ASA 8.x: Verlängern und Installieren des SSL-Zertifikats mit ASDM

Inhalt

Einführung

Das Verfahren in diesem Dokument ist ein Beispiel und kann als Richtlinie für jeden Zertifikatanbieter oder Ihren eigenen Stammzertifikatserver verwendet werden. In manchen Fällen sind vom Zertifikatanbieter spezielle Zertifizierungsparameter erforderlich. Dieses Dokument enthält jedoch die allgemeinen Schritte, die erforderlich sind, um ein SSL-Zertifikat zu verlängern und auf einer ASA zu installieren, die 8.0-Software verwendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Verfahren bezieht sich auf ASA 8.x mit ASDM Version 6.0(2) oder höher.

Das Verfahren in diesem Dokument basiert auf einer gültigen Konfiguration mit einem installierten und für den SSL VPN-Zugriff verwendeten Zertifikat. Dieses Verfahren hat keine Auswirkungen auf Ihr Netzwerk, solange das aktuelle Zertifikat nicht gelöscht wird. Dieses Verfahren beschreibt Schritt für Schritt, wie ein neuer CSR für ein aktuelles Zertifikat mit demselben Root-Zertifikat ausgegeben wird, das die ursprüngliche Root-Zertifizierungsstelle ausgestellt hat.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

potenziellen Auswirkungen eines Befehls verstehen.

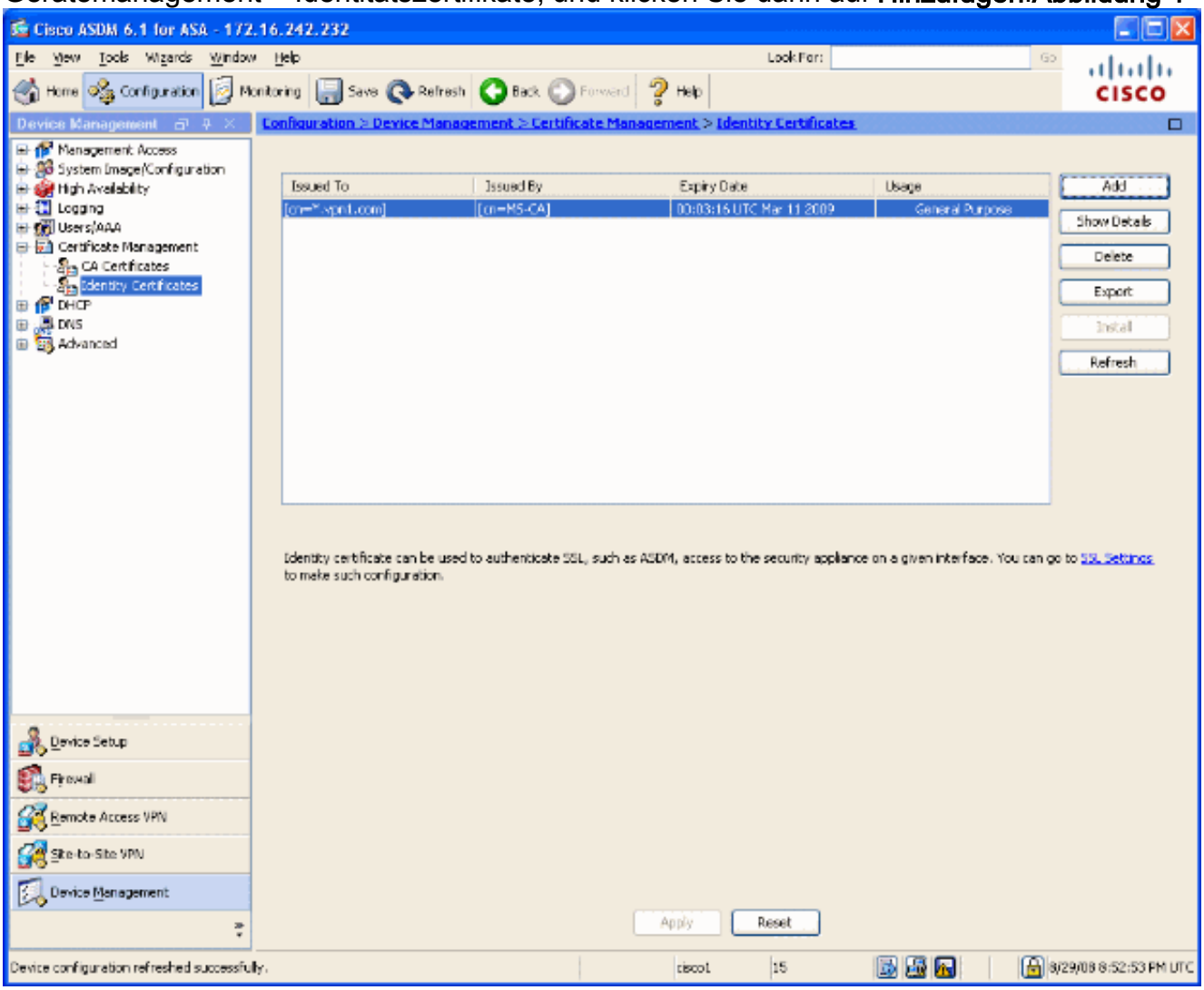
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

