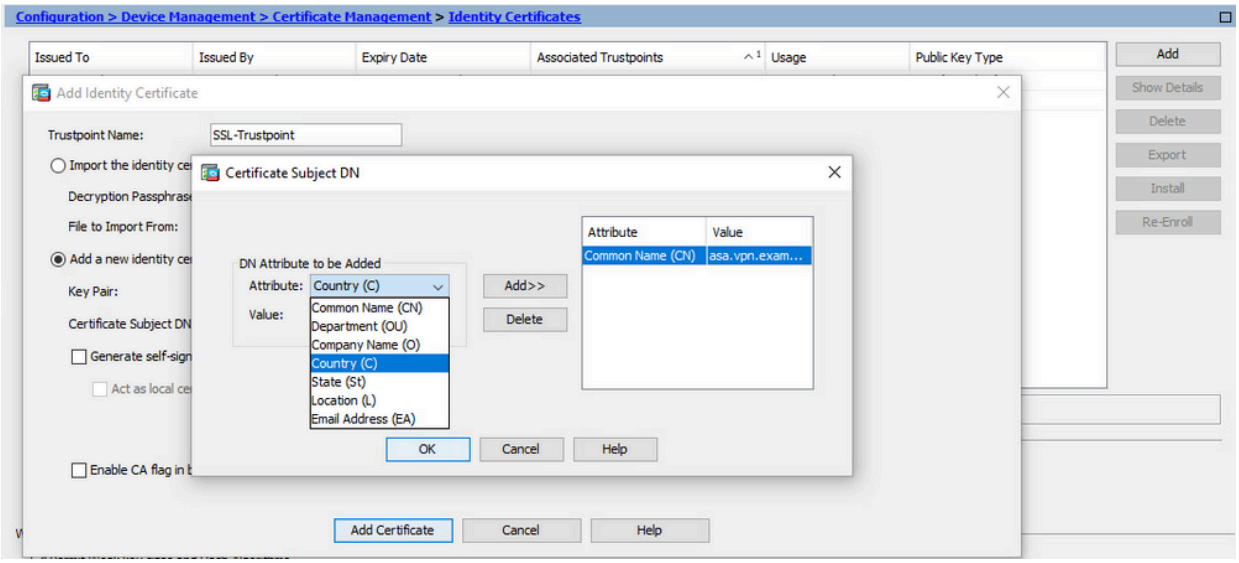
---

a. [Select] をクリックします。



b. Certificate Subject DNウィンドウで、certificate attributes - choose attribute fromドロップダウンリストを設定し、値を入力して、Addをクリックします。



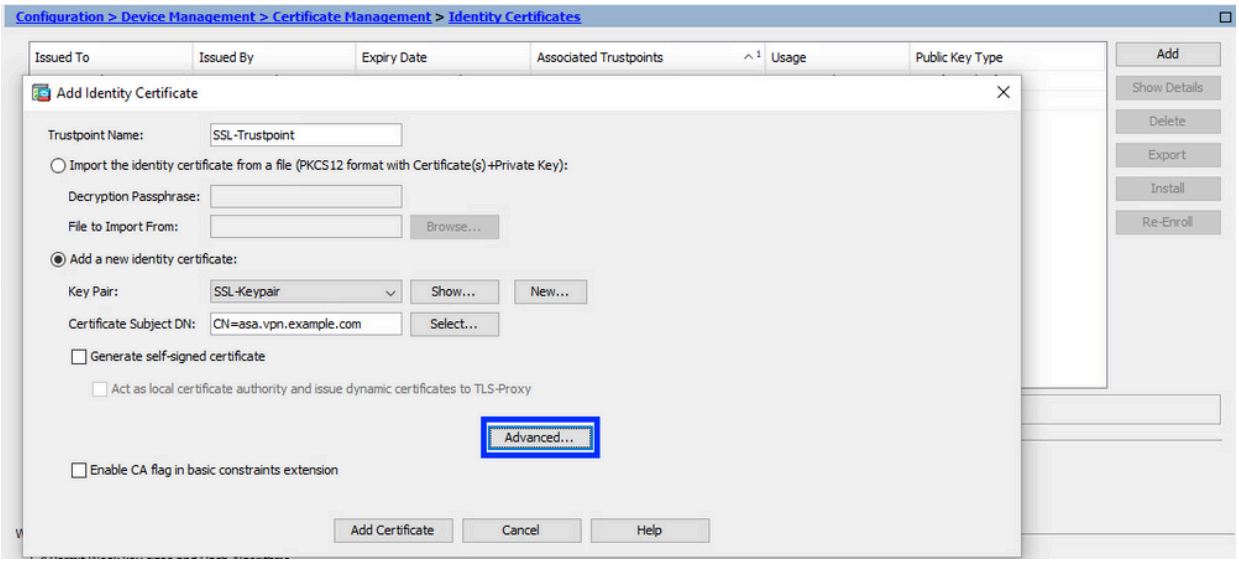


Attribute	説明
CN	ファイアウォールへのアクセスに使用される名前(通常は、vpn.example.comなどの完全修飾ドメイン名)。
OU	組織内の部署の名前
O	法的に登録されている組織/会社の名前
C	国コード（句読点のない 2 文字のコード）
ST	組織の所在する都道府県。
起	組織が所在する市区町村。
EA	電子メールアドレス

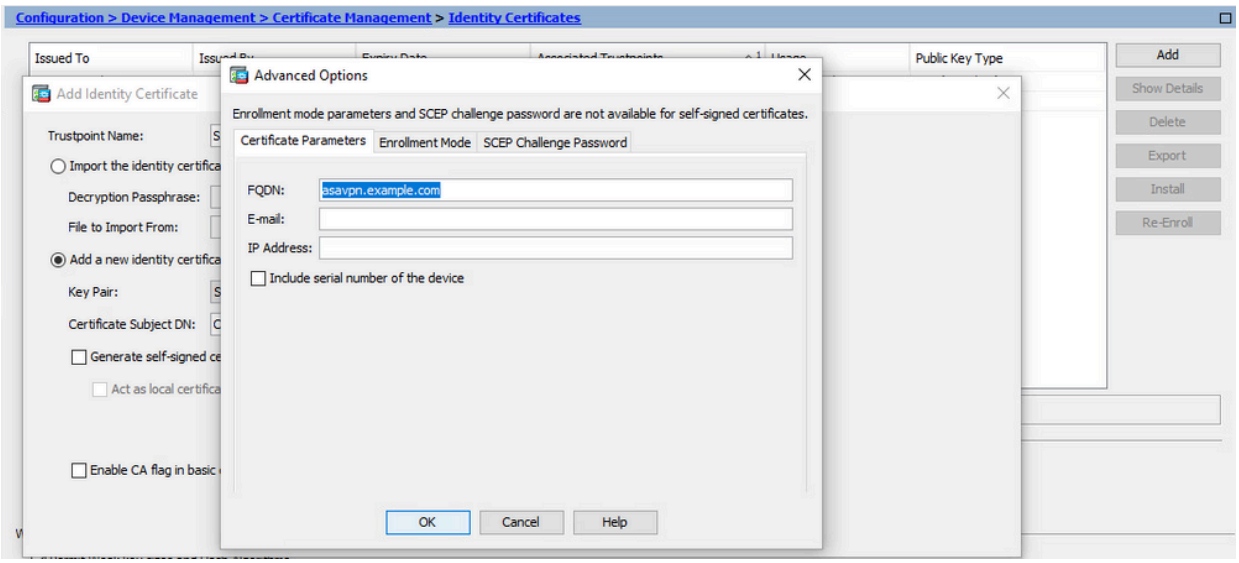
注：上記のフィールドの値はいずれも、64文字の制限を超えることはできません。この値を大きくすると、ID証明書のインストールで問題が発生する可能性があります。また、すべてのDN属性を定義する必要はありません。

すべての属性を追加したら、OKをクリックします。

c. デバイスのFQDNを設定し、Advancedをクリックします。

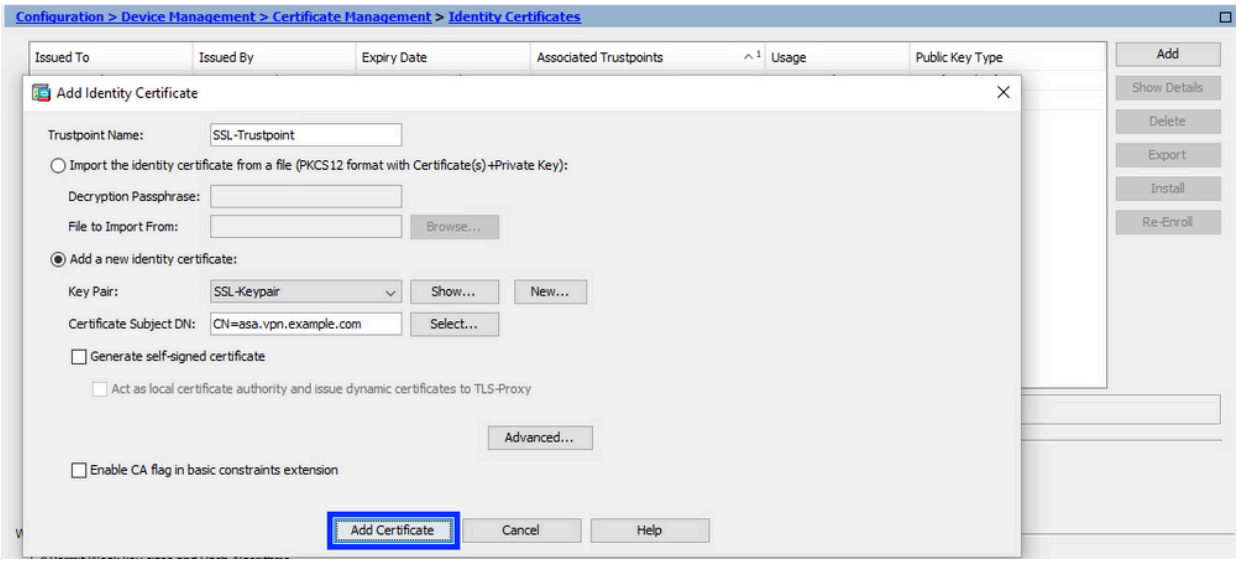


d. FQDNフィールドに、デバイスがインターネットからアクセス可能な完全修飾ドメイン名を入力します。[OK] をクリックします。

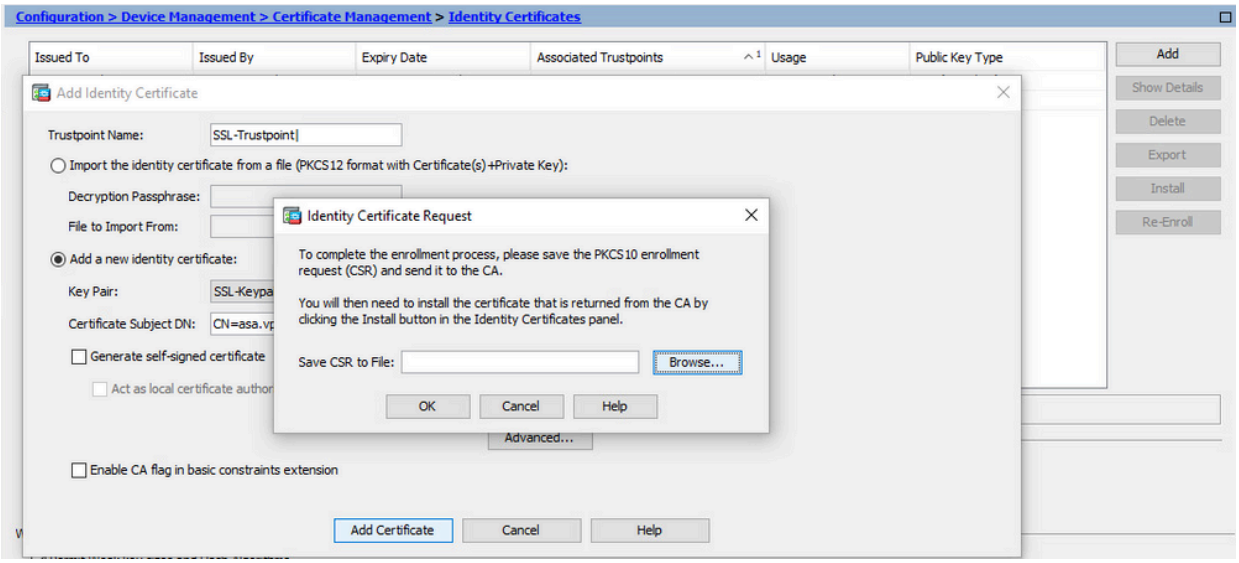


5. CSRの生成と保存

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



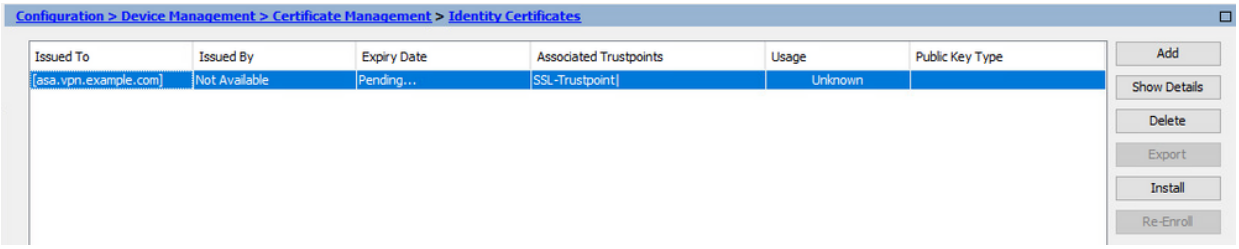
b. CSR をローカル マシン上のファイルに保存するためのプロンプトが表示されます。



