ASA 8.x： ASDM を使用した SSL 証明書の更新とインストール

目次

概要

このドキュメントの手順は、1 つの例であり、任意の証明書ベンダーまたは独自のルート証明書サーバを使用する場合のガイドラインとして使用できます。 証明書ベンダーが特定の証明書パラメータ要件を必要とすることがありますが、本ドキュメントの目的は SSL 証明書更新および 8.0 ソフトウェアを使用する ASA へのインストールのための一般的な手順を示すことです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この手順は、ASA バージョン 8.x および ASDM バージョン 6.0(2) 以降に適用されます。

本ドキュメントの手順は、証明書がインストールされ SSL VPN アクセスに使用される、有効な設定に基づいています。 この手順は、現在の証明書を削除しない限りネットワークに影響を与えません。 手順では、オリジナルのルート CA を発行したものと同じルート証明書を使用して、現在の証明書の新しい CSR を発行する方法をステップごとに説明します。

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たものです。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

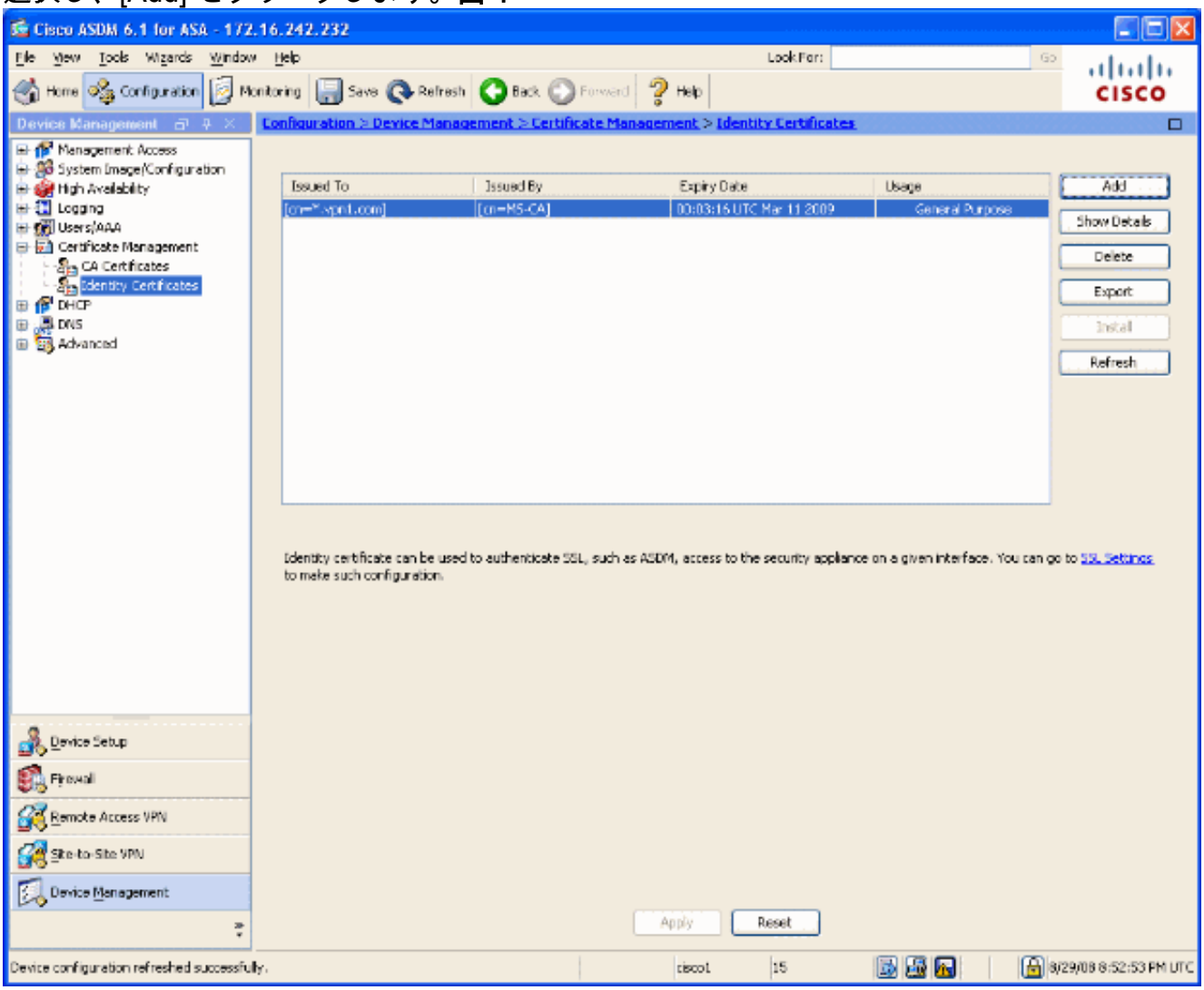
表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