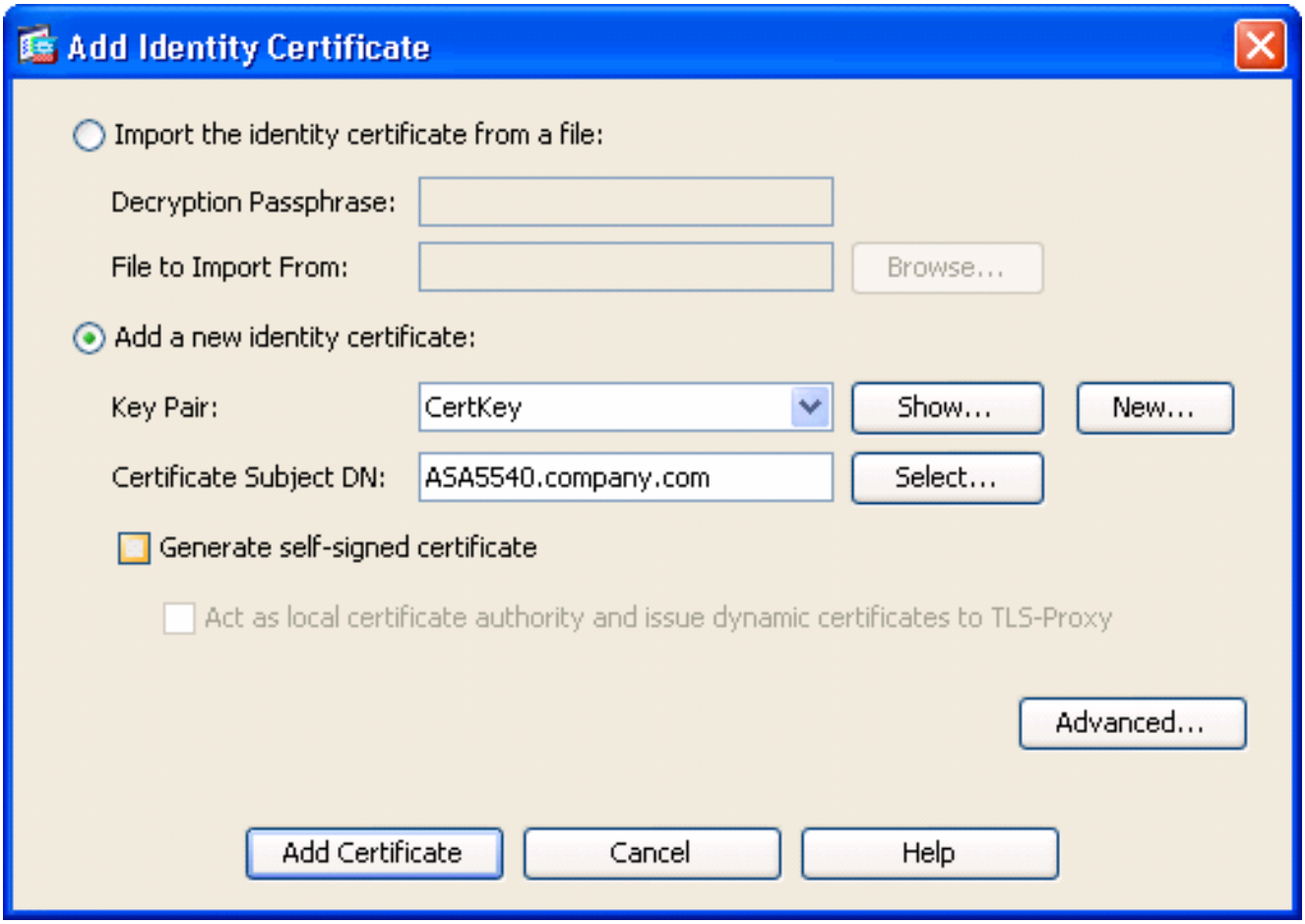
Vorgehensweise

Gehen Sie wie folgt vor:

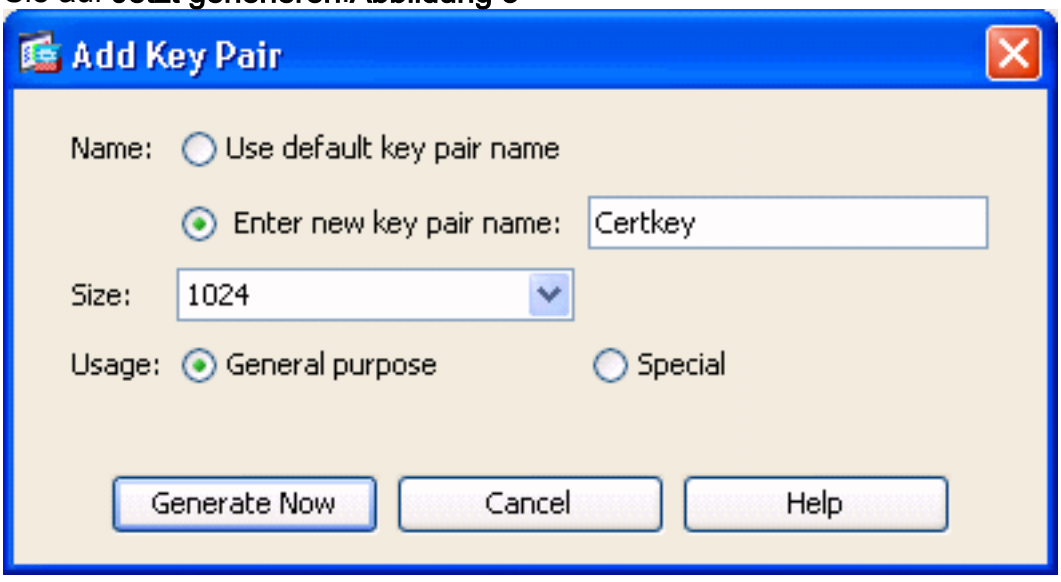
1. Wählen Sie das Zertifikat aus, das Sie verlängern möchten, unter Konfiguration > Gerätemanagement > Identitätszertifikate, und klicken Sie dann auf **Hinzufügen**.**Abbildung 1**



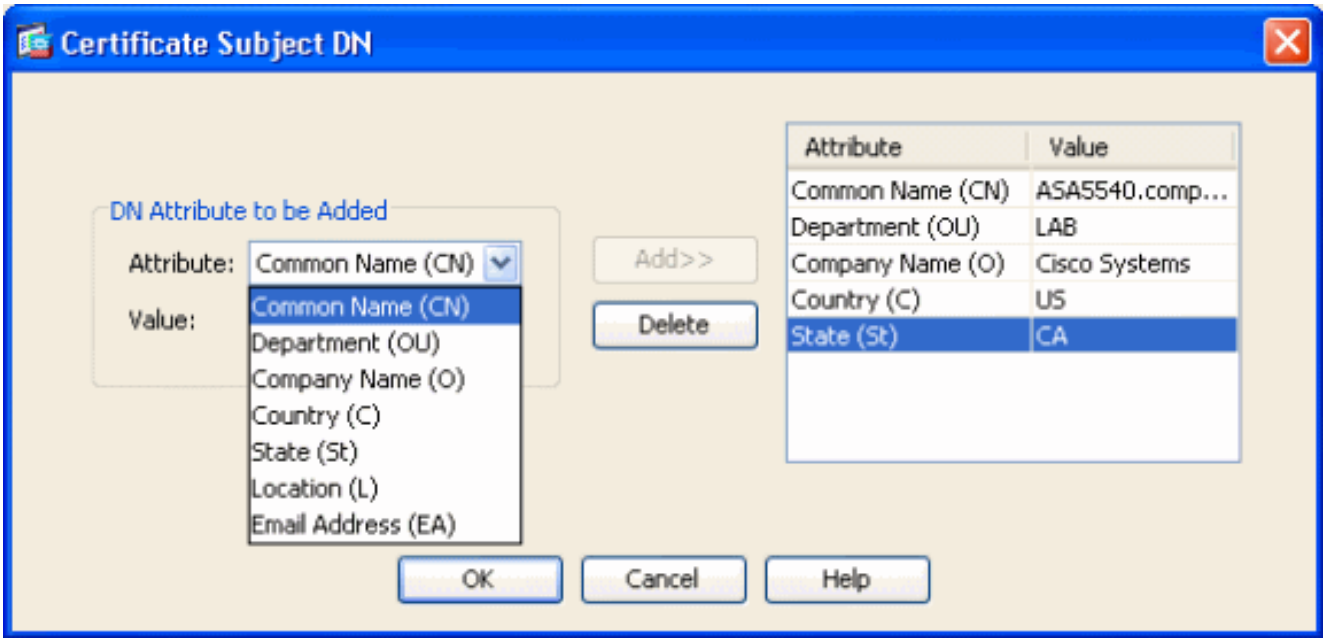
2. Wählen Sie unter Identitätszertifikat hinzufügen die Optionsschaltfläche **Neues Identitätszertifikat hinzufügen**, und wählen Sie das Schlüsselpaar aus dem Dropdown-Menü aus.**Hinweis:** Es wird nicht empfohlen, <Default-RSA-Key> zu verwenden, da Sie das Zertifikat ungültig machen, wenn Sie Ihren SSH-Schlüssel neu generieren. Wenn Sie keinen RSA-Schlüssel haben, führen Sie die Schritte a und b aus. Fahren Sie andernfalls mit Schritt 3 fort.**Abbildung 2**



(Optional) Führen Sie diese Schritte aus, wenn Sie noch keinen RSA-Schlüssel konfiguriert haben. Fahren Sie andernfalls mit Schritt 3 fort.Klicken Sie auf **Neu...**Geben Sie den Namen des Schlüsselpaars in das Feld **Name des neuen Schlüsselpaars eingeben ein**, und klicken Sie auf **Jetzt generieren**.**Abbildung 3**