[Browse] をクリックし、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：ファイルを.txt拡張子で保存すると、PKCS#10要求をテキストエディタ（メモ帳など）で開いて表示できます。

c. 新しいトラストポイントがPending状態で表示されます。

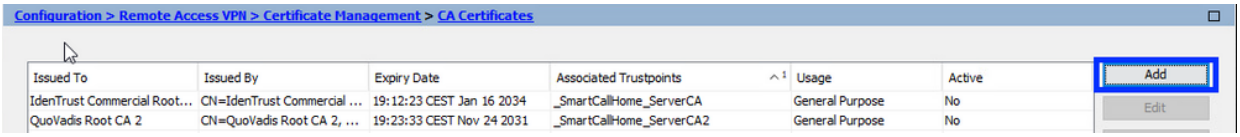


ASDMを使用したPEM形式でのID証明書のインストール

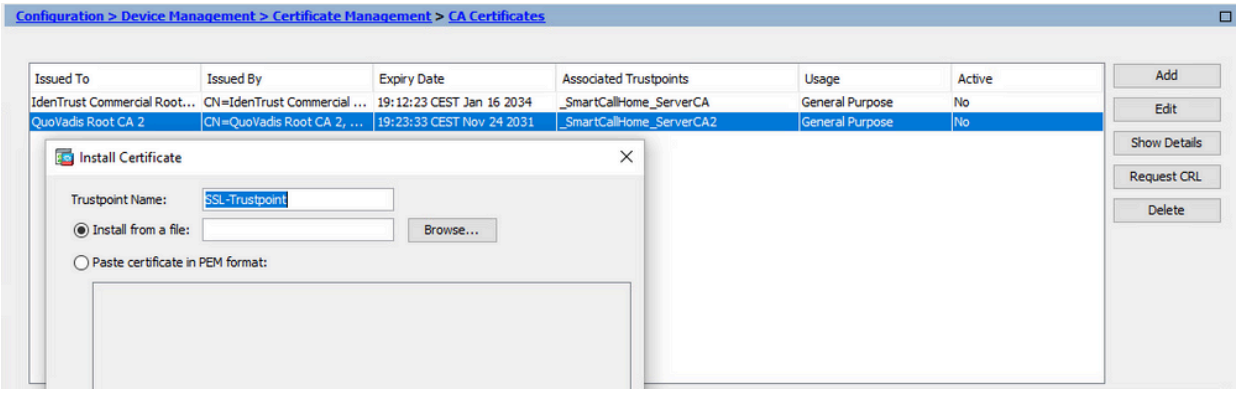
インストール手順では、CAがCSRに署名し、PEMエンコード(.pem、.cer、.crt)のID証明書とCA証明書バンドルが提供されていることを前提としています。

1. CSRに署名したCA証明書のインストール

a. Configuration > Device Management > Certificate Management >の順に移動し、CA Certificatesを選択します。[Add] をクリックします。

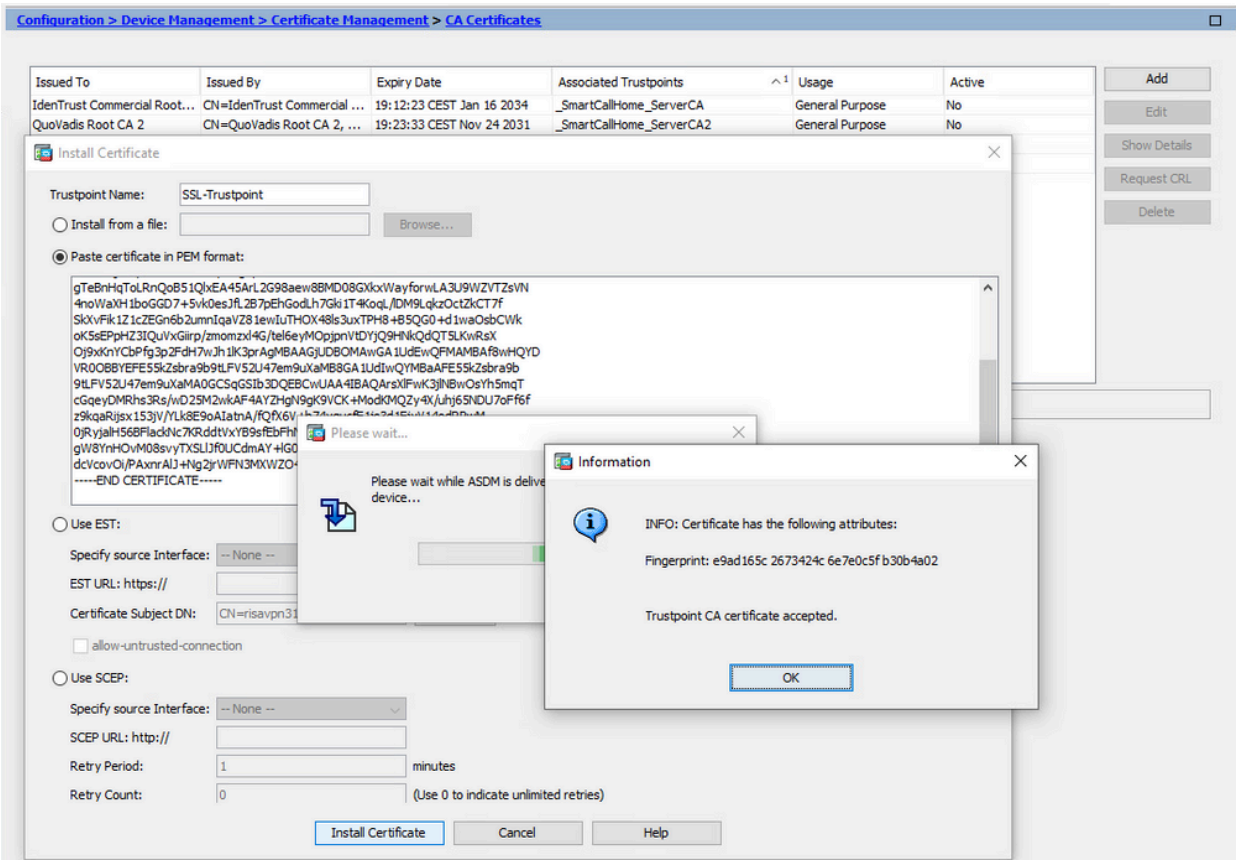


b. トラストポイント名を入力してInstall From Fileを選択し、Browseボタンをクリックして中間証明書を選択します。または、テキストファイルのPEMエンコードCA証明書をテキストフィールドに貼り付けます。



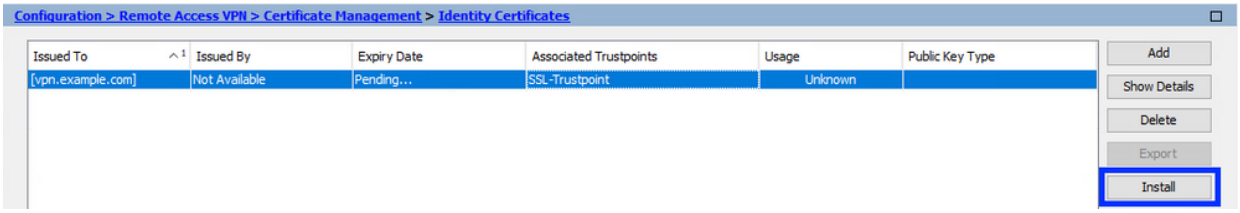
注:CSRに署名したCA証明書をインストールし、ID証明書と同じトラストポイント名を使用します。PKI階層の上位にあるその他のCA証明書は、別々のトラストポイントにインストールできます。

c. [Install Certificate] をクリックします。



2. ID 証明書のインストール

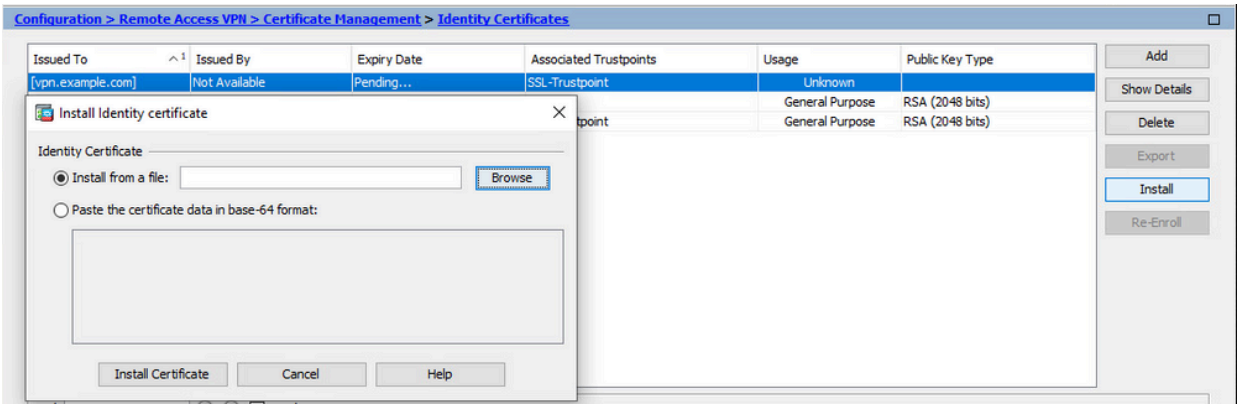
a. CSRの生成中に以前に作成したID証明書を選択します。[INSTALL] をクリックします。



注:ID証明書では、Issued Byフィールドを Not available、Expiry Dateフィールドを Pendingにすることができます。

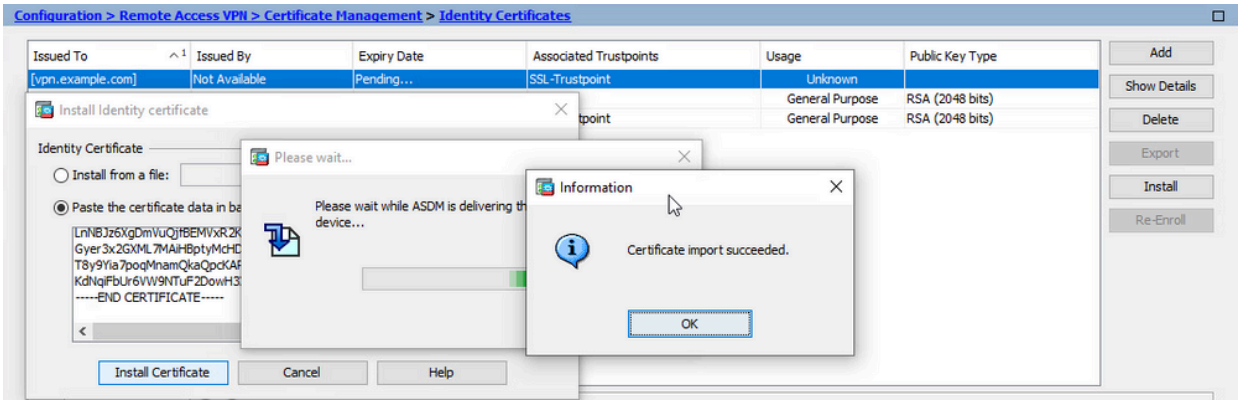
---

b. CAから受信したPEMでエンコードされたID証明書を含むファイルを選択するか、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、CAから提供されたID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。



注:ID証明書は、.pem、.cer、.crt形式でインストールできます。

c. [Install Certificate] をクリックします。



3. ASDMを使用したインターフェイスへの新しい証明書のバインド

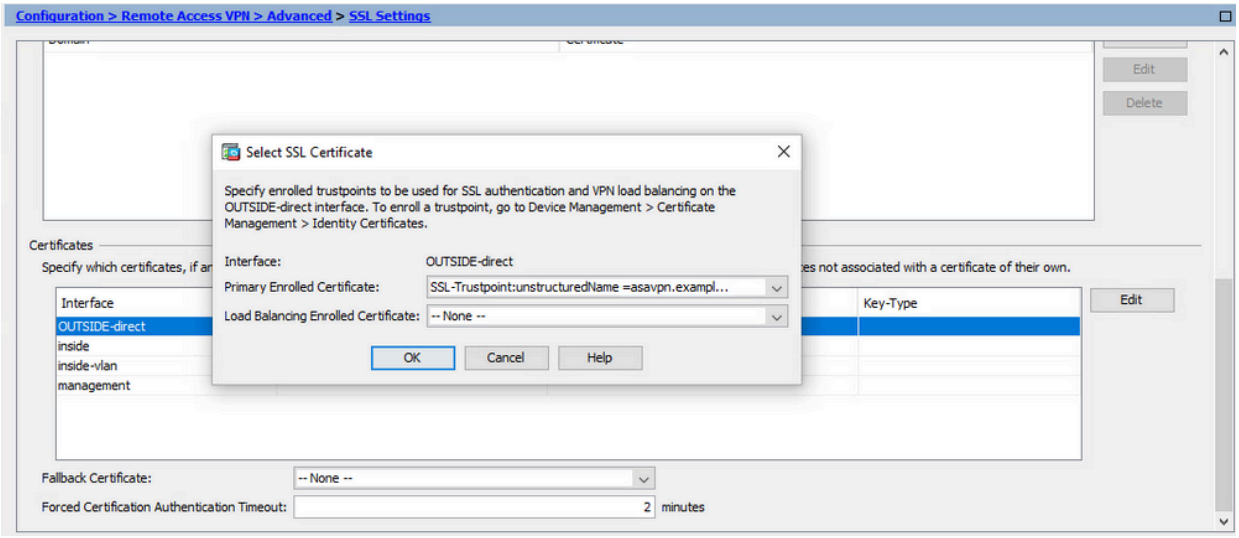
指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用するようにASAを設定する必要があります。

a. [構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [詳細（Advanced）] > [SSL設定（SSL Settings）] の順に移動します。

b. [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。

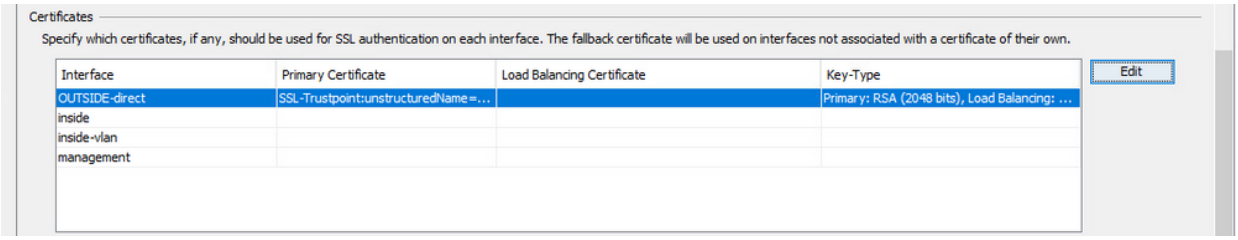
[Edit] をクリックします。

c. [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。



d. [OK] をクリックします。

e. [APPLY] をクリックします。



これで、新しいID証明書が使用されています。

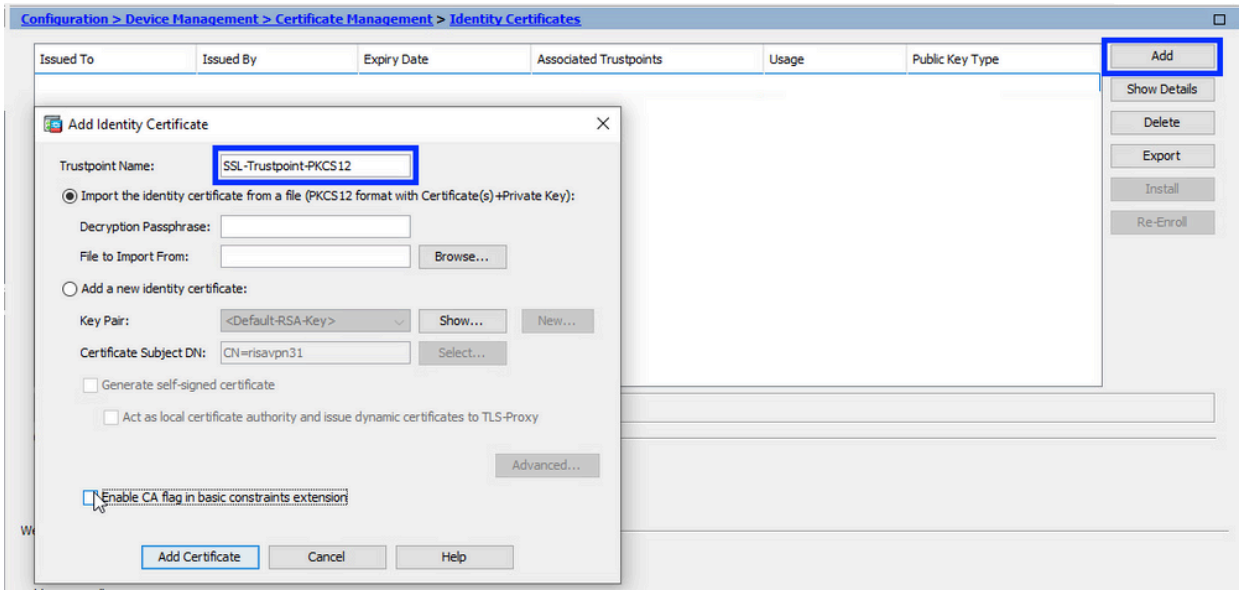
ASDMを使用したPKCS12形式で受信したID証明書のインストール

PKCS12ファイル（.p12または.pfx形式）には、ID証明書、キーペア、およびCA証明書が含まれています。これは、CAによって作成されます（ワイルドカード証明書の場合など）。または、別のデバイスからエクスポートされます。これはバイナリファイルであり、テキストエディタで表示することはできません。