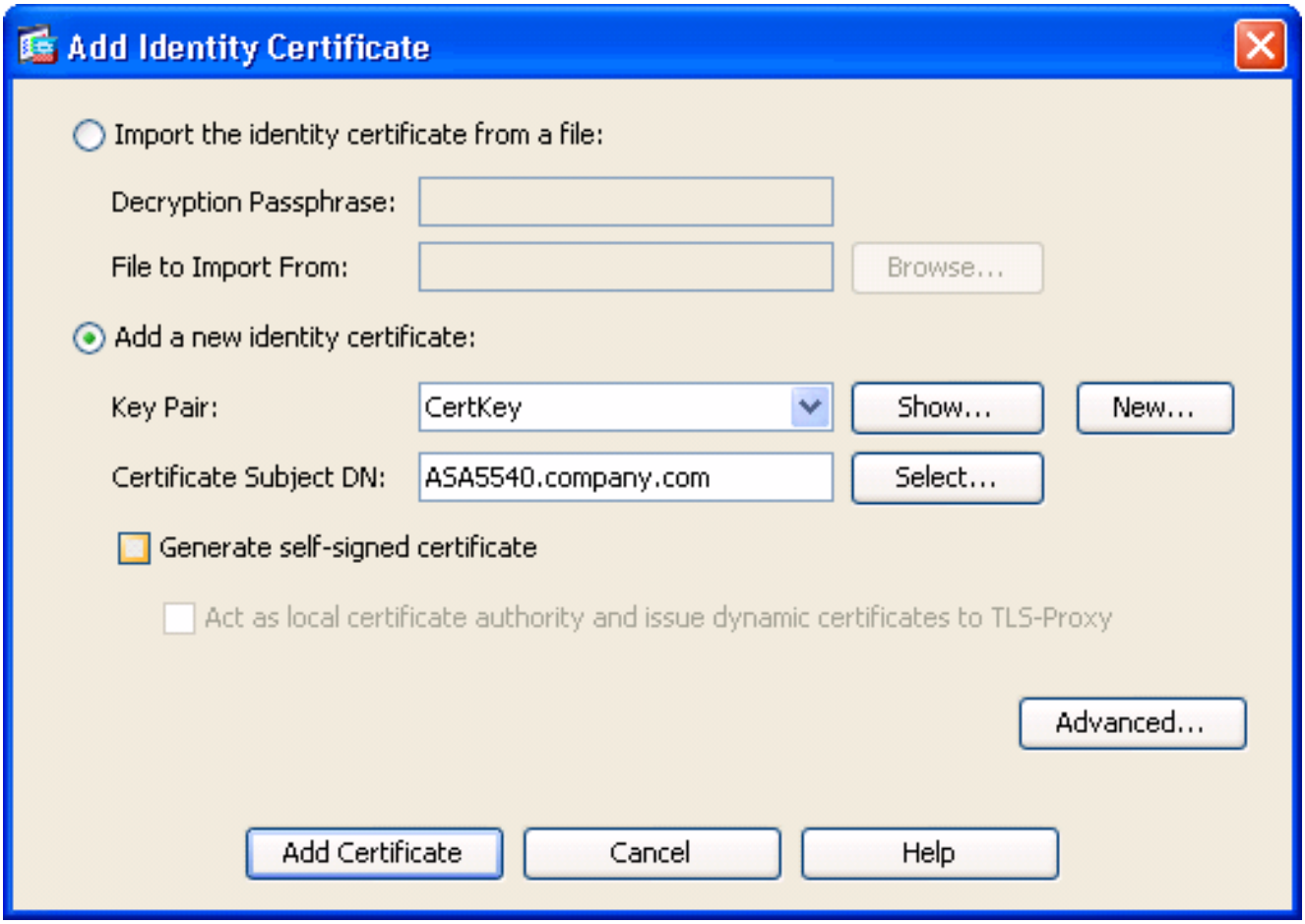
手順

次の手順を実行します。

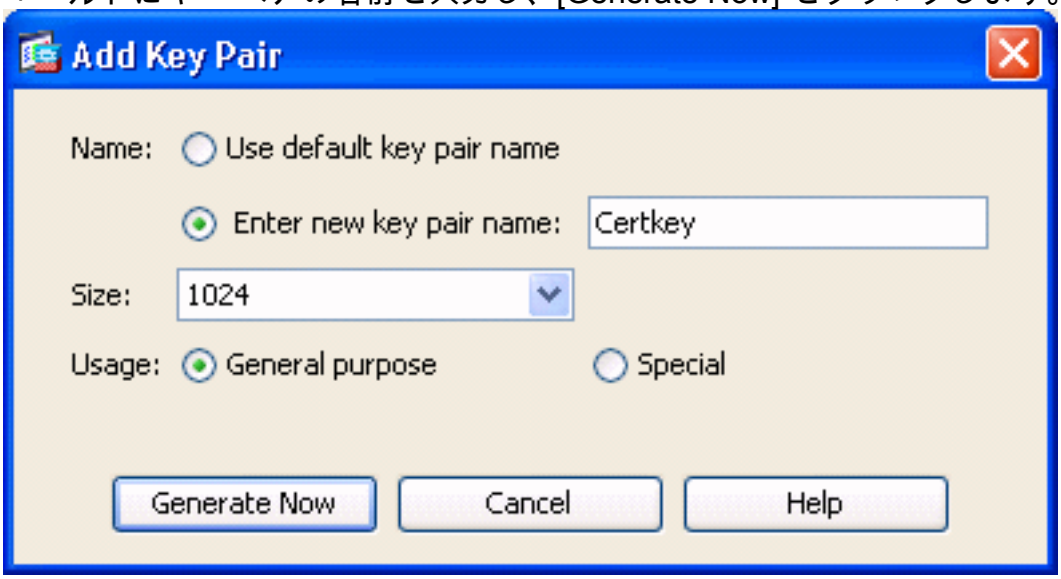
1. 更新する証明書の下の [Configuration] > [Device Management] > [Identity Certificates] を順に選択し、[Add] をクリックします。**図 1**



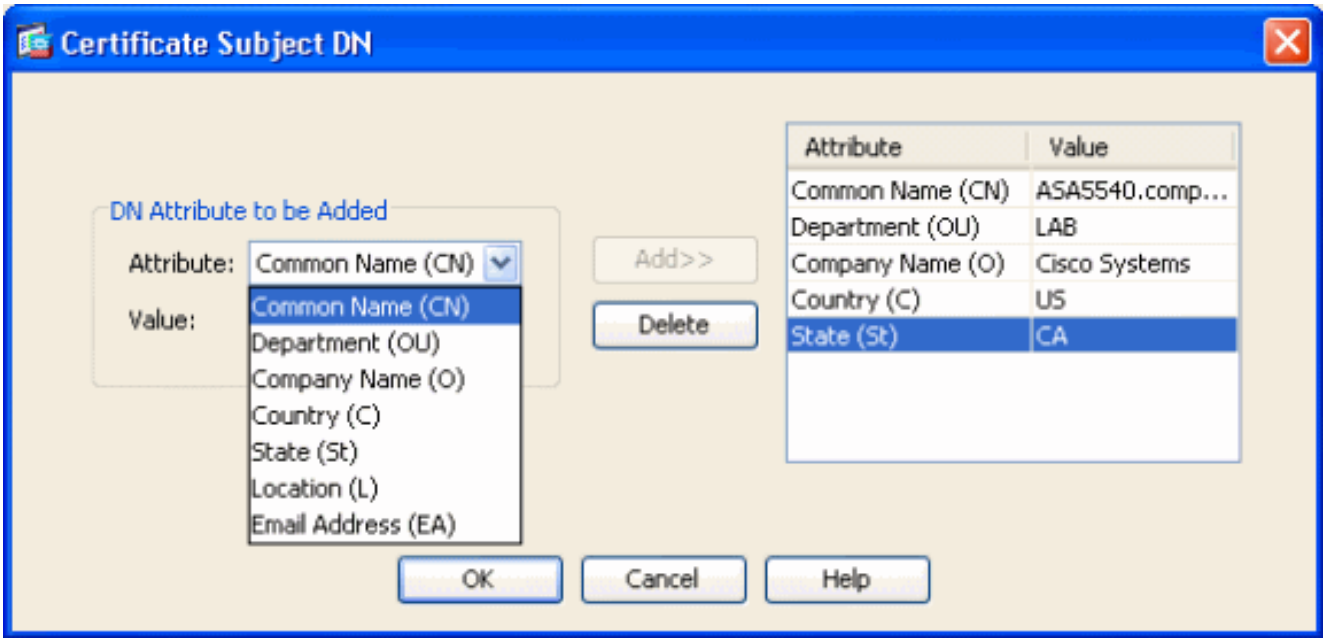
2. [Add Identity Certificate] で、[Add a new identity certificate] オプション ボタンを選択し、ドロップダウン メニューからキー ペアを選択します。**注:** ご利用の SSH キーを再生成するとその証明書が無効になるため、<Default-RSA-Key> を使用することは推奨されません。RSA キーがない場合は、ステップ a と b を実行します。 それ以外の場合は、ステップ 3 に進みます。**図 2**



（オプション）RSA キーがまだ設定されていない場合は、次のステップを実行し、それ以外の場合はステップ 3 に進みます。[New] をクリックします。[Enter new key pair name] フィールドにキー ペアの名前を入力し、[Generate Now] をクリックします。**図3**



3. [Select] をクリックします。
4. 図 4 に示すように、該当する証明書の属性を入力します。 終了したら、[OK] をクリックします。 次に、[Add Certificate] をクリックします。**図 4**