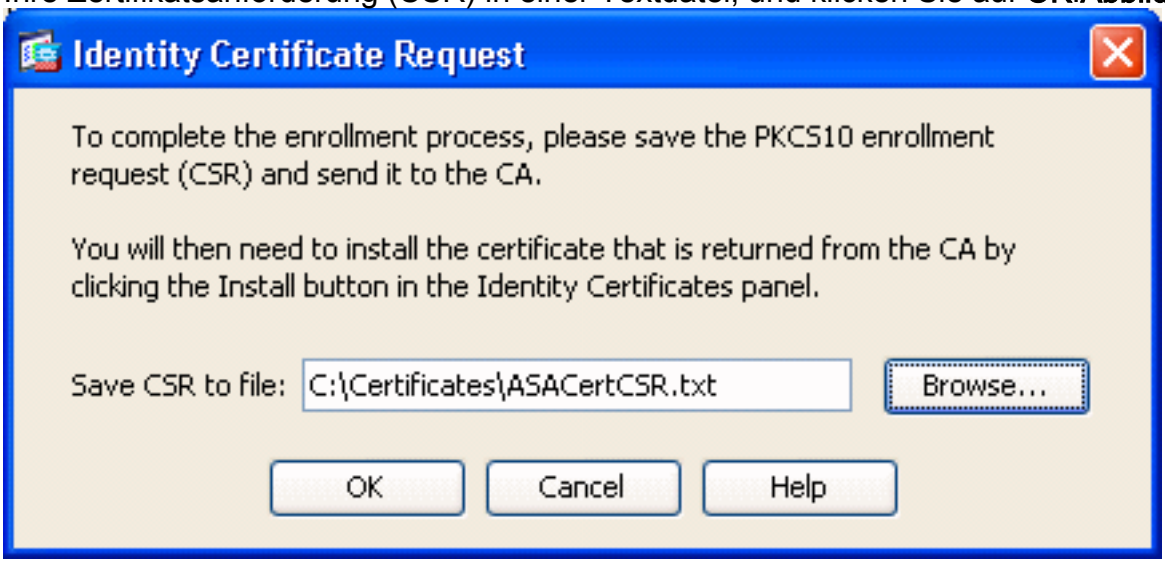
3. Klicken Sie auf **Auswählen**.
4. Geben Sie die entsprechenden Zertifikatsattribute ein (siehe Abbildung 4). Klicken Sie abschließend auf **OK**. Klicken Sie anschließend auf **Zertifikat hinzufügen**.**Abbildung 4**



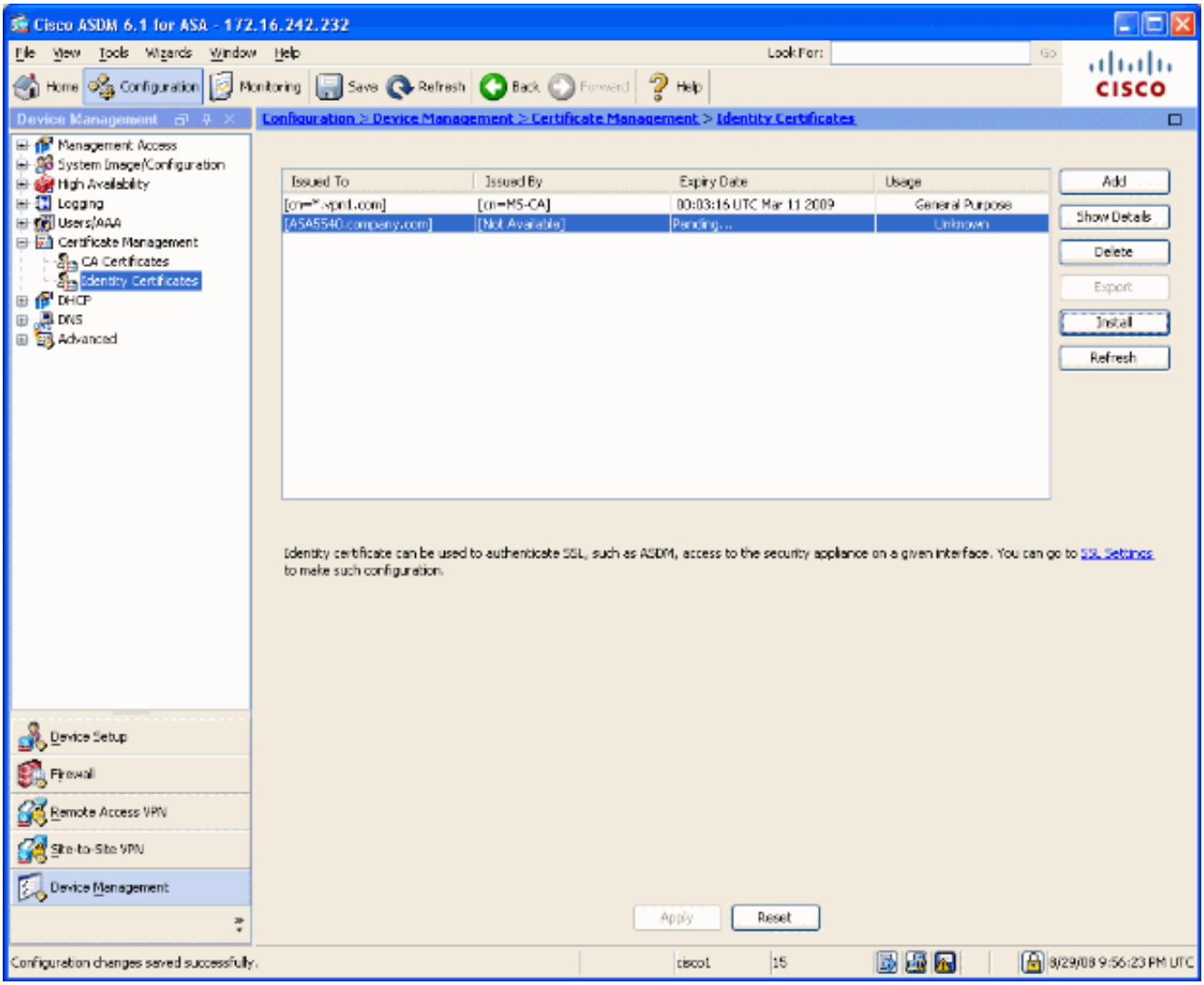
CLI-Ausgabe:

```
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
```