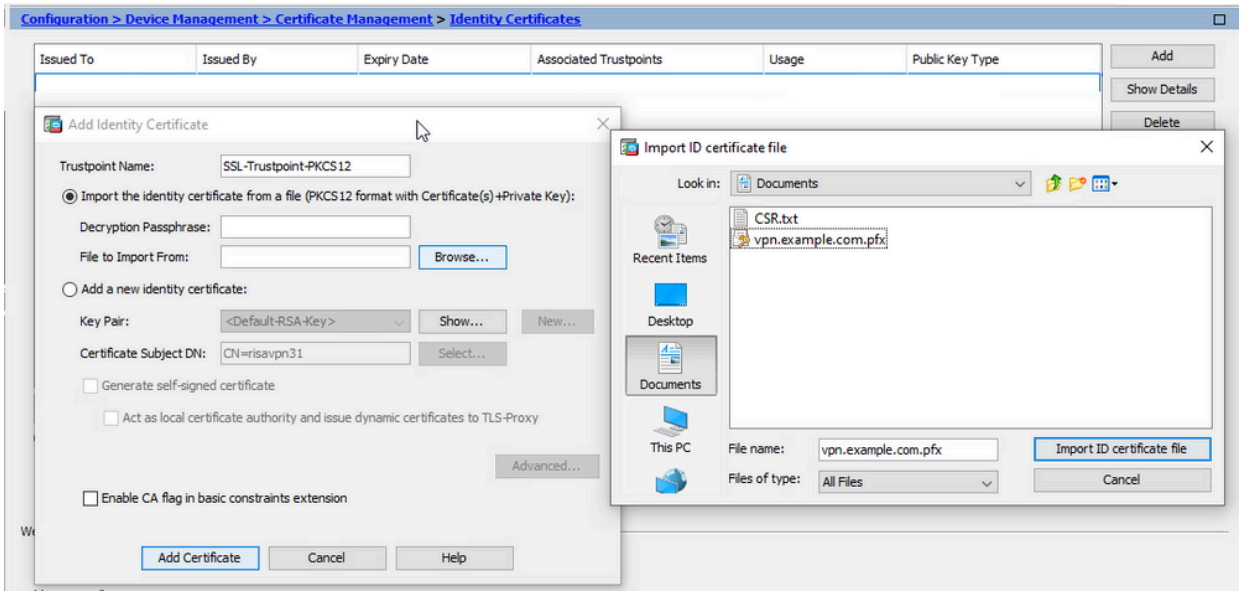
1. PKCS12ファイルからのID証明書とCA証明書のインストール

ID証明書、CA証明書、およびキーペアを1つのPKCS12ファイルにバンドルする必要があります。

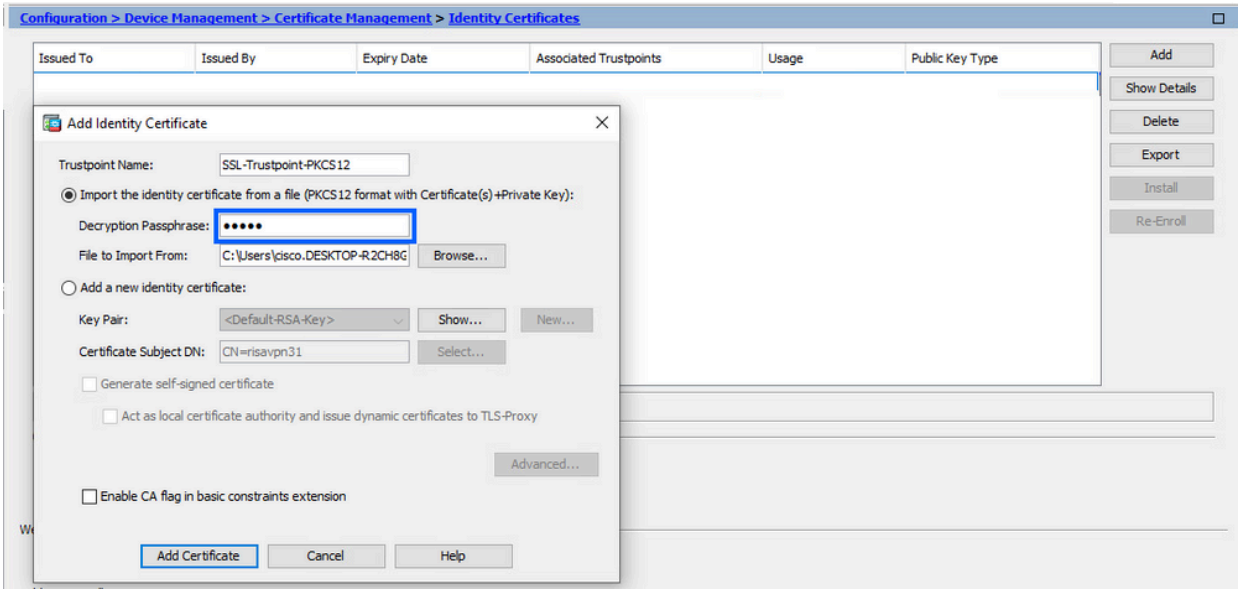
a. Configuration > Device Management > Certificate Managementの順に移動し、Identity Certificatesを選択します。
b. [Add] をクリックします。
c. トラストポイント名を指定します。



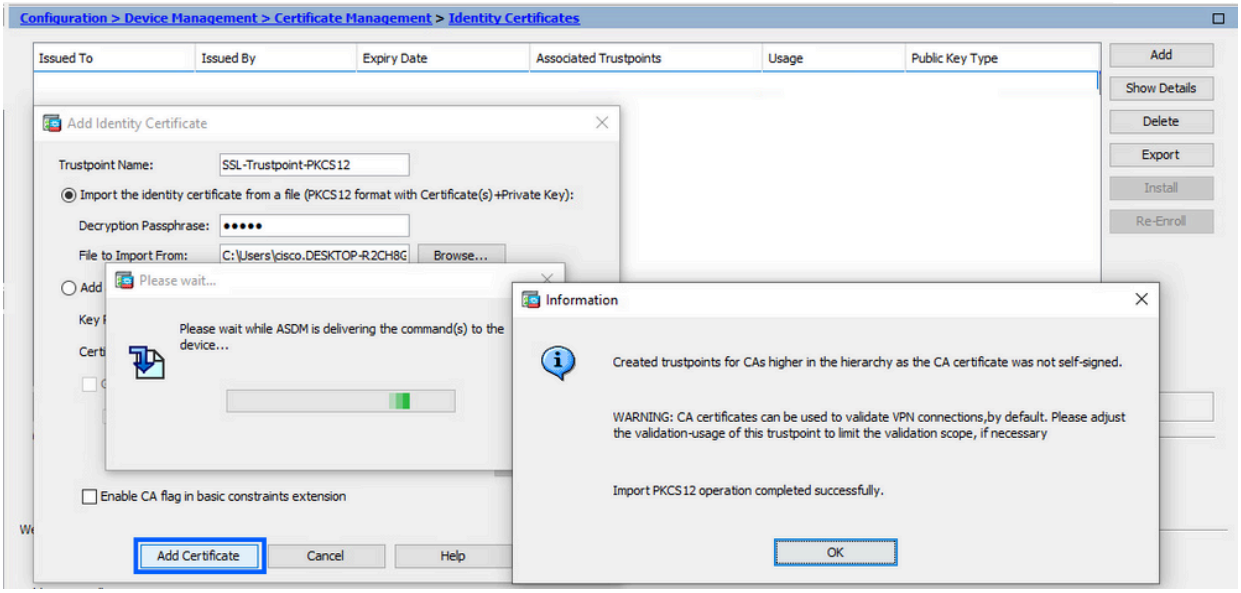
d. [アイデンティティ証明書をファイルからインポートする（Import the identity certificate from a file）] ラジオ ボタンをクリックします。



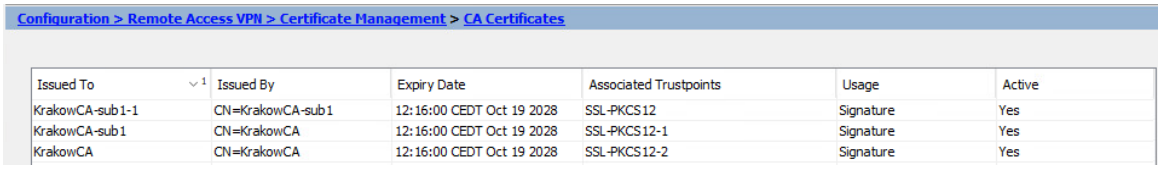
e. PKCS12 ファイルの作成に使用するパスフレーズを入力します。



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



注:CA証明書チェーンを含むPKCS12をインポートすると、ASDMは追加された– numberサフィックスを持つ名前でアップストリームCAトラストポイントを自動的に作成します。



2. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用するようにASAを設定する必要があります。

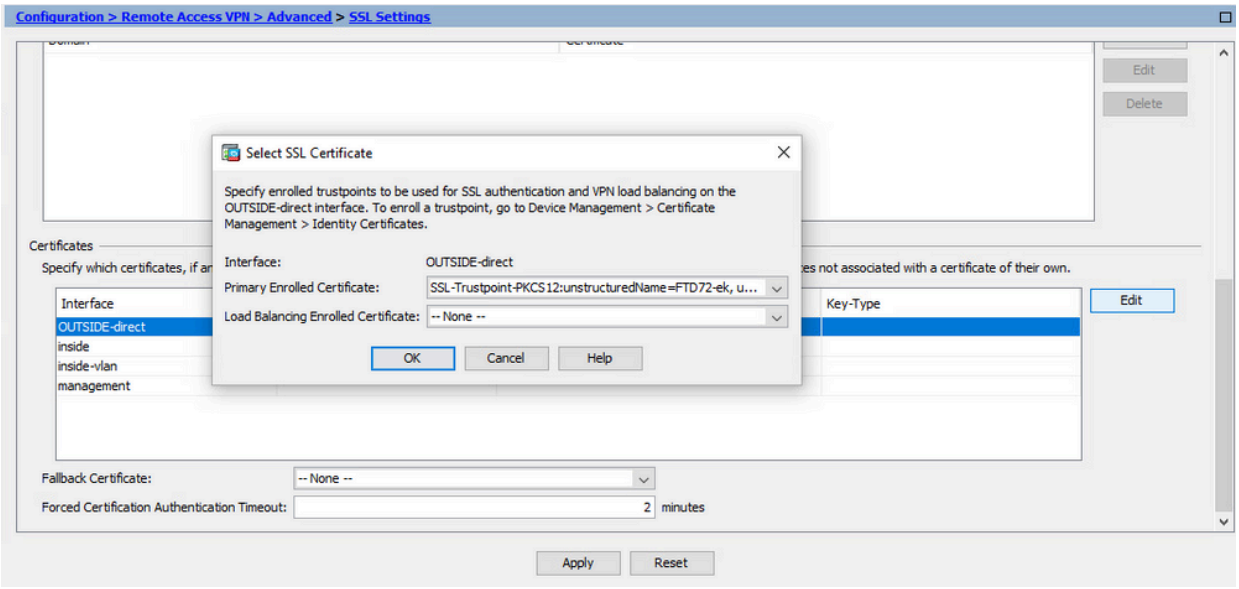
a. [構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [詳細

（Advanced）] > [SSL設定（SSL Settings）] の順に移動します。

b. [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。

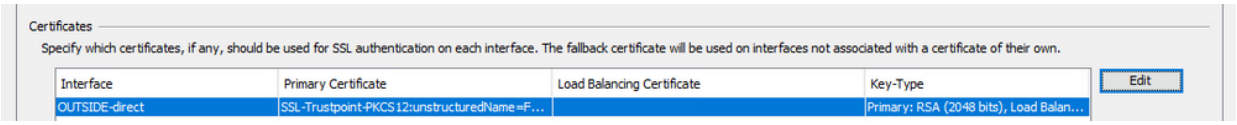
[Edit] をクリックします。

c. [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。



d. [OK] をクリックします。

e. [APPLY] をクリックします。



これで、新しいID証明書が使用されています。

証明書の更新

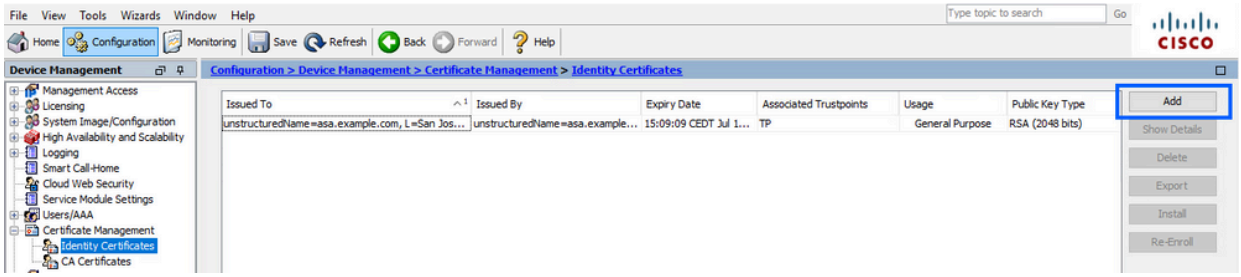
ASDMを使用した証明書署名要求(CSR)に登録された証明書の更新

CSRに登録された証明書の証明書の更新では、新しいトラストポイントを作成して登録する必要があります。別の名前（登録年のサフィックスを持つ古い名前など）にする必要があります。古い証明書と同じパラメータとキーペアを使用することも、異なるパラメータとキーペアを使用することもできます。