CLI の出力：

```
crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```

5. [Identity Certificate Request] ポップアップ ウィンドウで、Certificate Signing Request（CSR; 証明書署名要求）をテキスト ファイルに保存し、[OK] をクリックします。

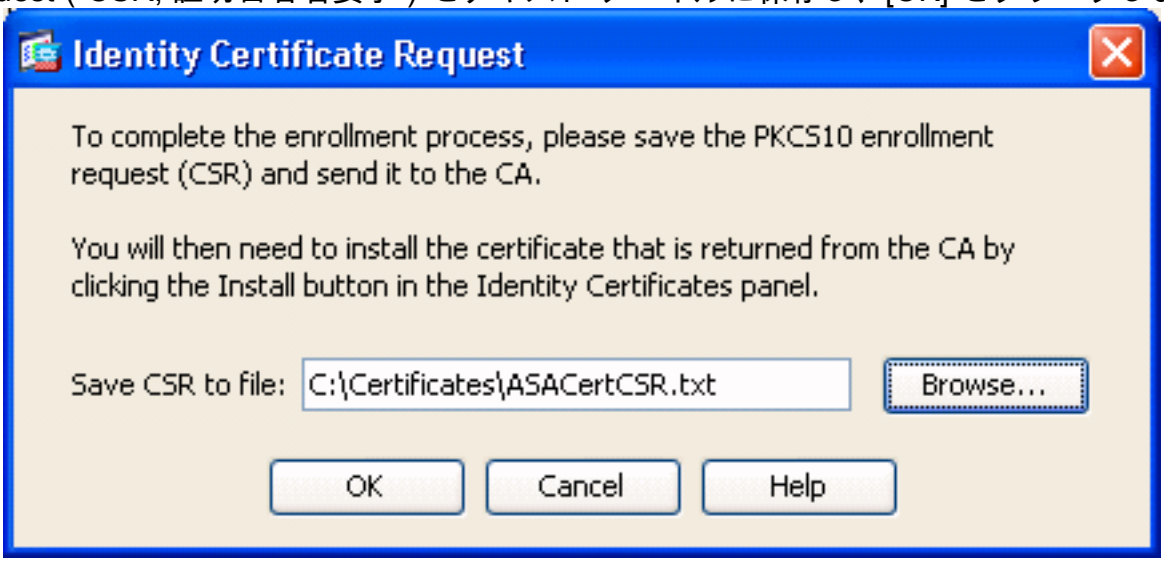
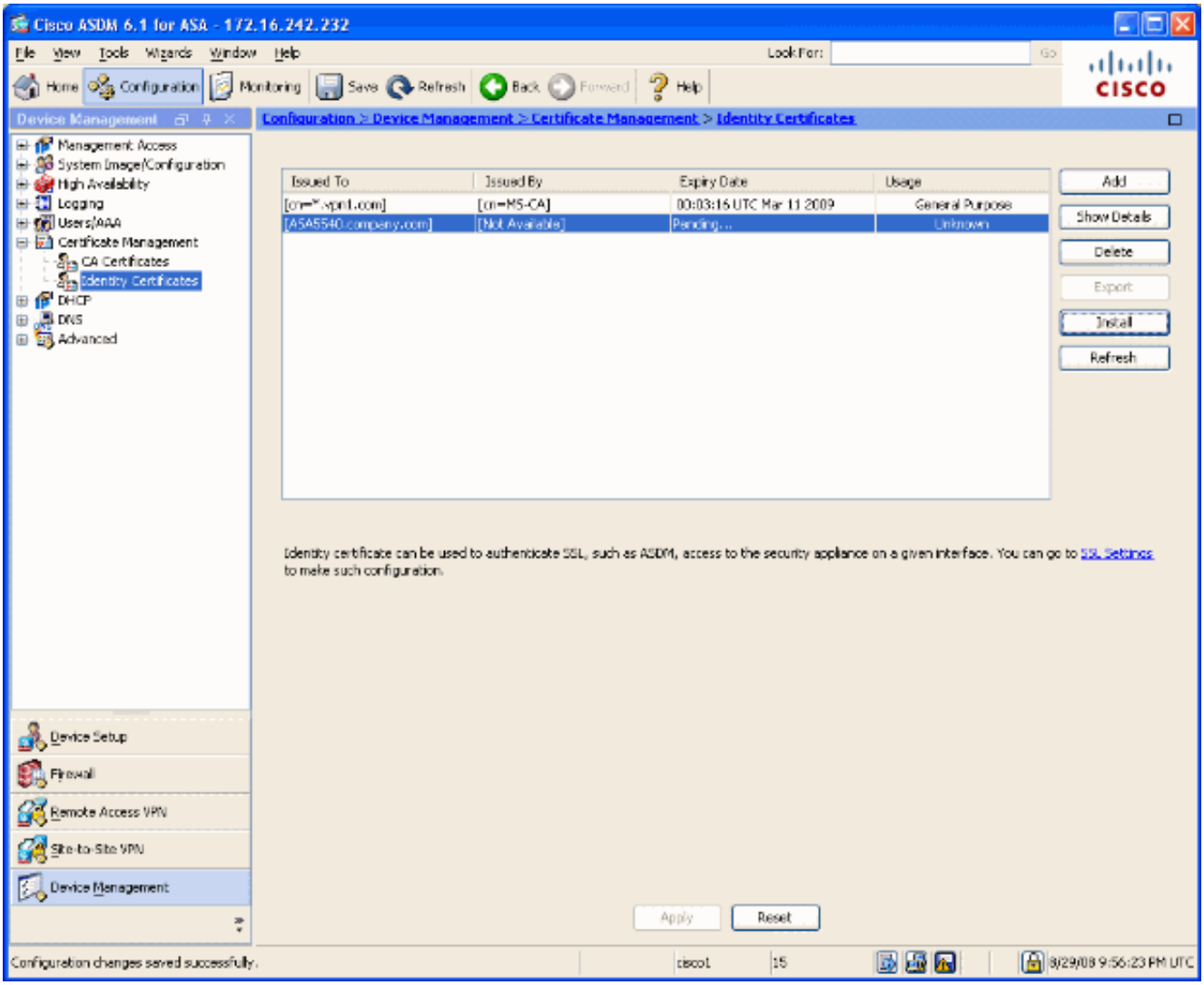
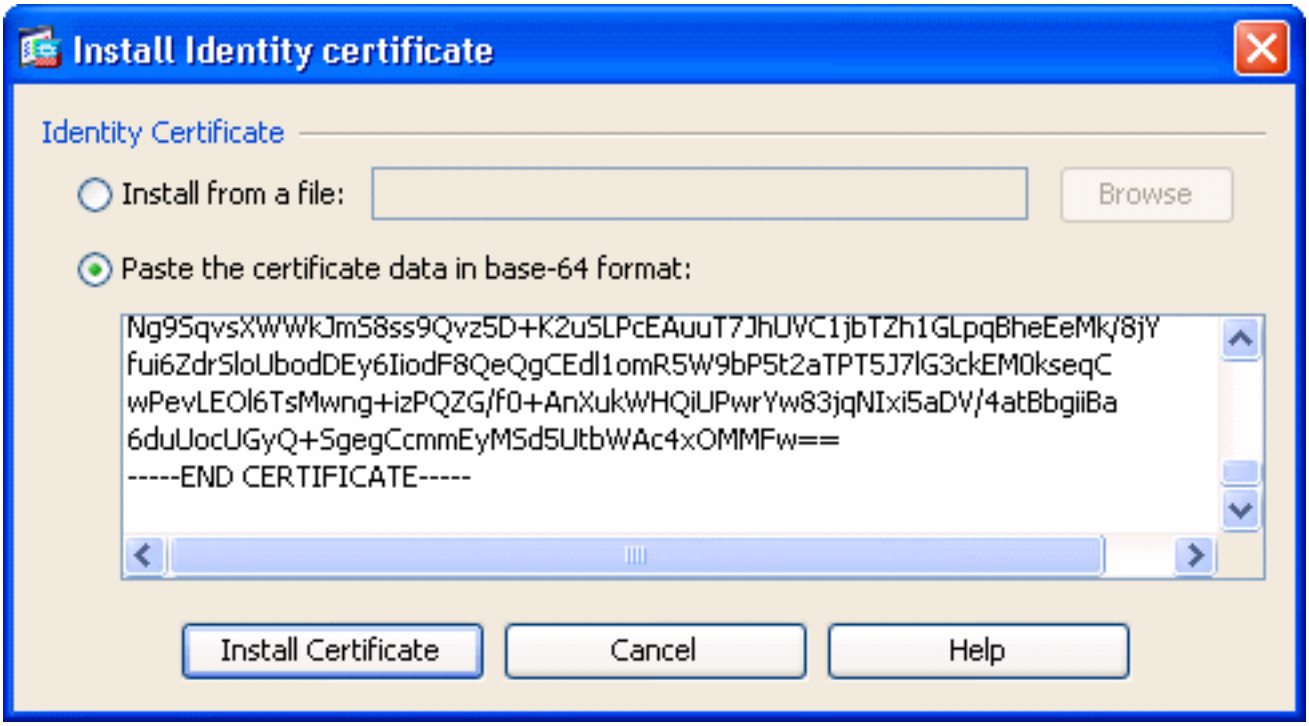


図 5

6. （オプション）図 6 に示すように、ASDM で CSR が保留中であることを確認します。**図 6**



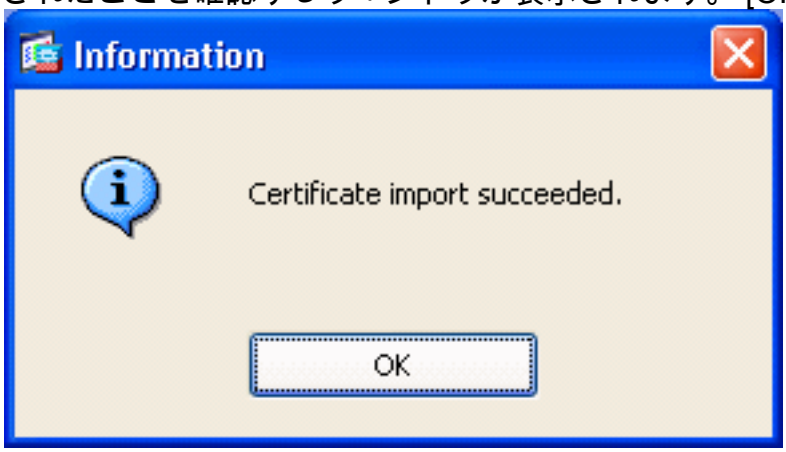