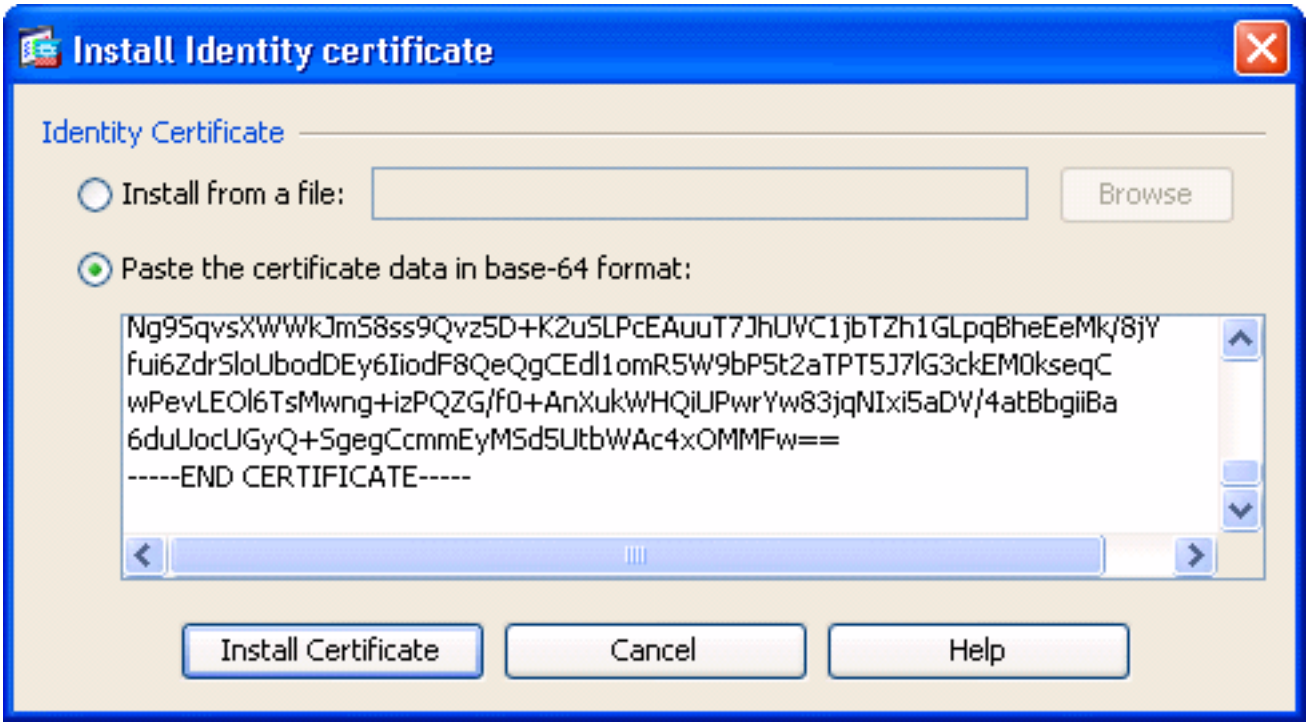
5. Speichern Sie im Popup-Fenster **Identity Certificate Request** (Identitätszertifikatanforderung) Ihre Zertifikatsanforderung (CSR) in einer Textdatei, und klicken Sie auf **OK**.**Abbildung 5**



6. (Optional) Überprüfen Sie im ASDM, dass die CSR aussteht, wie in Abbildung 6 gezeigt.**Abbildung 6**