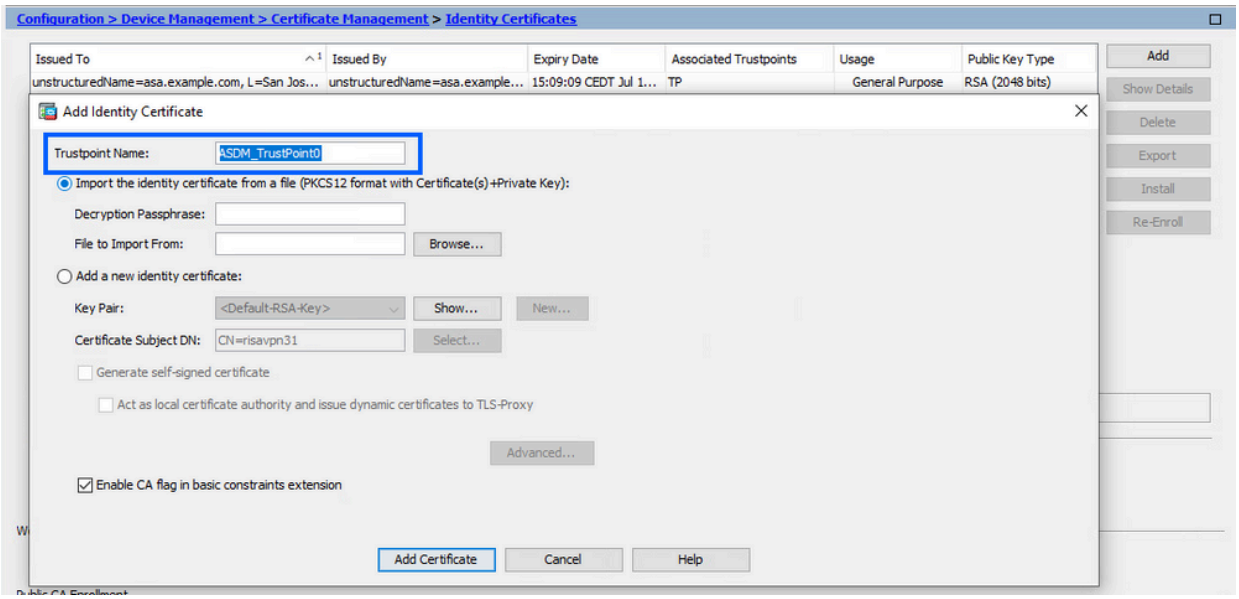
ASDMを使用したCSRの生成

1. 特定の名前で新しいトラストポイントを作成します。

   a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動します。



   b. [Add] をクリックします。
   c. トラストポイント名を定義します。



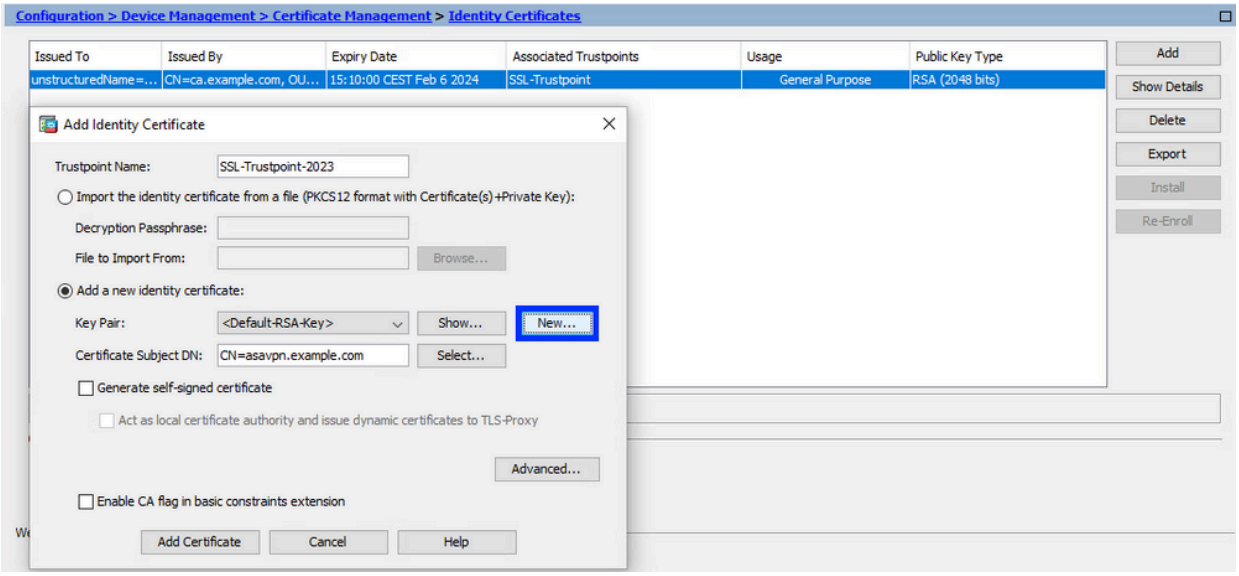
   d. [Add a new identity certificate] オプション ボタンをクリックします。

2. （オプション）新しいキーペアの作成

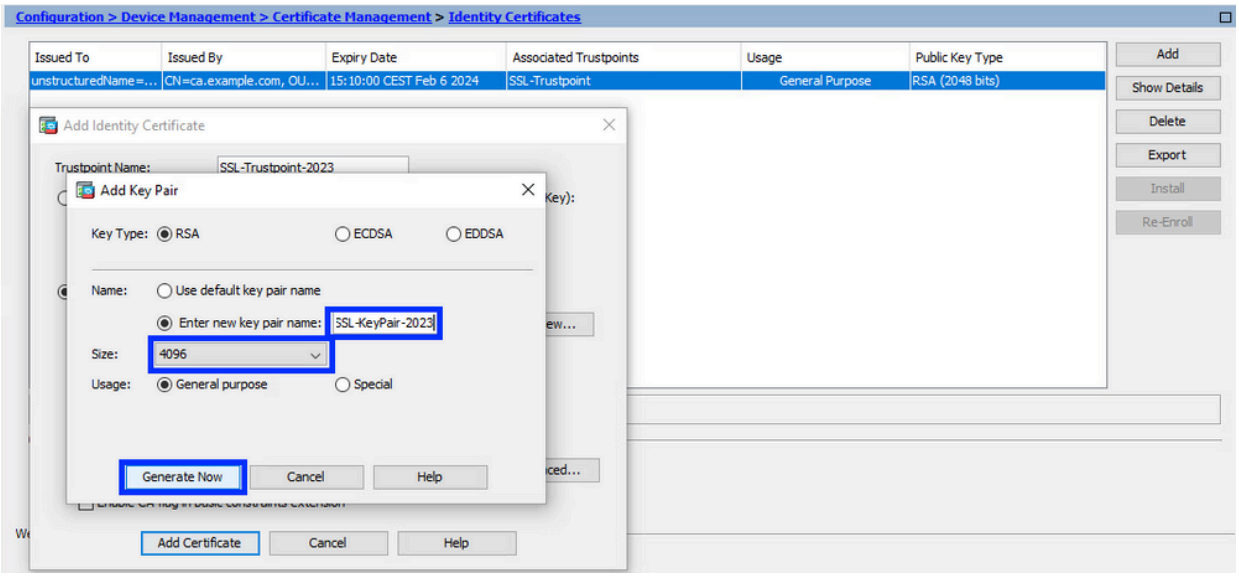
注：デフォルトでは、Default-RSA-Keyという名前とサイズが2048のRSAキーが使用されますが、各ID証明書に一意の秘密キーと公開キーのペアを使用することをお勧めします。

---

   a. Newをクリックして、新しいキーペアを生成します。

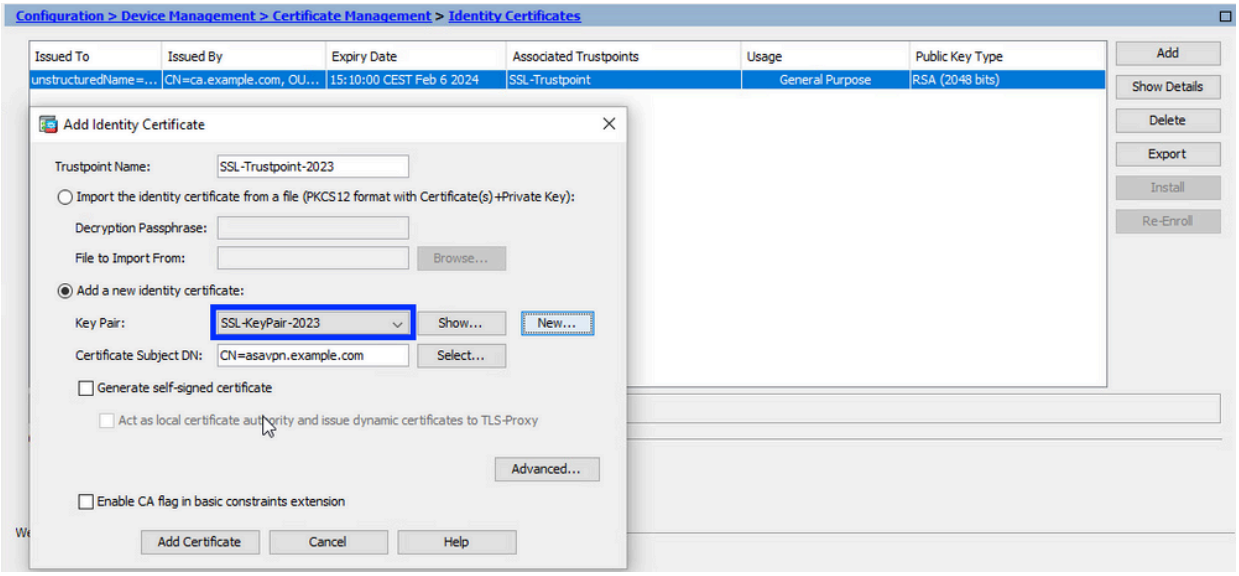


b. Enter new Key Pair nameオプションを選択し、新しいキーペアの名前を入力します。
c. [キータイプ（Key Type）] に RSA または ECDSA を選択します。
d. Key Sizeを選択します。RSAの場合は、UsageのGeneral purposeを選択します。
e. [Generate Now] をクリックします。これでキーペアが作成されます。



3. キーペア名の選択

CSRに署名し、新しい証明書にバインドするキーペアを選択します。



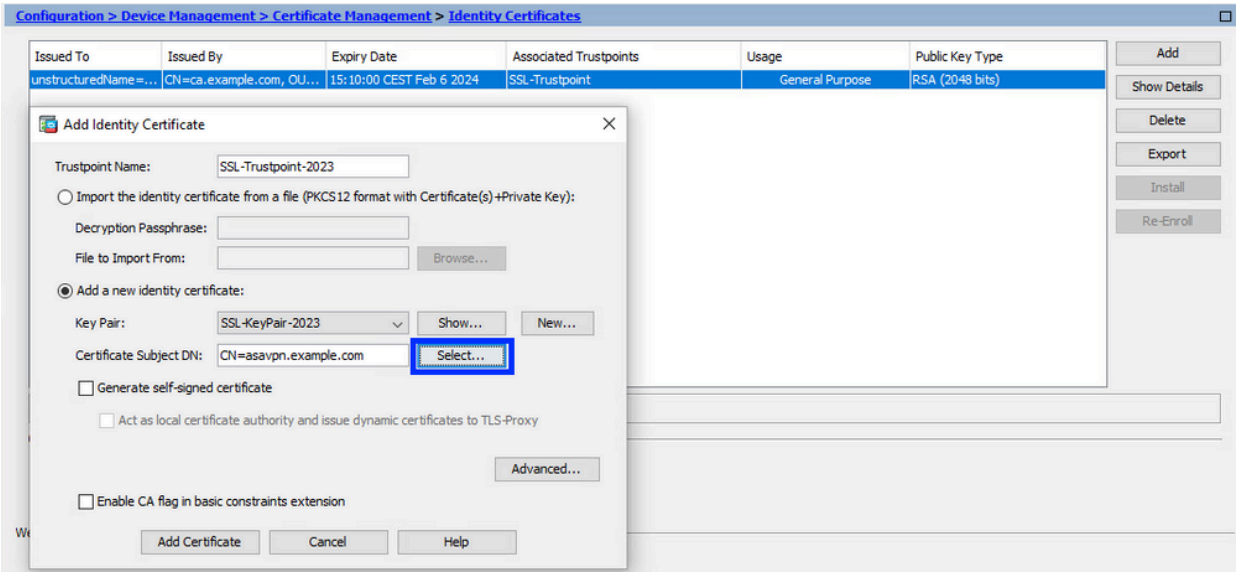
4. 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定

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。このパラメーターは、証明書のサブジェクト代替名(SAN)を設定します。SANフィールドは、証明書が接続先のFQDNと一致するかどうかを確認するためにSSL/TLS/IKEv2クライアントによって使用されます。

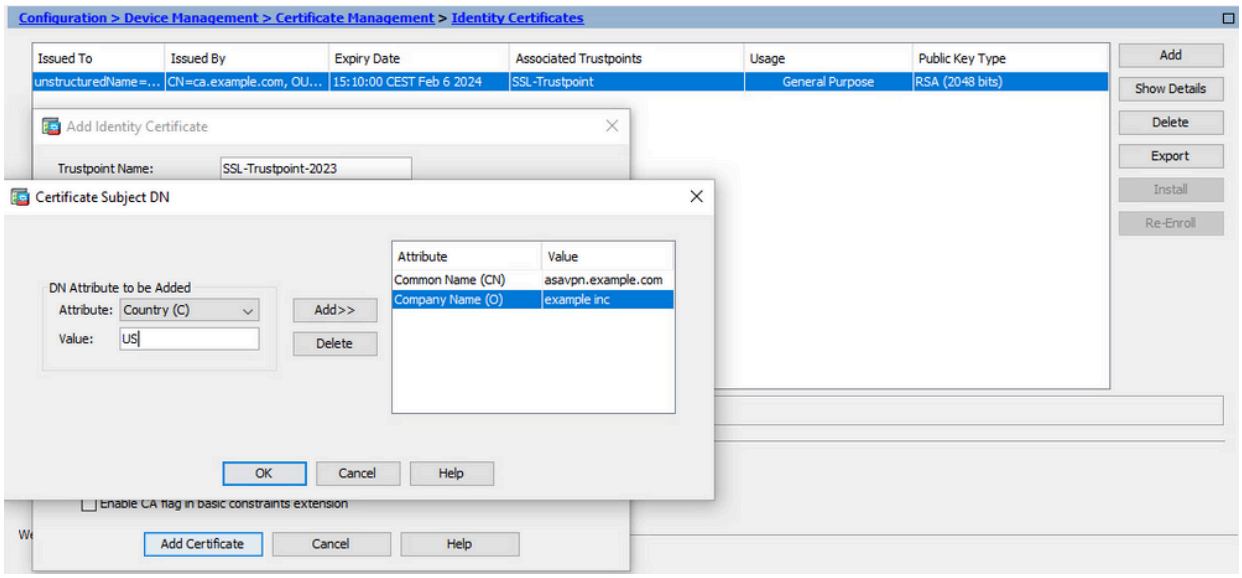
注：CAは、CSRに署名して署名付きID証明書を作成するときに、トラストポイントで定義されているFQDNパラメータとサブジェクト名パラメータを変更できます。