7. 証明書要求を証明書管理者に送信します。証明書管理者は、サーバで証明書を発行します。これは、Web インターフェイス、電子メールを使用しても可能であり、または直接、証明書発行プロセスのルート CA サーバへも送信できます。
8. 更新された証明書をインストールするには、次のステップを実行します。図 6 に示すように、[Configuration] > [Device Management] > [Identity Certificates] の下にある保留状態の証明書要求を選択し、[Install] をクリックします。[Install Identity Certificate] ウィンドウで、[Paste the certificate data in base-64 format] オプションボタンを選択し、[Install Certificate] をクリックします。**注:** あるいは、証明書がテキストベースのファイルまたは電子メールではなく、.cer ファイルに発行された場合は、[Install from a file] を選択して該当する PC 上のファイルを検索し、[Install ID certificate file] をクリックしてから [Install Certificate] をクリックします。**図 7**



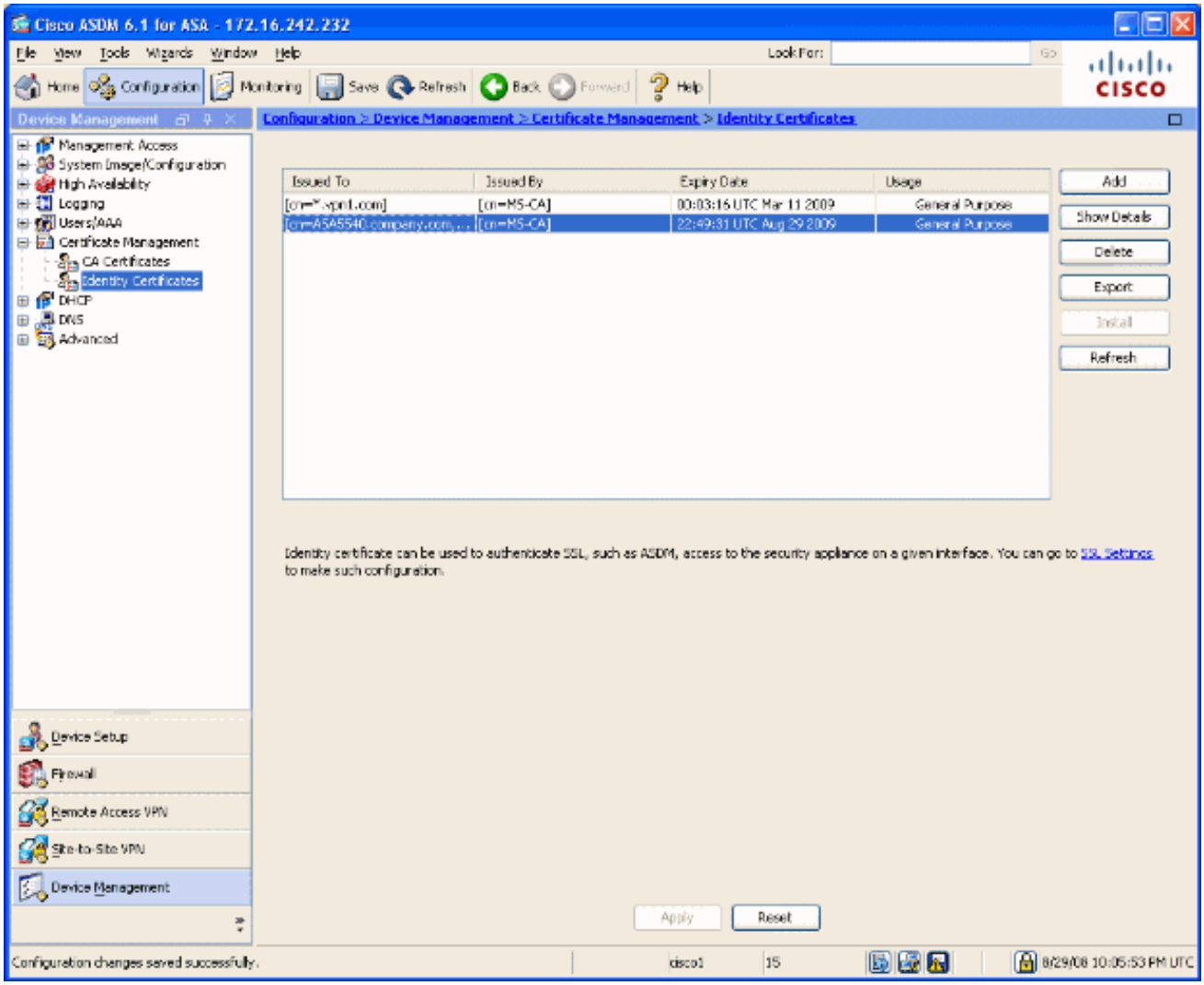
CLI の出力：

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

9. 証明書が正常にインストールされたことを確認するウィンドウが表示されます。 [OK] をクリックして確定します。**図 8**

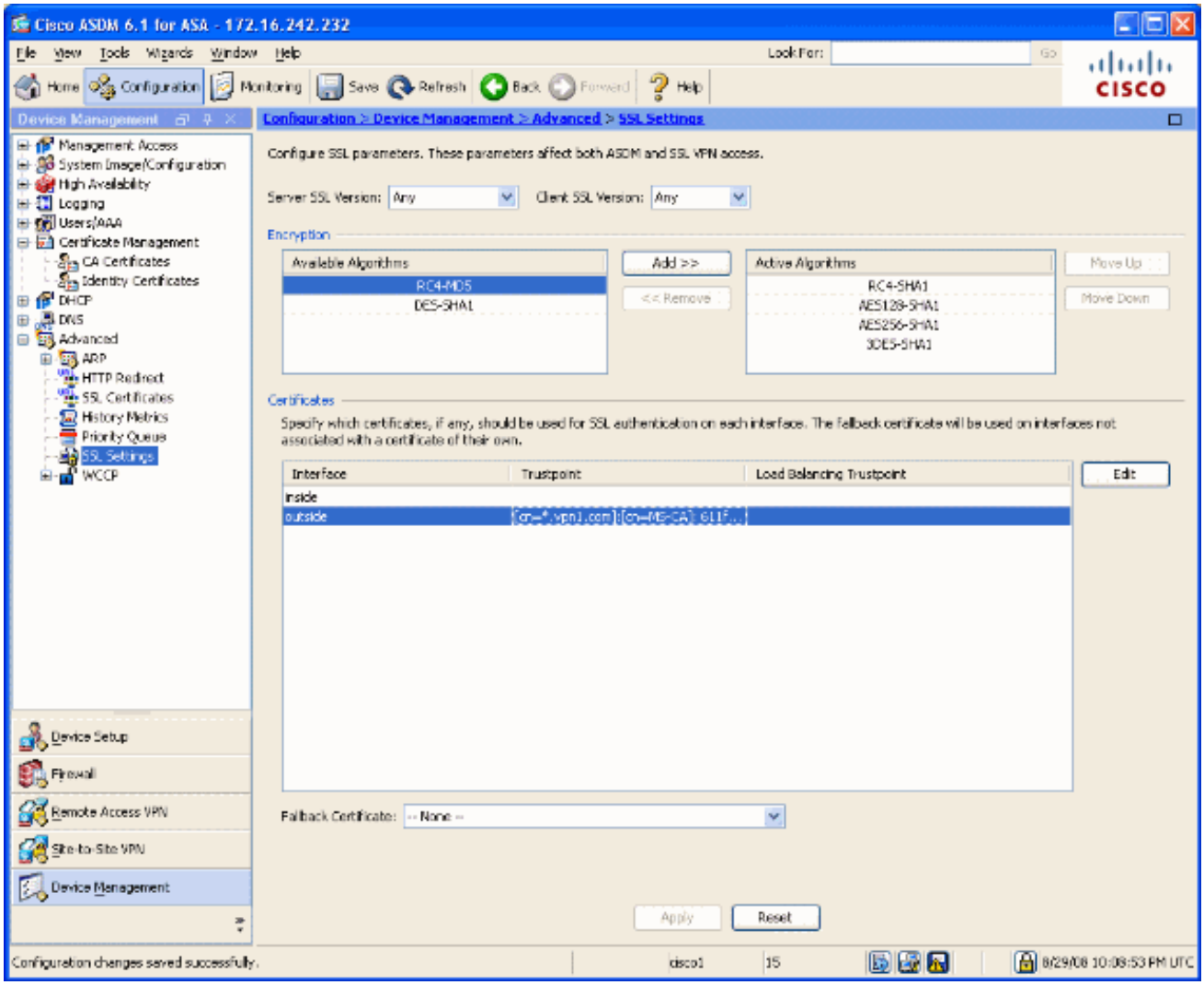


10. 新しい証明書が [Identity Certificates] に表示されることを確認します。**図 9**

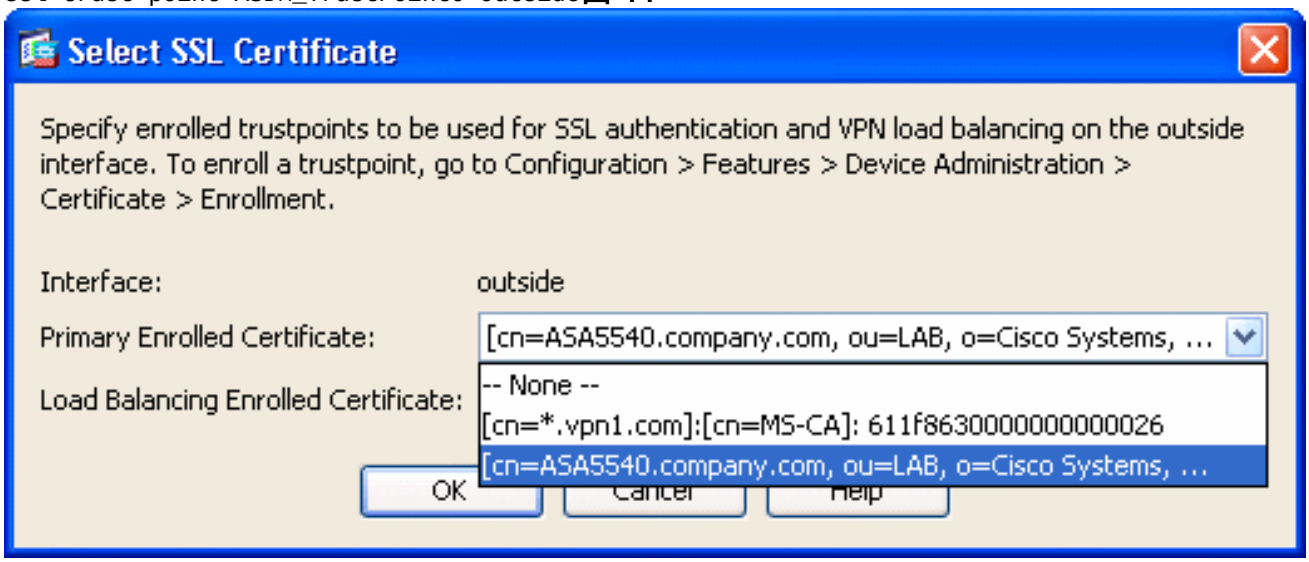


11. 新しい証明書をインターフェイスにバインドするには、次にステップを実行します。図 10 に示すように、[Configuration] > [Device Management] > [Advanced] > [SSL Settings] を順に選択します。[Certificates] の下でインターフェイスを選択し、[Edit] をクリックします。

図 10



12. ドロップダウン メニューから新しい証明書を選択し、[OK] をクリックし、[Apply] をクリックします。`ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1`
`ssl trust-point ASDM_TrustPoint0 outside`図 11



13. ASDM または CLI で設定を保存します。

確認

次のサンプル出力に示すように、CLI を使用して ASA に新しい証明書が正しくインストールされたことを確認できます。