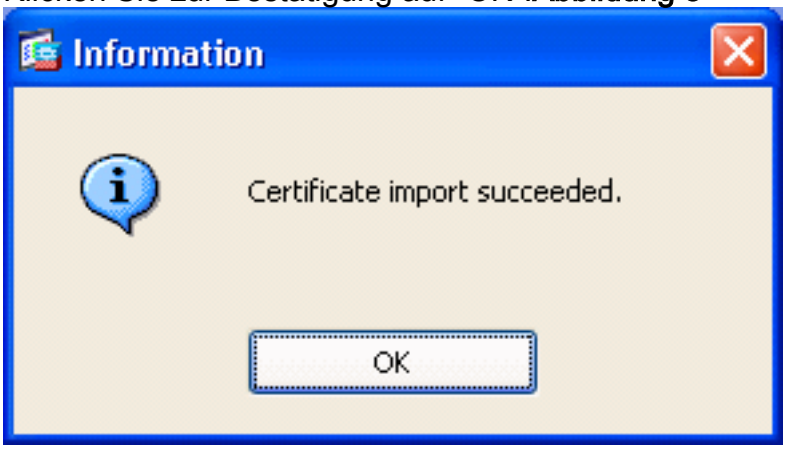
7. Senden Sie die Zertifikatsanforderung an den Zertifikatadministrator, der das Zertifikat auf dem Server ausstellt. Dies kann entweder über eine Webschnittstelle, per E-Mail oder direkt an den Stammserver der Zertifizierungsstelle erfolgen, um das Zertifikat auszustellen.
8. Führen Sie diese Schritte aus, um das erneuerte Zertifikat zu installieren.Wählen Sie die ausstehende Zertifikatsanforderung unter Configuration > Device Management > Identity Certificates (Konfiguration > Gerätemanagement > Identitätszertifikate) aus, wie in Abbildung 6 dargestellt, und klicken Sie auf **Install (Installieren)**.Wählen Sie im Fenster Identitätszertifikat installieren das Optionsfeld **Zertifikatsdaten in Base-64-Format einfügen aus**, und klicken Sie auf **Zertifikat installieren**.**Hinweis:** Wenn das Zertifikat nicht in einer textbasierten Datei oder per E-Mail, sondern in einer CSER-Datei ausgegeben wird, können Sie auch **Aus einer Datei installieren** auswählen, die entsprechende Datei auf Ihrem PC aufrufen, auf **ID-Zertifikatsdatei installieren** klicken und dann auf **Zertifikat installieren**.**Abbildung 7**



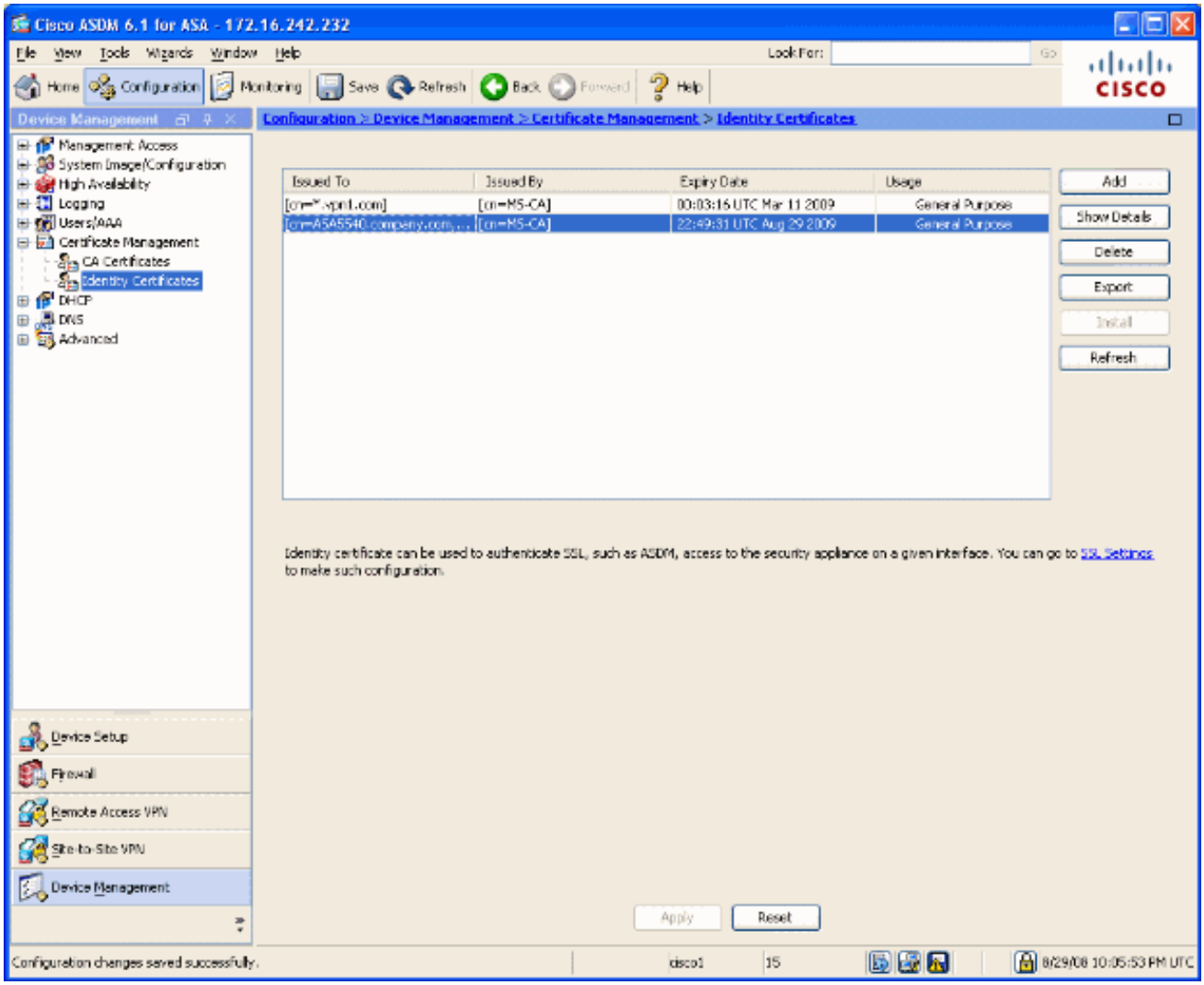
CLI-Ausgabe:

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

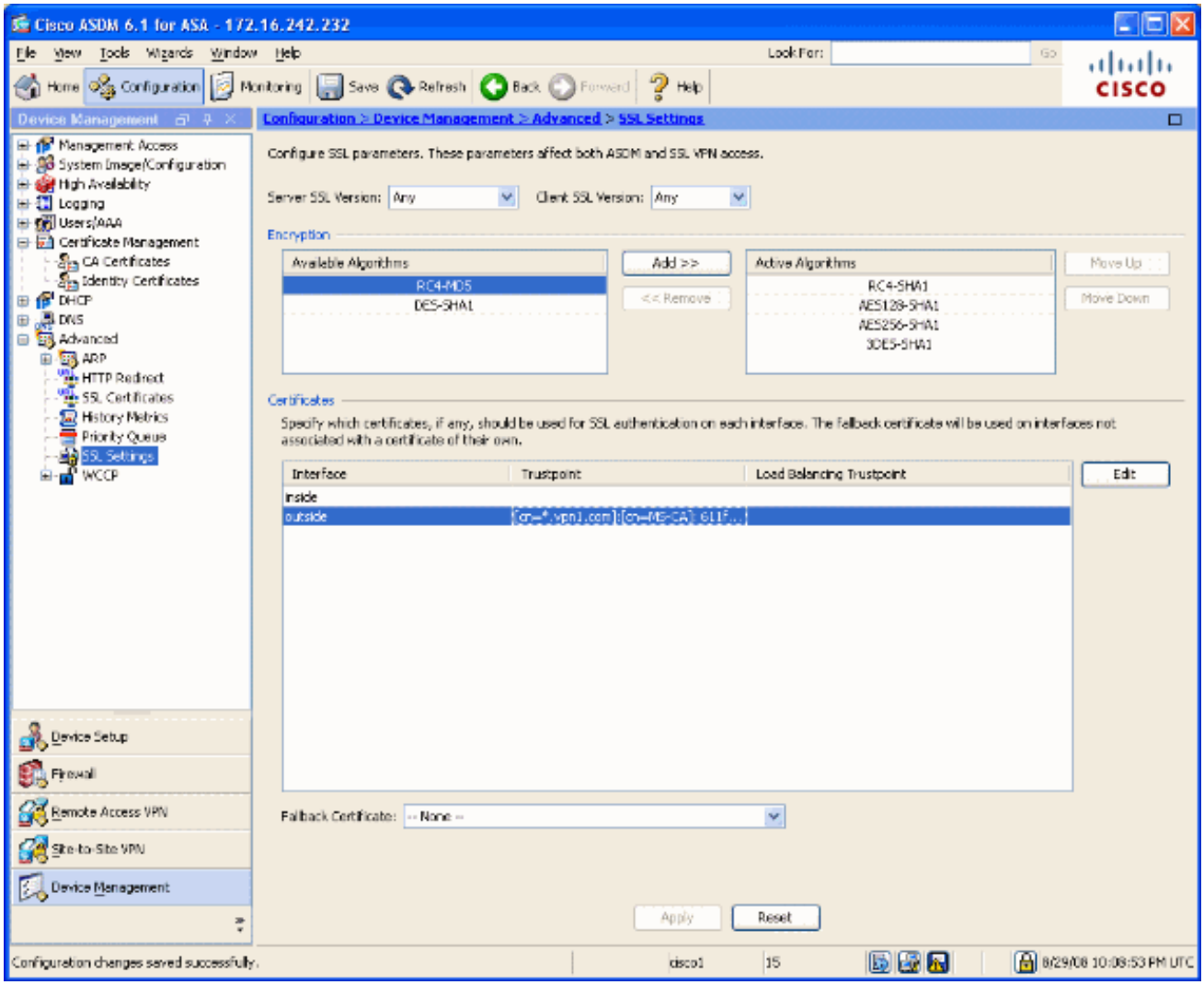
9. Es wird ein Fenster angezeigt, das bestätigt, dass das Zertifikat erfolgreich installiert wurde. Klicken Sie zur Bestätigung auf "OK".**Abbildung 8**