---

a. [Select] をクリックします。



b. Certificate Subject DNウィンドウで、certificate attributes - select attribute fromドロップダウンリストを設定し、値を入力して、Addをクリックします。

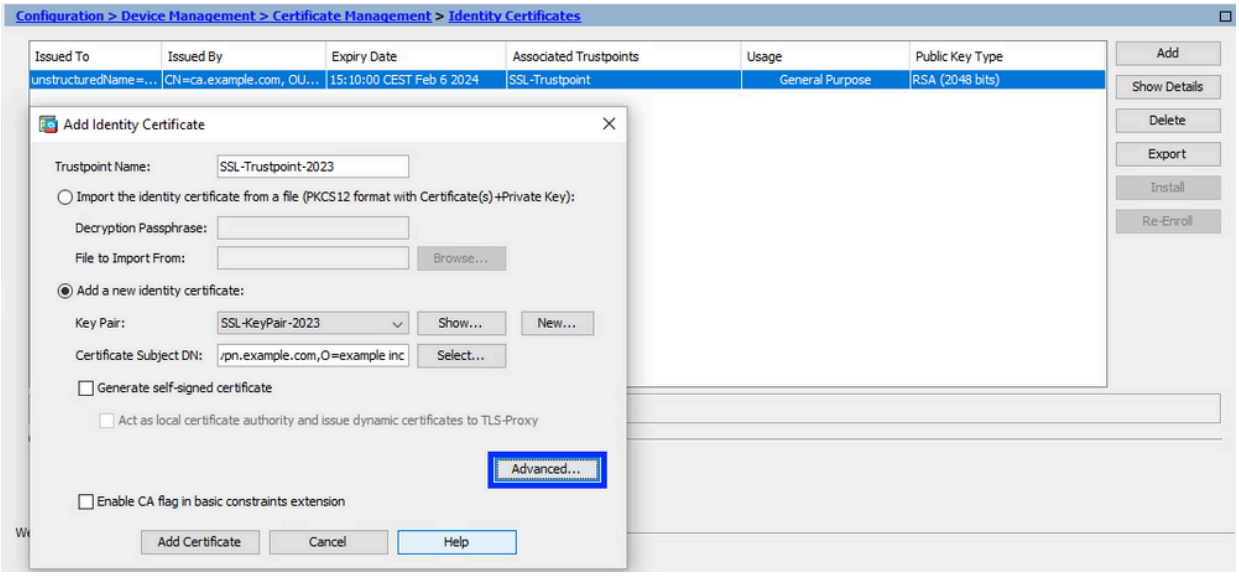


Attribute	説明
CN	ファイアウォールへのアクセスに使用される名前(通常は、vpn.example.comなどの完全修飾ドメイン名)。
OU	組織内の部署の名前
O	法的に登録されている組織/会社の名前
C	国コード（句読点のない 2 文字のコード）
ST	組織の所在する都道府県。
起	組織が所在する市区町村。
EA	電子メールアドレス

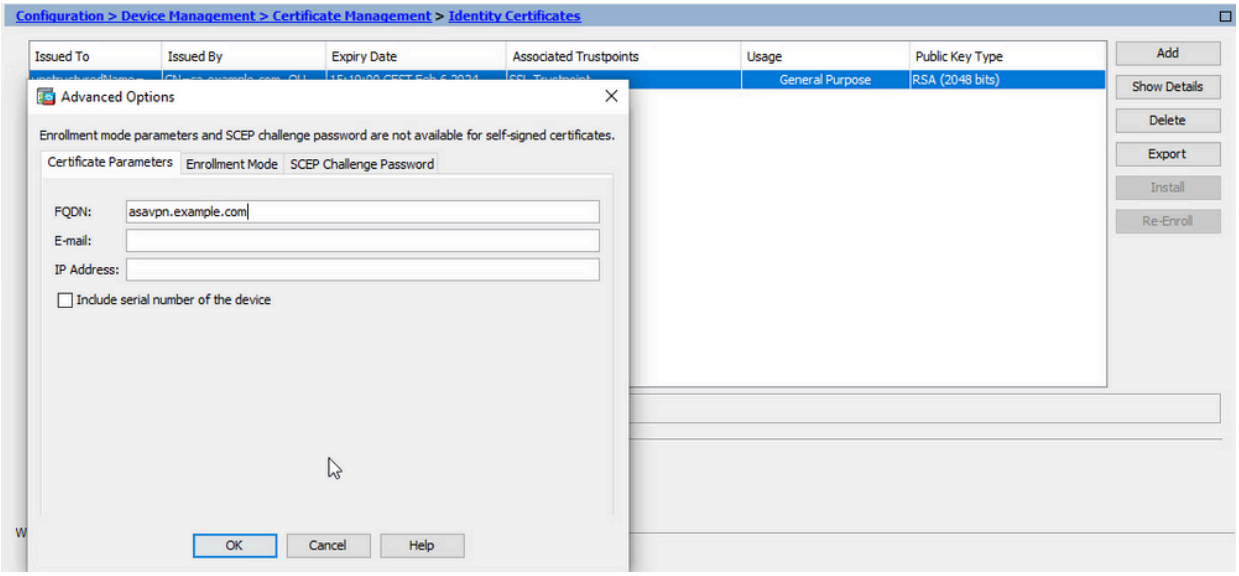
注：上記のフィールドはいずれも、64文字の制限を超えることはできません。この値を大きくすると、ID証明書のインストールで問題が発生する可能性があります。また、すべてのDN属性を定義する必要はありません。

すべての属性を追加したら、OKをクリックします。

c. デバイスのFQDNを設定するには、Advancedをクリックします。

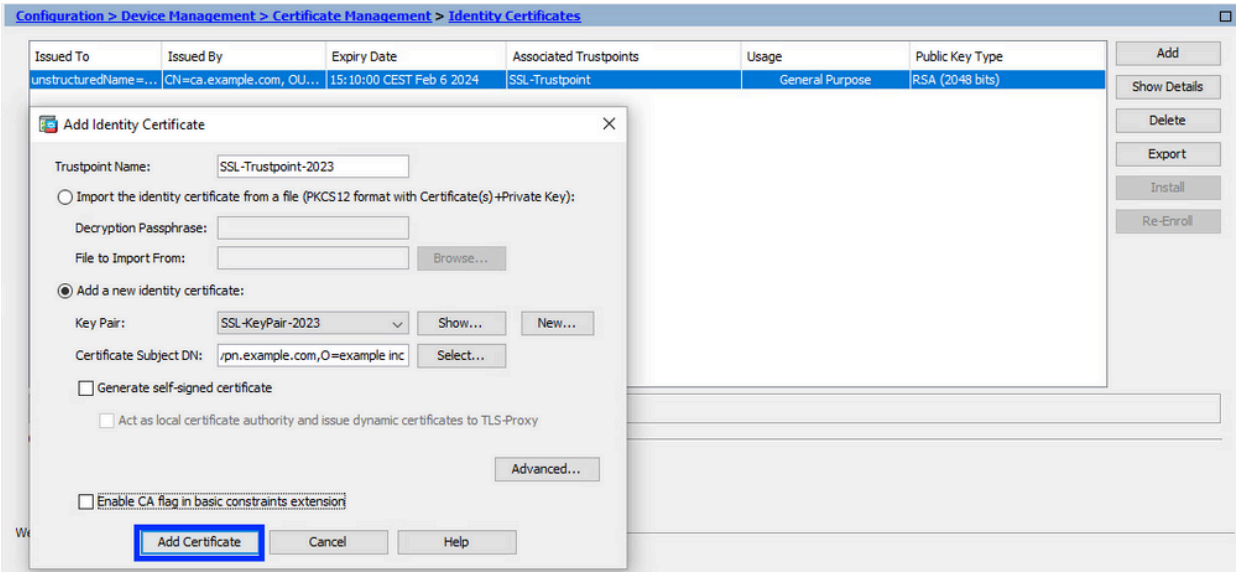


d. FQDNフィールドに、デバイスがインターネットからアクセス可能な完全修飾ドメイン名を入力します。[OK] をクリックします。

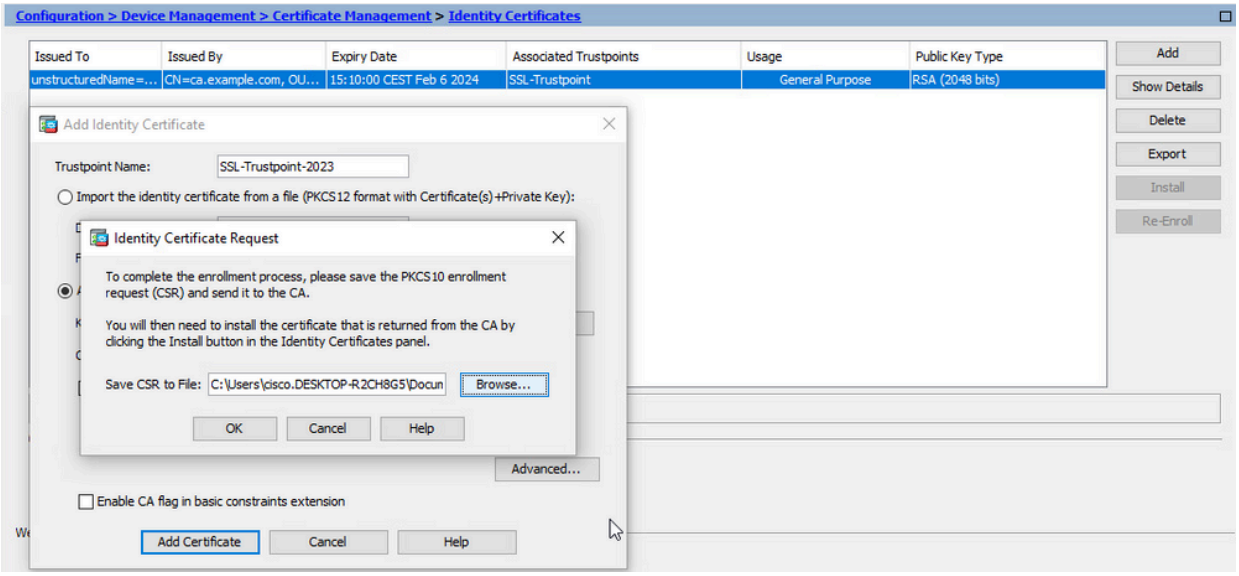


5. CSRの生成と保存

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



b. CSR をローカル マシン上のファイルに保存するためのプロンプトが表示されます。

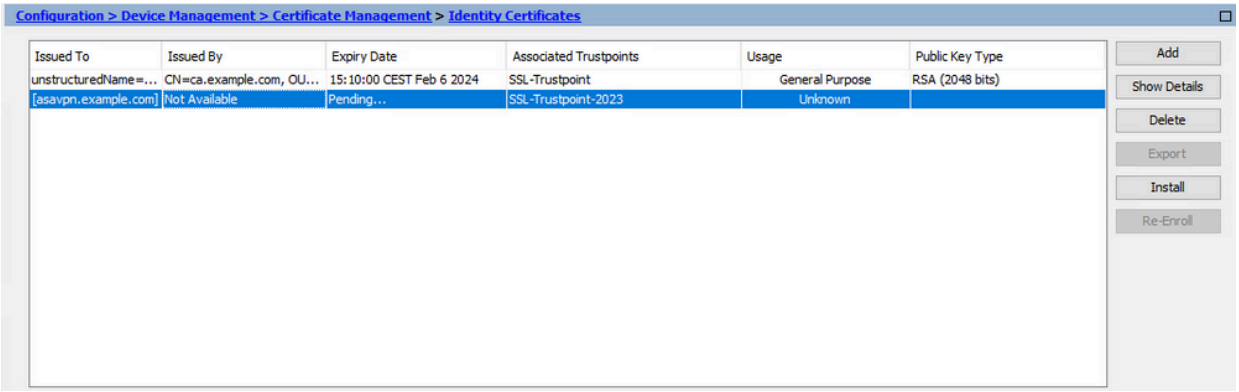


[Browse] をクリックします。 CSRを保存する場所を選択し、.txt拡張子を付けてファイルを保存します。

注：ファイルを.txt拡張子で保存すると、PKCS#10要求をテキストエディタ（メモ帳など）で開いて表示できます。

---

c. 新しいトラストポイントがPending状態で表示されます。



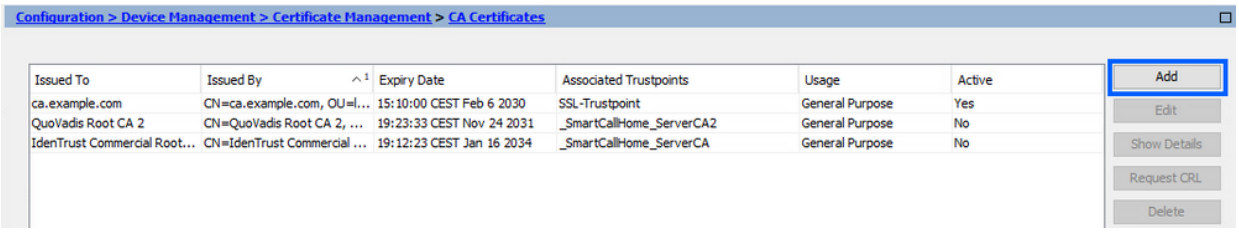
ASDMを使用したPEM形式でのID証明書のインストール

インストール手順では、CAがCSRに署名し、PEMエンコード(.pem、.cer、.crt)された新しいID証明書およびCA証明書バンドルが提供されていることを前提としています。

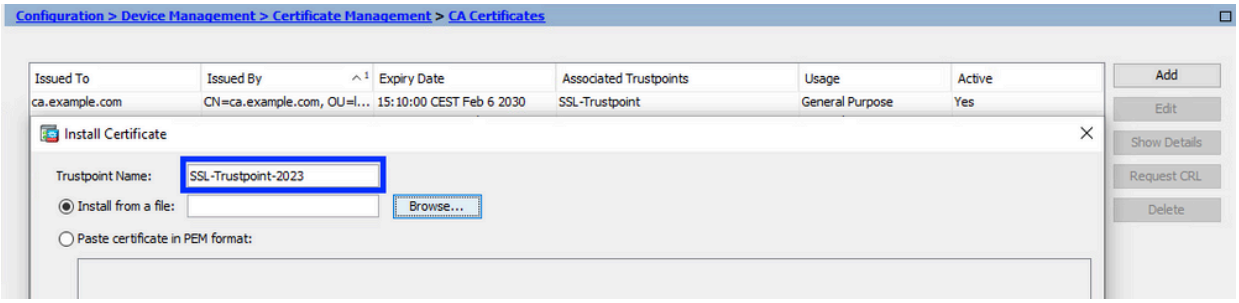
1. CSRに署名したCA証明書のインストール

   ID証明書に署名したCA証明書は、ID証明書用に作成されたトラストポイントにインストールできます。ID証明書が中間CAによって署名されている場合、このCA証明書をID証明書トラストポイントにインストールできます。階層内のアップストリームのすべてのCA証明書は、個別のCAトラストポイントにインストールできます。

   a. Configuration > Device Management >Certificate Management >の順に移動し、CA Certificatesを選択します。[Add] をクリックします。



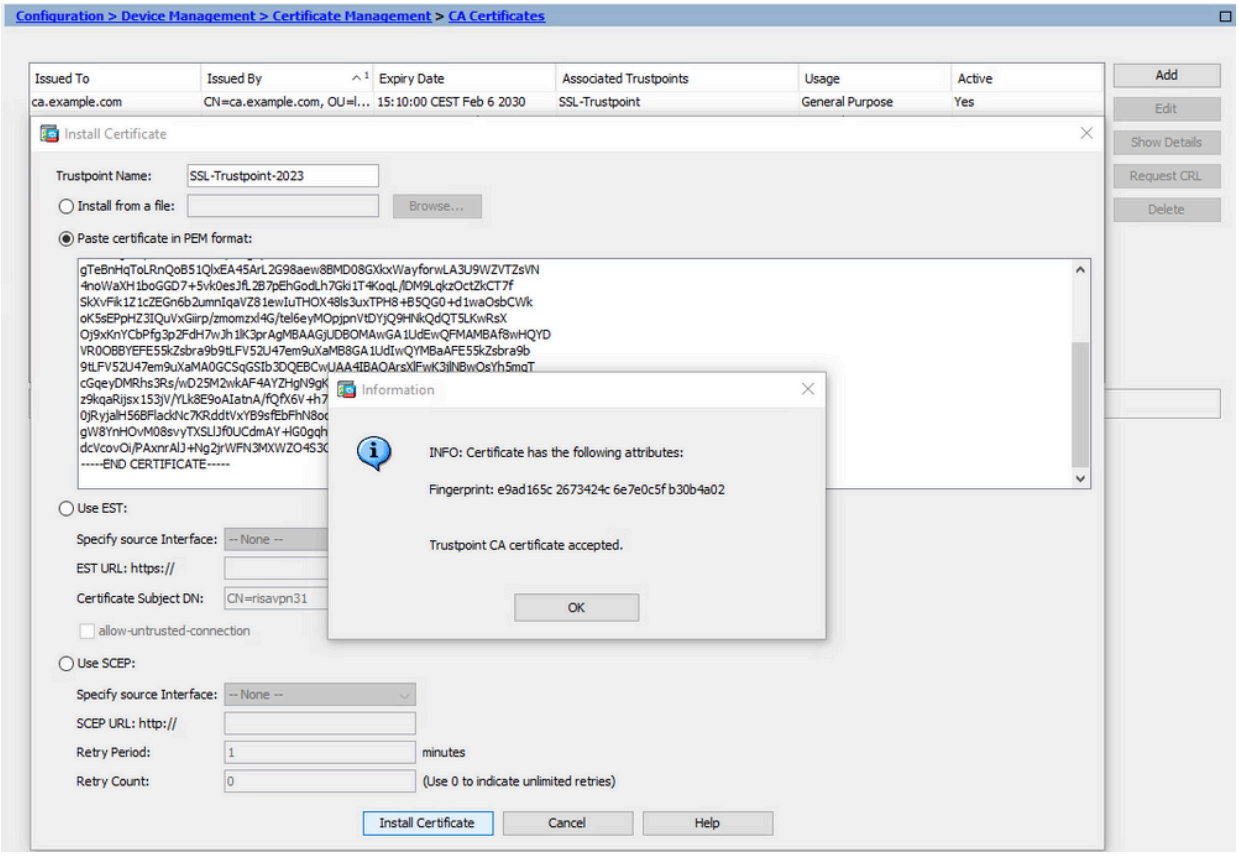
   b. トラストポイント名を入力し、Install From Fileを選択して、Browseボタンをクリックし、intermediate証明書を選択します。または、テキストファイルのPEMエンコードCA証明書をテキストフィールドに貼り付けます。



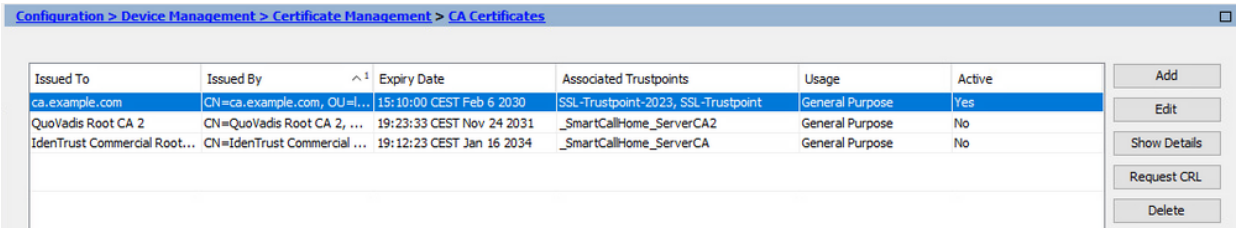
注:ID証明書が中間CA証明書によって署名されている場合は、ID証明書のトラストポイント名と同じトラストポイント名を持つ中間証明書をインストールします。

---

c. [Install Certificate] をクリックします。

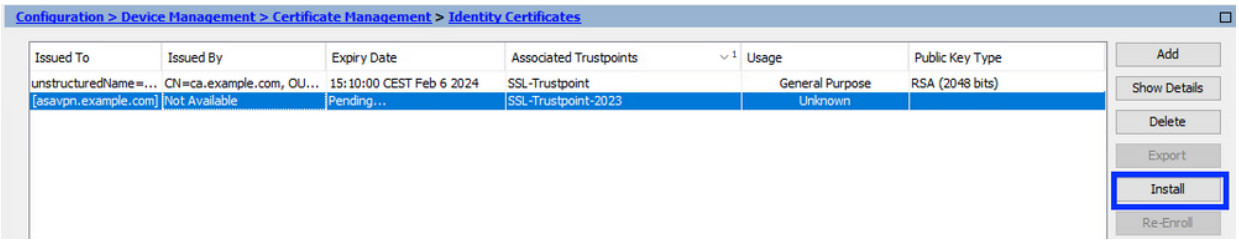


この例では、新しい証明書が古い証明書と同じCA証明書で署名されています。同じCA証明書が2つのトラストポイントに関連付けられました。



2. ID 証明書のインストール

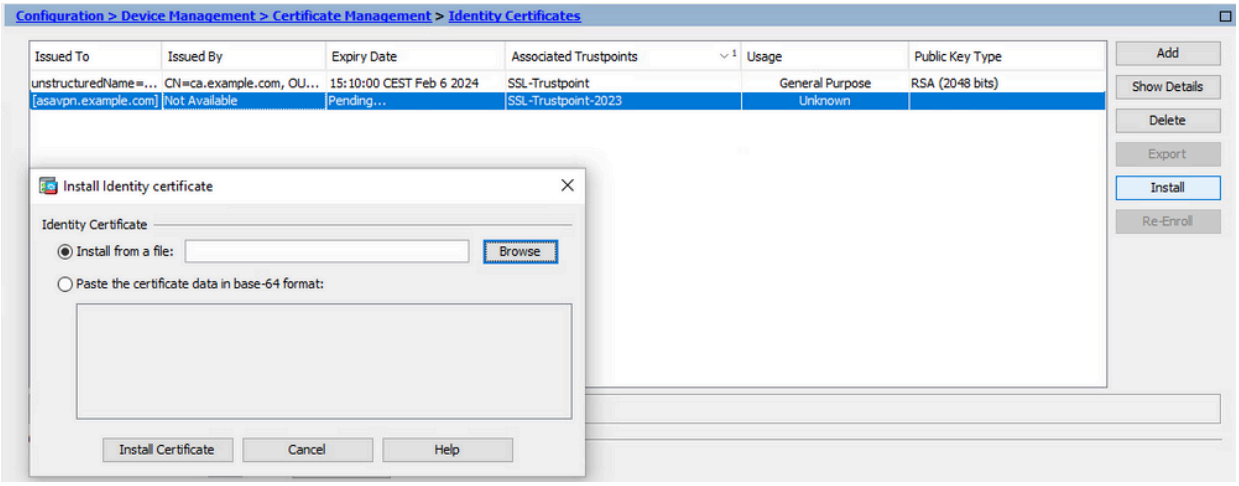
a. CSR生成で以前作成したID証明書を選択します。[INSTALL] をクリックします。



注:ID証明書では、Issued Byフィールドを Not available に、Expiry Dateフィールドを Pending に設定できます。

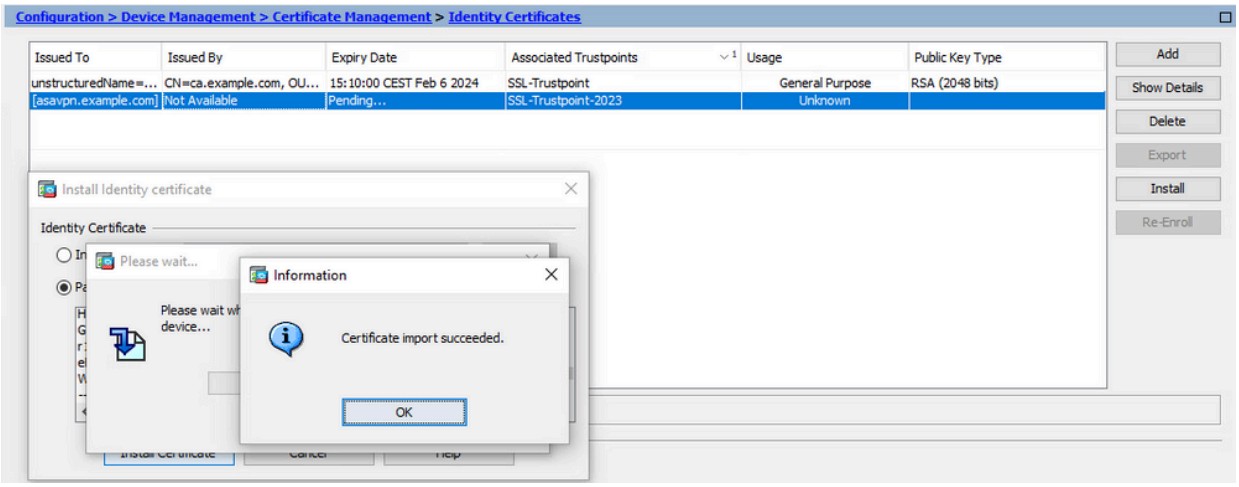
b. CAから受信したPEMでエンコードされたID証明書を含むファイルを選択するか、

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、CAから提供された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。

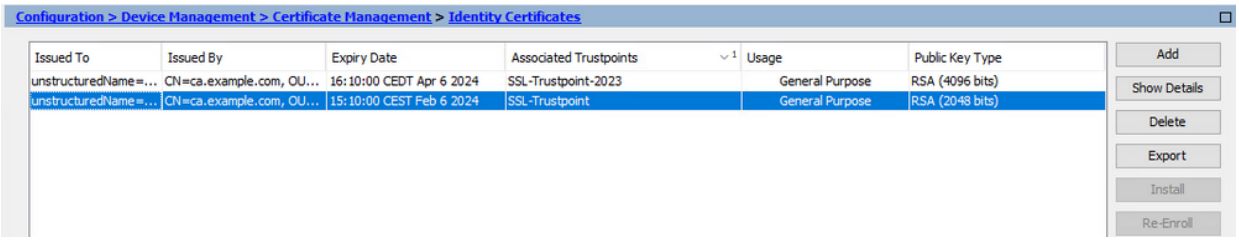


注:ID証明書は、.pem、.cer、.crt形式でインストールできます。

c. [Install Certificate] をクリックします。



インストール後、古いID証明書と新しいID証明書が存在します。



3. ASDMを使用したインターフェイスへの新しい証明書のバインド

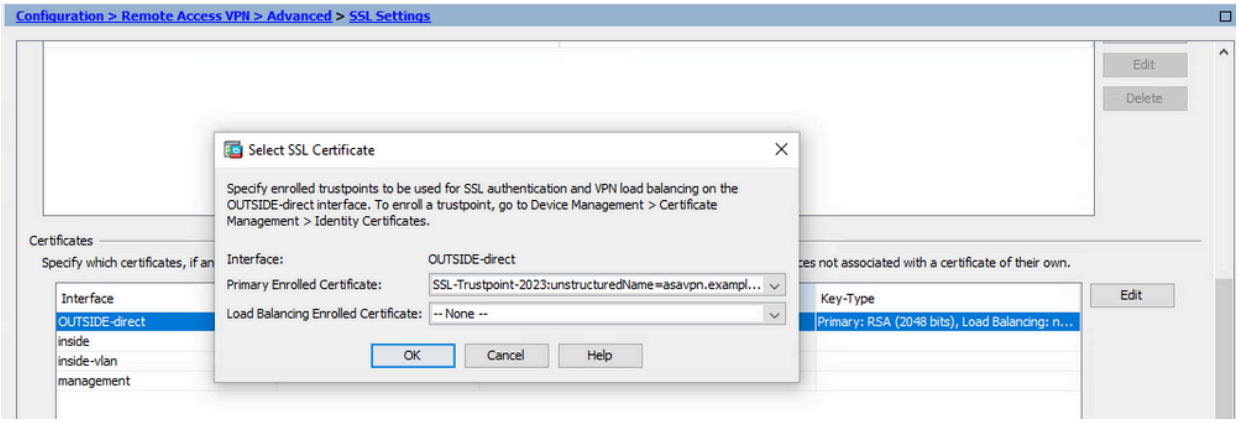
指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用するようにASAを設定する必要があります。

a. [構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [詳細（Advanced）] > [SSL設定（SSL Settings）] の順に移動します。

b. [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。

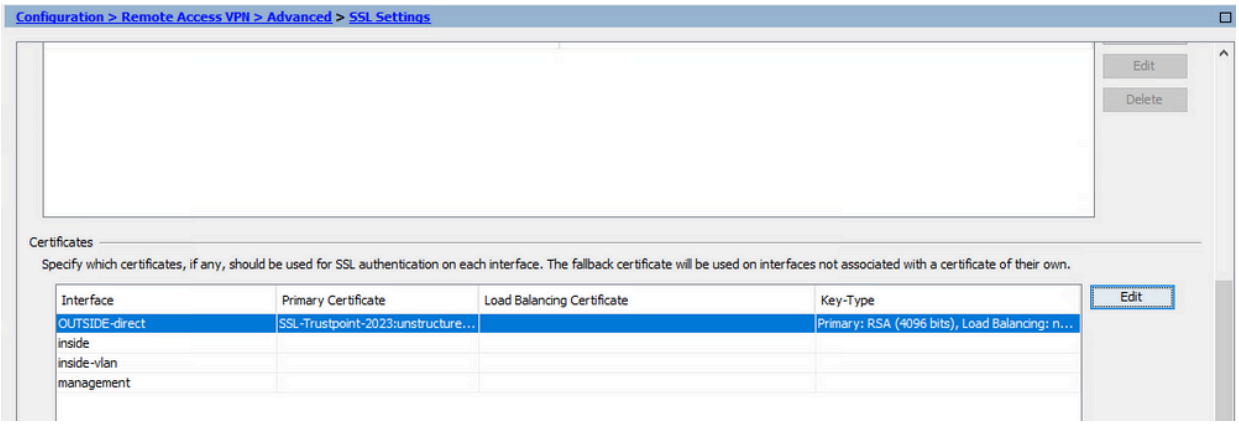
[Edit] をクリックします。

c. [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。



d. [OK] をクリックします。

e. [APPLY] をクリックします。これで、新しいID証明書が使用されています。



ASDMを使用したPKCS12ファイルに登録された証明書の更新

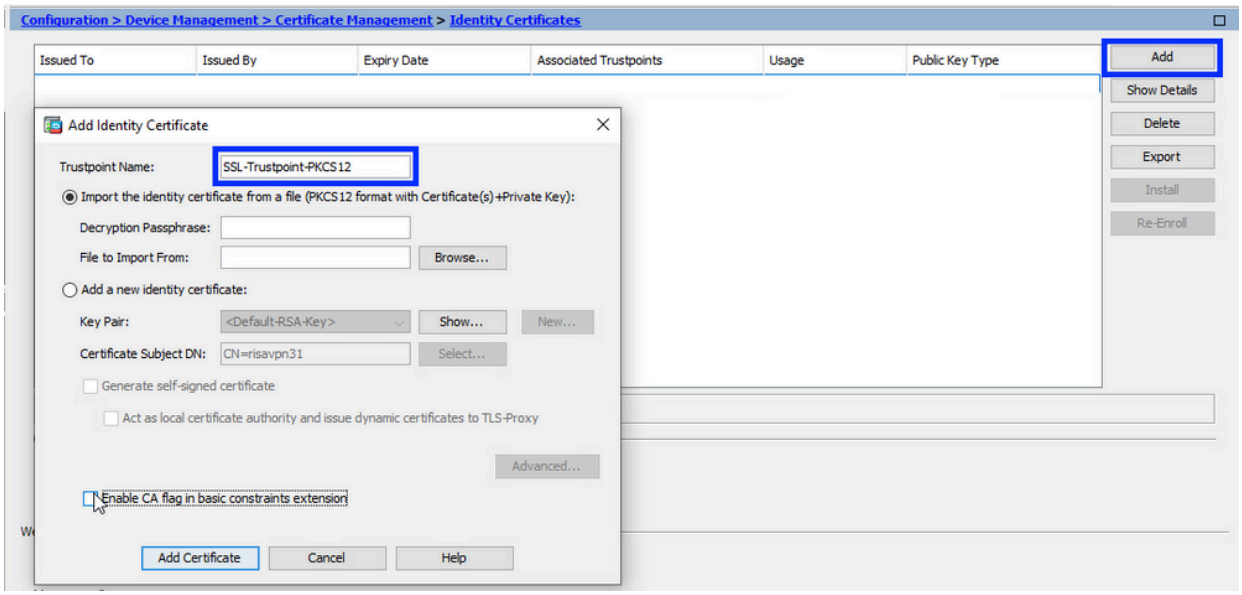
PKCS12登録済み証明書の証明書の更新では、新しいトラストポイントを作成して登録する必要があります。別の名前（登録年のサフィックスを持つ古い名前など）にする必要があります。

PKCS12ファイル（.p12または.pfx形式）には、ID証明書、キーペア、およびCA証明書が含まれています。これは、たとえばワイルドカード証明書の場合にCAによって作成されるか、または別のデバイスからエクスポートされます。これはバイナリファイルであり、テキストエディタでは表示できません。

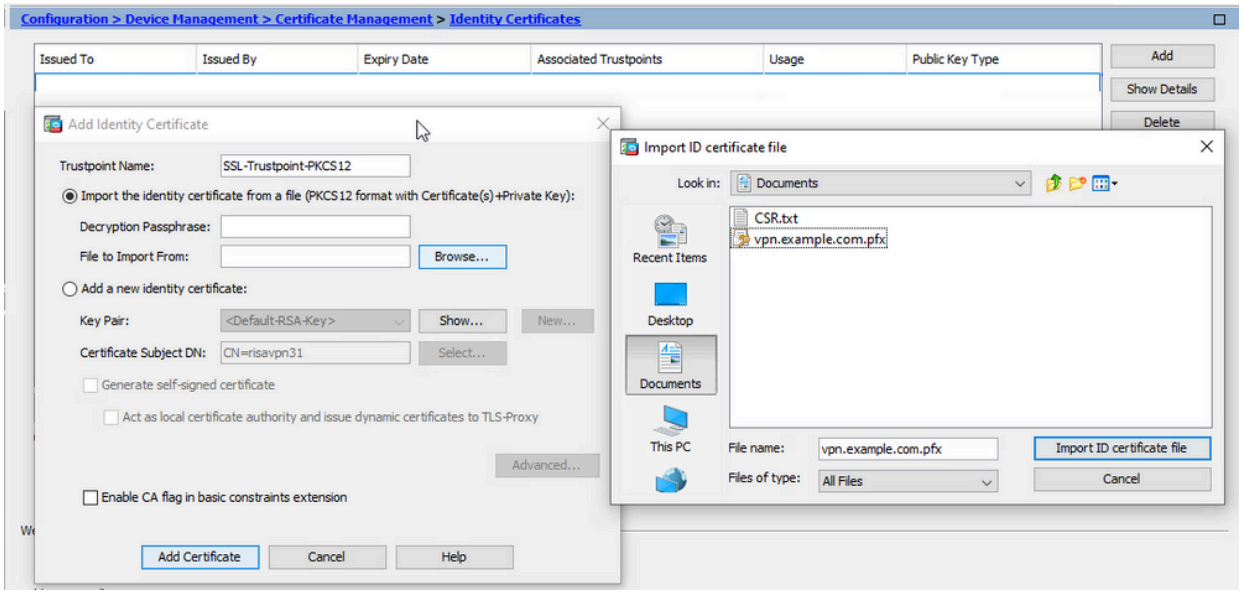
1. PKCS12ファイルからの更新されたID証明書とCA証明書のインストール

ID証明書、CA証明書、およびキーペアを1つのPKCS12ファイルにバンドルする必要があります。

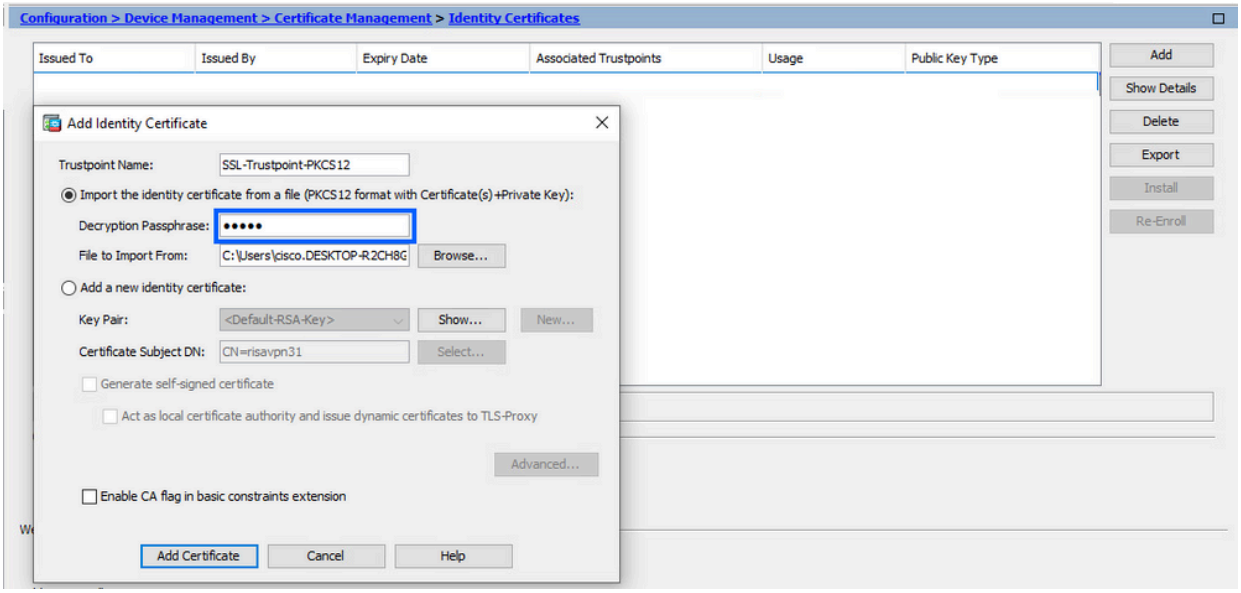
a. Configuration > Device Management > Certificate Managementの順に移動し、Identity Certificatesを選択します。
b. [Add] をクリックします。
c. 新しいトラストポイント名を指定します。



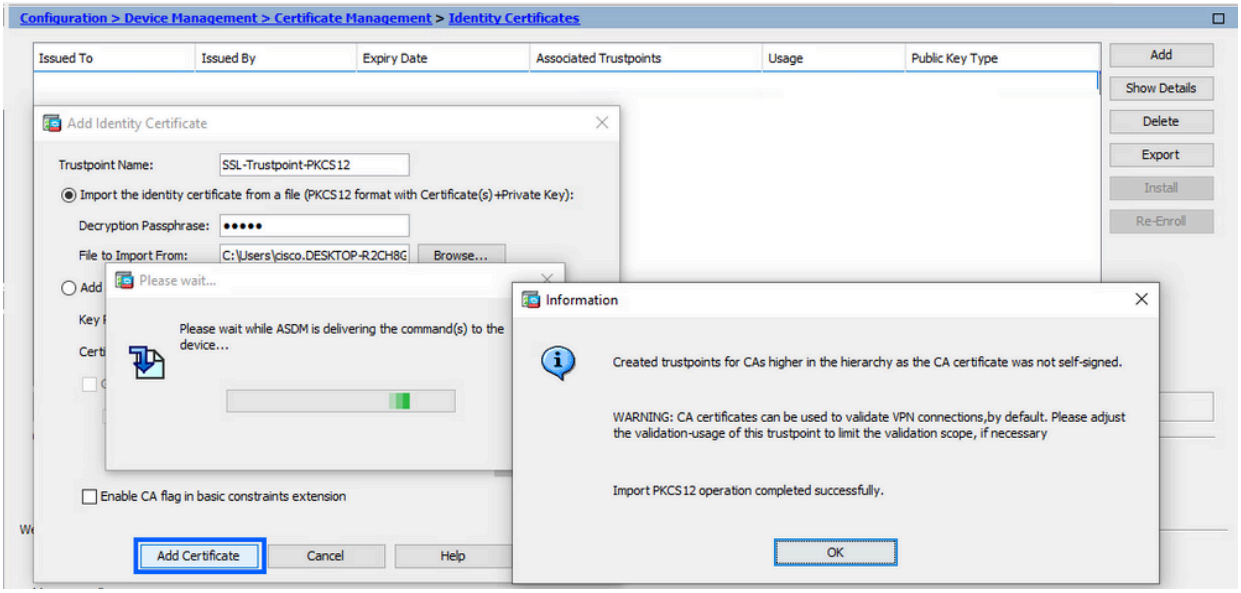
d. [アイデンティティ証明書をファイルからインポートする（Import the identity certificate from a file）] ラジオ ボタンをクリックします。



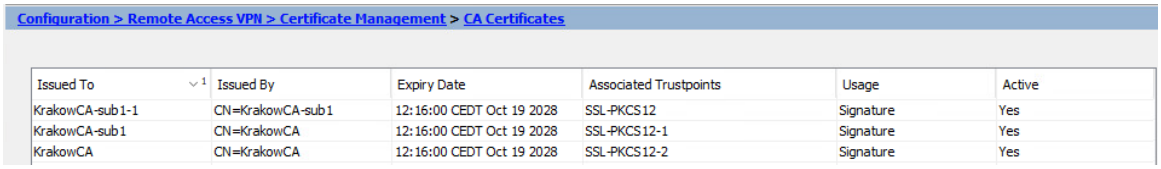
e. PKCS12 ファイルの作成に使用するパスフレーズを入力します。



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



注:CA証明書チェーンを持つPKCS12がインポートされると、ASDMは、追加された – numberサフィックスを持つ名前でアップストリームCAトラストポイントを自動的に作成します。



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用するようにASAを設定する必要があります。

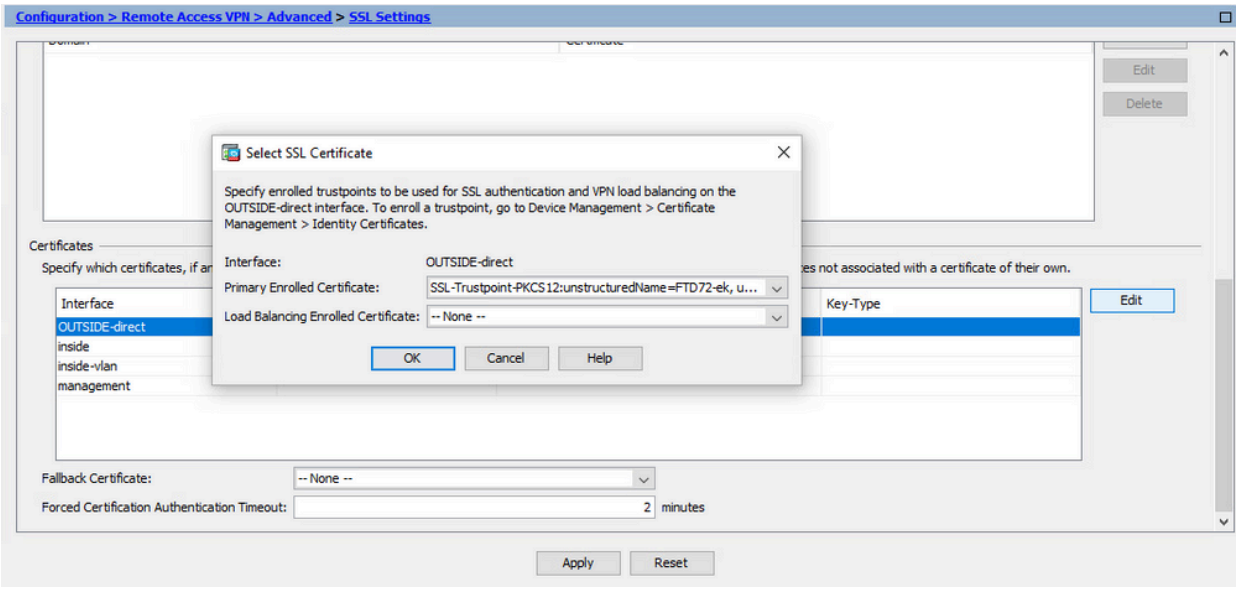
a. [構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [詳細

（Advanced）] > [SSL設定（SSL Settings）] の順に移動します。

b. [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。

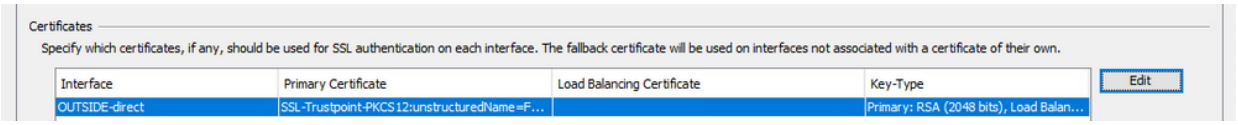
[Edit] をクリックします。

c. [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。



d. [OK] をクリックします。

e. [APPLY] をクリックします。



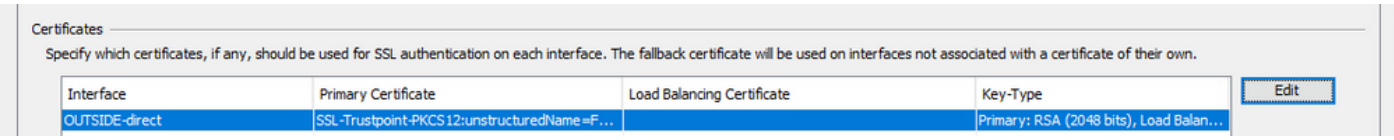
これで、新しいID証明書が使用されています。

確認

サードパーティベンダーの証明書が正常にインストールされたことを確認し、SSL VPN接続に使用するには、次の手順を使用します。

ASDM を使用してインストールされた証明書の表示

1. [構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] の順に移動して、[アイデンティティ証明書（Identity Certificates）] を選択します。
2. サードパーティベンダーによって発行されたID証明書が表示される場合があります。



トラブルシュート

このdebugコマンドは、SSL証明書のインストールが失敗した場合にCLIで収集されます。

- debug crypto ca 14

よく寄せられる質問（FAQ）

Q. PKCS12とは何ですか。
A.暗号化では、PKCS12は、多数の暗号化オブジェクトを1つのファイルとして保存するために作成されるアーカイブファイル形式を定義します。通常、秘密キーをX.509証明書とバンドルしたり、信頼のチェーンのすべてのメンバーをバンドルしたりするために使用されます。

Q. CSRとは何ですか。
A.Public Key Infrastructure（PKI；公開キーインフラストラクチャ）システムでは、証明書署名要求（CSRまたは証明書要求）は、デジタルID証明書を申請するために申請者から公開キーインフラストラクチャの登録機関に送信されるメッセージです。通常は、証明書を発行できる公開キー、署名付き証明書を識別するために使用される情報（サブジェクト内のドメイン名など）、および整合性の保護（デジタル署名など）が含まれます。

Q. PKCS12のパスワードはどこにありますか。
A.証明書とキーペアがPKCS12ファイルにエクスポートされる際に、パスワードはexportコマンドで指定されます。 pkcs12ファイルをインポートするには、CAサーバの所有者または別のデバイスからPKCS12をエクスポートしたユーザがパスワードを提供する必要があります。

Q.ルートとアイデンティティの違いは何ですか。
A.暗号化とコンピュータセキュリティでは、ルート証明書はルート認証局(CA)を識別する公開キー証明書です。ルート証明書は自己署名され（証明書がクロス署名されたルートによって発行されたかなど、複数の信頼パスを持つことが可能です）、X.509ベースの公開キーインフラストラクチャ(PKI)の基盤を形成します。公開鍵証明書は、デジタル証明書またはID証明書とも呼ばれ、公開鍵の所有権を証明するために使用される電子文書です。証明書には、キーに関する情報、所有者の身元に関する情報（サブジェクトと呼ばれます）、証明書の内容を検証したエンティティのデジタル署名（発行者と呼ばれます）が含まれます。署名が有効で、証明書を検査するソフトウェアが発行者を信頼する場合、そのキーを使用して証明書のサブジェクトと安全に通信できます。

Q.証明書をインストールしましたが、なぜそれが機能しないのですか。
A.これは、次のようなさまざまな原因が考えられます。

1.証明書とトラストポイントが設定されているが、それらを使用する必要があるプロセスにバインドされていない。 たとえば、使用されるトラストポイントは、Anyconnectクライアントを終

端する外部インターフェイスにバインドされません。

2. PKCS12ファイルがインストールされていますが、中間CA証明書がPKCS12ファイルにないため、エラーが発生します。中間CA証明書を信頼できる証明書として持つが、ルートCA証明書を信頼できないクライアントは、証明書チェーン全体を検証できず、サーバID証明書を信頼できないとして報告できません。

3.誤った属性が設定された証明書は、インストール障害またはクライアント側のエラーの原因となる可能性があります。たとえば、特定の属性が誤った形式でエンコードされている可能性があります。もう1つの理由は、ID証明書にサブジェクト代替名(SAN)がないか、サーバへのアクセスに使用されるドメイン名がSANとして存在しないことです。

Q.新しい証明書をインストールすると、メンテナンス期間が必要になるか、ダウンタイムが発生しますか。
A. 新しい証明書（IDまたはCA）のインストールに手間がかかることはないため、ダウンタイムが発生したり、メンテナンス期間が必要になることはありません。既存のサービスに対して新しい証明書を使用できるようにするには、変更が必要であり、変更要求/メンテナンスウィンドウが必要になる可能性があります。

Q.証明書を追加または変更すると、接続されているユーザの接続が切断される可能性がありますか。
A.いいえ、現在接続されているユーザの接続は維持されます。証明書は接続の確立時に使用されます。ユーザが再接続すると、新しい証明書が使用されます。

Q.ワイルドカードを使用してCSRを作成するにはどうすればよいですか。またはサブジェクトの別名(SAN)を選択してください。
A.現在、ASA/FTDはワイルドカードを使用してCSRを作成できませんが、このプロセスはOpenSSLで実行できます。CSRとIDキーを生成するには、次のコマンドを実行します。

```
openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new
```

トラストポイントに完全修飾ドメイン名(FQDN)属性が設定されている場合、ASA/FTDによって作成されるCSRには、その値を持つSANが含まれます。CSRに署名するときにCAが追加できるSAN属性が増えたり、OpenSSLでCSRを作成したりすることもできます

Q.証明書の置き換えは、すぐに有効になりますか。

A. 新しいサーバID証明書は、新しい接続にのみ使用されます。新しい証明書は、変更後すぐに使用できる状態になっていますが、実際には新しい接続で使用されます。

Q.インストールが正常に行われたかどうかを確認するには、どうすればよいですか。
A.確認するCLIコマンド：show crypto ca cert <trustpointname>

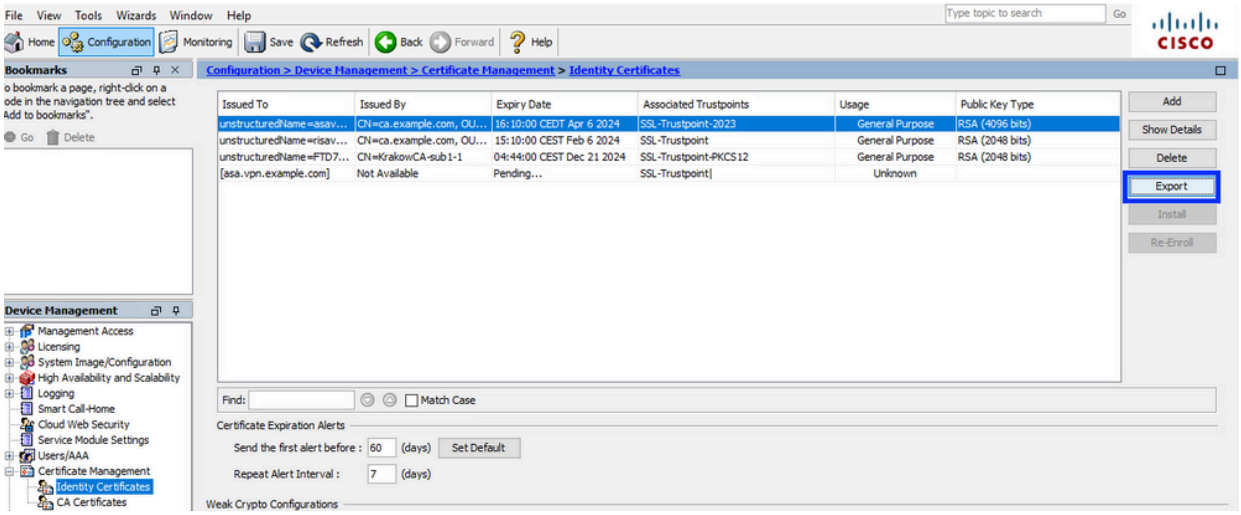
Q.ID証明書、CA証明書、および秘密キーからPKCS12を生成する方法は？
A. PKCS12は、次のコマンドを使用してOpenSSLで作成できます。

```
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt
```

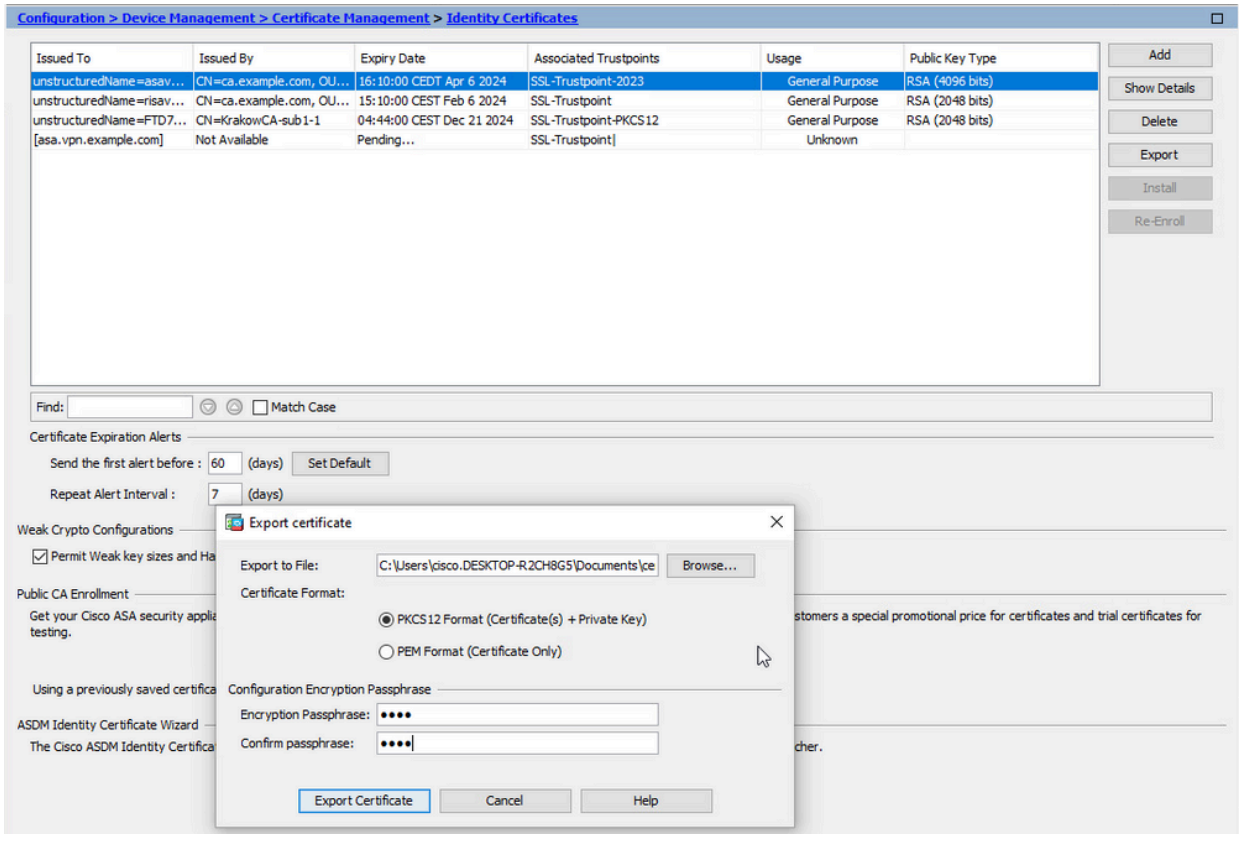
Q.証明書をエクスポートして新しいASAにインストールする方法は？
A.

- CLIを使用する場合：コマンドcrypto ca export <trustpointname> pkcs12 <password>
- ASDMを使用：

a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動し、Identity Certificateを選択します。[Export] をクリックします。



b. ファイルのエクスポート先を選択し、エクスポートパスワードを指定して、Export Certificateをクリックします。



エクスポートされた証明書は、コンピュータのディスクに保存できます。安全な場所でパスフレーズを書き留めてください、ファイルはそれなしで役に立ちません。

Q. ECDSAキーを使用する場合、SSL証明書の生成プロセスは異なりますか。
A.設定の唯一の違いは、キーペア生成の手順です。この手順では、RSAキーペアの代わりにECDSAキーペアを生成できます。手順のそれ以外の部分は変わりません。

Q.新しいキーペアを生成する必要は常にありますか。
A.キーペアの生成手順はオプションです。既存のキーペアを使用することも、PKCS12の場合は証明書と一緒にキーペアをインポートすることもできます。それぞれの登録/再登録タイプについては、「キーペア名の選択」セクションを参照してください。

Q.新しいID証明書の新しいキーペアを生成しても安全ですか。
A.新しいキーペア名が使用されている限り、プロセスは安全です。この場合、古いキーペアは変更されません。

Q.ファイアウォールを交換する（RMAなど）際にキーを再生成する必要がありますか。
A.設計上の新しいファイアウォールには、古いファイアウォールに存在するキーペアはありません。
実行コンフィギュレーションのバックアップには、キーペアは含まれません。
ASDMで実行される完全バックアップには、キーペアを含めることができます。
ID証明書は、ASDMまたはCLIを使用して、失敗する前にASAからエクスポートできます。
フェールオーバーペアの場合、証明書とキーペアはwrite standbyコマンドを使用してスタンバイユニットに同期されます。フェールオーバーペアの1つのノードが交換された場合は、基本的なフェールオーバーを設定し、新しいデバイスに設定をプッシュするだけで十分です。
キーペアがデバイスで失われ、バックアップがない場合は、新しいデバイスに存在するキーペアで新しい証明書に署名する必要があります。

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。