```
ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number:
61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=MS-CA Subject Name: cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems
st=CA c=US CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008
end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate
Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

トラブルシューティング

（オプション）CLI で、正しい証明書がインターフェイスに適用されていることを確認します。

```
ASA(config)#show running-config ssl ssl trust-point ASDM_TrustPoint0 outside !--- Shows that the
correct trustpoint is tied to the outside interface that terminates SSL VPN. ASA(config)#
```

SSL 証明書を ASA から他の ASA へコピーする方法

これは、エクスポートできるキーを生成した場合に実行できます。 証明書を PKCS ファイルにエクスポートする必要があります。 これには、関連付けられたすべてのキーのエクスポートが含まれます。

CLI で証明書をエクスポートするには、次のコマンドを使用しします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

注: パスフレーズ：pkcs12 ファイルを保護するために使用されます。

CLI で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。

```
SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase>
```

注: このパスフレーズは、ファイルをエクスポートしたときに使用したものと同じでなければなりません。

ASA フェールオーバー ペアの場合、SSL 証明書を ASA から他の ASA にコピーするには、ASDM を使用することもできます。 それには次のステップを実行します。

1. プライマリ ASA に ASDM によってログインし、『Tools』 を選択 して下さい**----> バックアップコンフィギュレーション。**
2. すべて、または証明書だけをバックアップできます。
3. スタンバイで、開いた ASDM は『Tools』 を選択 し、 **----> 復元 設定。**

関連情報

- Cisco 適応型セキュリティ アプライアンスに関するサポート ページ
- ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例

- テクニカルサポートとドキュメント - Cisco Systems