10. Stellen Sie sicher, dass Ihr neues Zertifikat unter Identitätszertifikate angezeigt wird.**Abbildung 9**



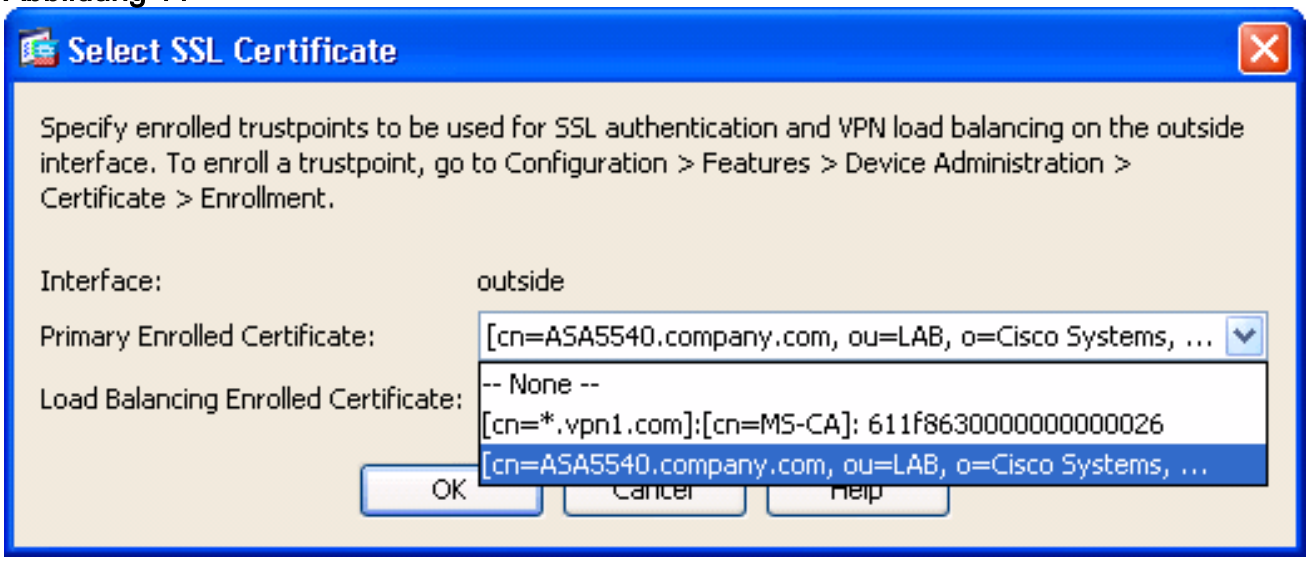
11. Gehen Sie wie folgt vor, um das neue Zertifikat an die Schnittstelle zu binden:Wählen Sie **Configuration > Device Management > Advanced > SSL Settings** (Konfiguration > Gerätemanagement > Erweitert > SSL-Einstellungen) aus, wie in Abbildung 10 dargestellt.Wählen Sie Ihre Schnittstelle unter Zertifikate aus, und klicken Sie auf **Bearbeiten**.**Abbildung 10**



12. Wählen Sie aus dem Dropdown-Menü Ihr neues Zertifikat aus, klicken Sie auf **OK**, und klicken Sie auf **Übernehmen**.

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 outside
```

Abbildung 11



13. Speichern Sie Ihre Konfiguration entweder im ASDM oder in der CLI.

Überprüfen

Sie können die CLI-Schnittstelle verwenden, um zu überprüfen, ob das neue Zertifikat korrekt auf

der ASA installiert ist, wie in dieser Beispielausgabe gezeigt:

```
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)#
```

Fehlerbehebung

(Optional) Überprüfen Sie in der CLI, ob das richtige Zertifikat auf die Schnittstelle angewendet wird:

```
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)#
```

Kopieren von SSL-Zertifikaten von einer ASA in eine andere

Dies ist möglich, wenn Sie exportierbare Schlüssel generiert haben. Sie müssen das Zertifikat in eine PKCS-Datei exportieren. Dazu gehört auch der Export aller zugeordneten Schlüssel.

Verwenden Sie diesen Befehl, um das Zertifikat über die CLI zu exportieren:

```
ASA(config)#crypto ca export
```

Hinweis: Passphrase - wird zum Schutz der Datei pkcs12 verwendet.

Verwenden Sie diesen Befehl, um das Zertifikat über die CLI zu importieren:

```
SA(config)#crypto ca import
```

Hinweis: Diese Passphrase sollte mit der beim Exportieren der Datei verwendeten Passphrase identisch sein.

Dies kann auch über ASDM für ein ASA-Failover-Paar erfolgen. Gehen Sie wie folgt vor:

1. Melden Sie sich über ASDM bei der primären ASA an, und wählen Sie **Tools -> Backup Configuration aus**.
2. Sie können alles oder nur die Zertifikate sichern.
3. Öffnen Sie im Standby-Modus ASDM, und wählen Sie **Tools -> Restore Configuration (Konfiguration wiederherstellen) aus**.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliance (ASA)
- ASA 8.x Manuelles Installieren von Drittanbieter-Zertifikaten zur Verwendung mit WebVPN - Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems