ASA 8.x: Rinnovare e installare il certificato SSL con ASDM

Sommario

Introduzione

La procedura illustrata in questo documento è un esempio e può essere utilizzata come riferimento con qualsiasi fornitore di certificati o con il proprio server di certificazione radice. A volte, il fornitore del certificato richiede requisiti speciali per i parametri del certificato, ma questo documento illustra la procedura generale necessaria per rinnovare un certificato SSL e installarlo su un'appliance ASA che usa il software 8.0.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Questa procedura è relativa alle versioni 8.x di ASA con ASDM versione 6.0(2) o successive.

La procedura illustrata in questo documento si basa su una configurazione valida con un certificato installato e utilizzato per l'accesso VPN SSL. Questa procedura non influisce sulla rete finché il certificato corrente non viene eliminato. Questa procedura descrive in modo dettagliato come emettere un nuovo CSR per un certificato corrente con lo stesso certificato radice che ha emesso la CA radice originale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Se la rete è operativa, valutare attentamente eventuali conseguenze

derivanti dall'uso dei comandi.

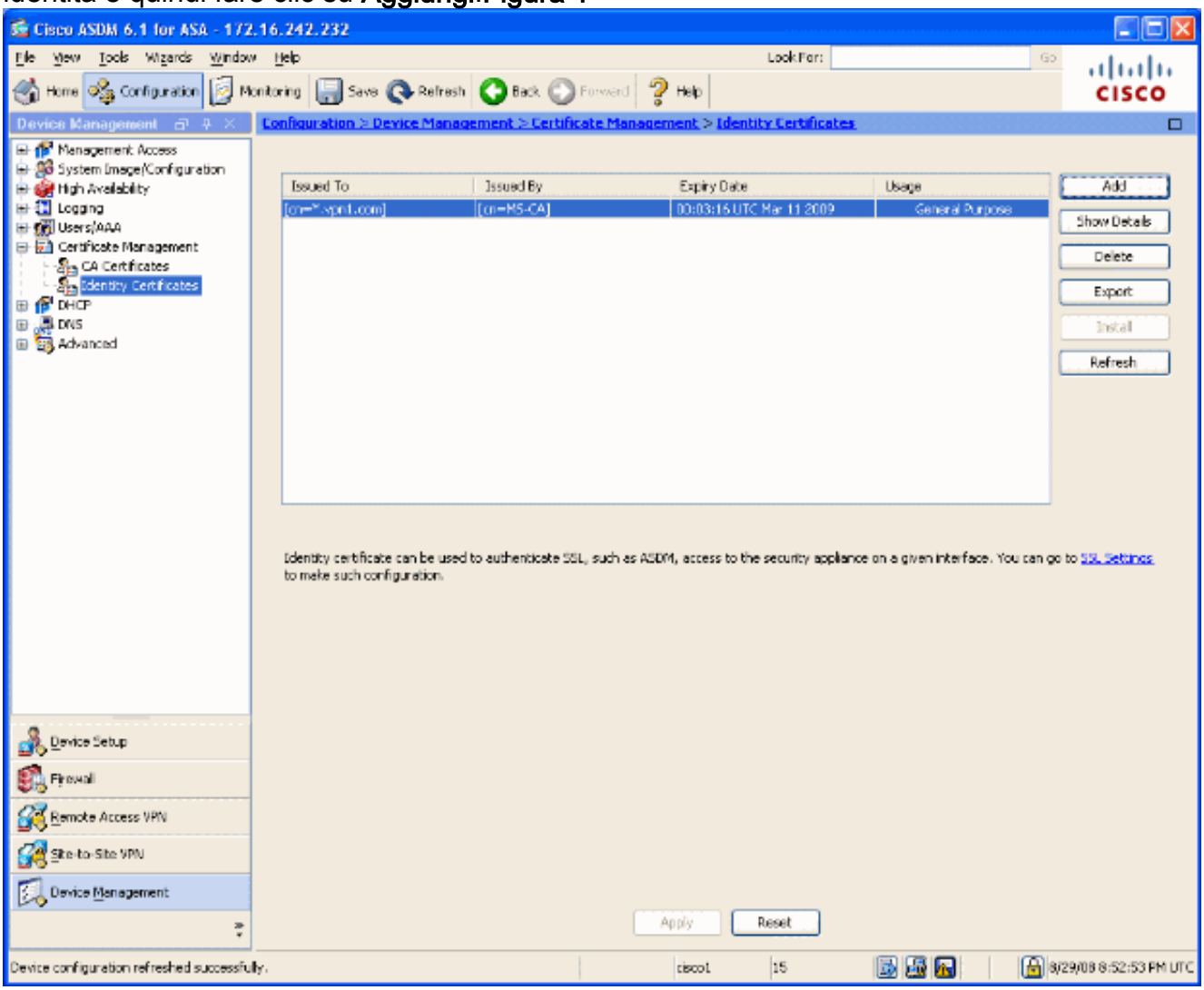
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

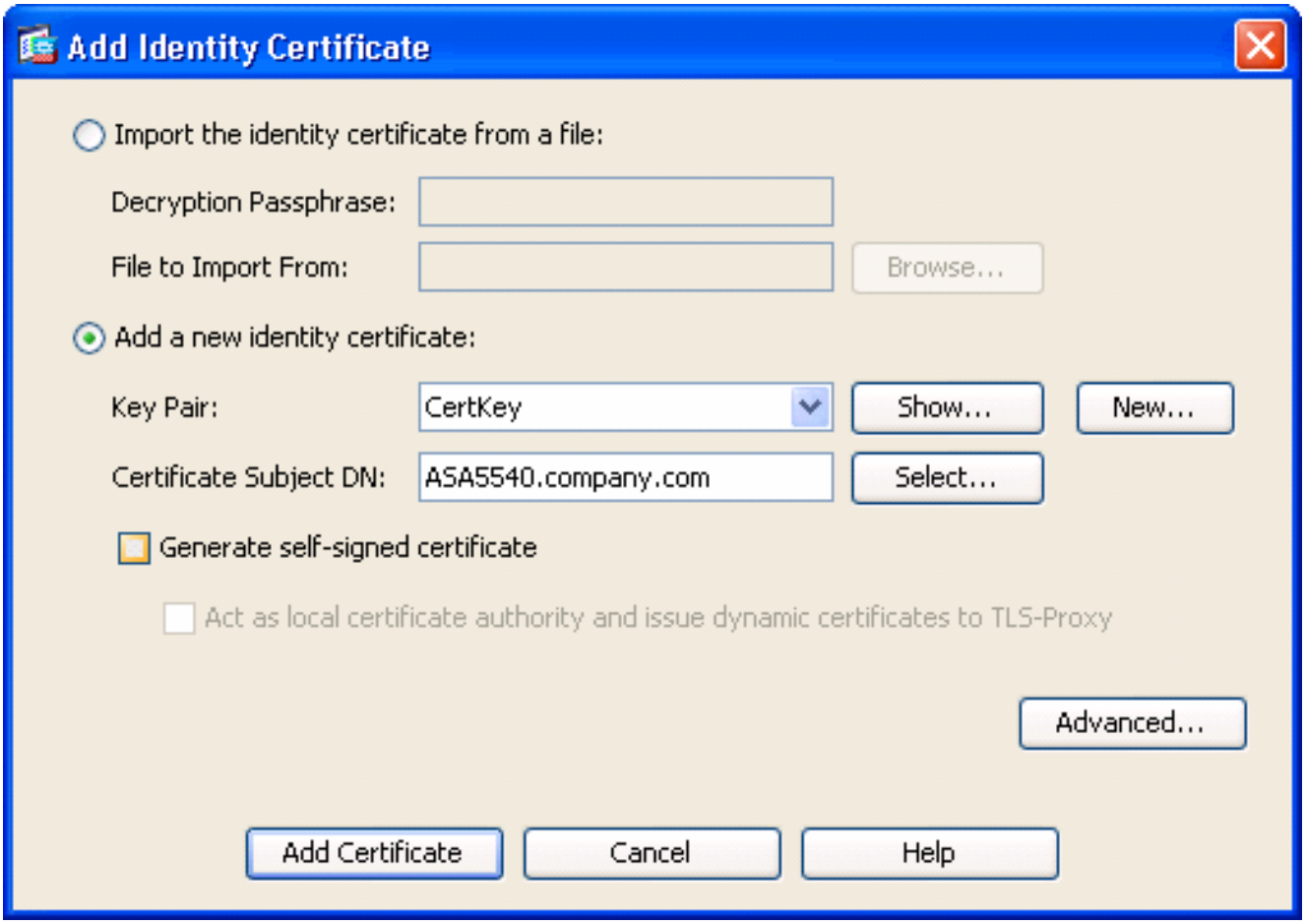
Procedura

Attenersi alla seguente procedura:

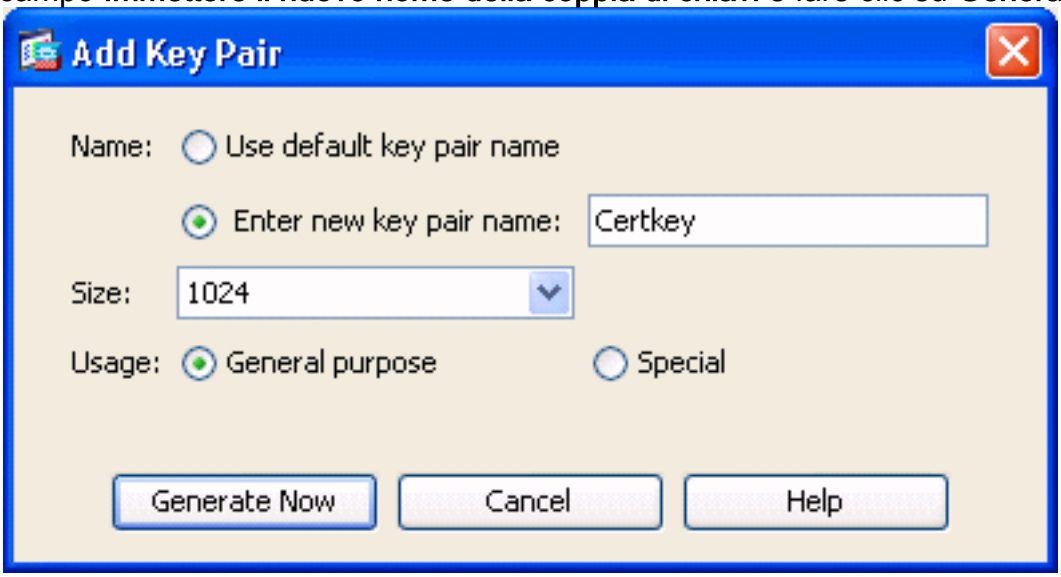
1. Selezionare il certificato da rinnovare in Configurazione > Gestione dispositivi > Certificati di identità e quindi fare clic su **Aggiungi**.**Figura 1**



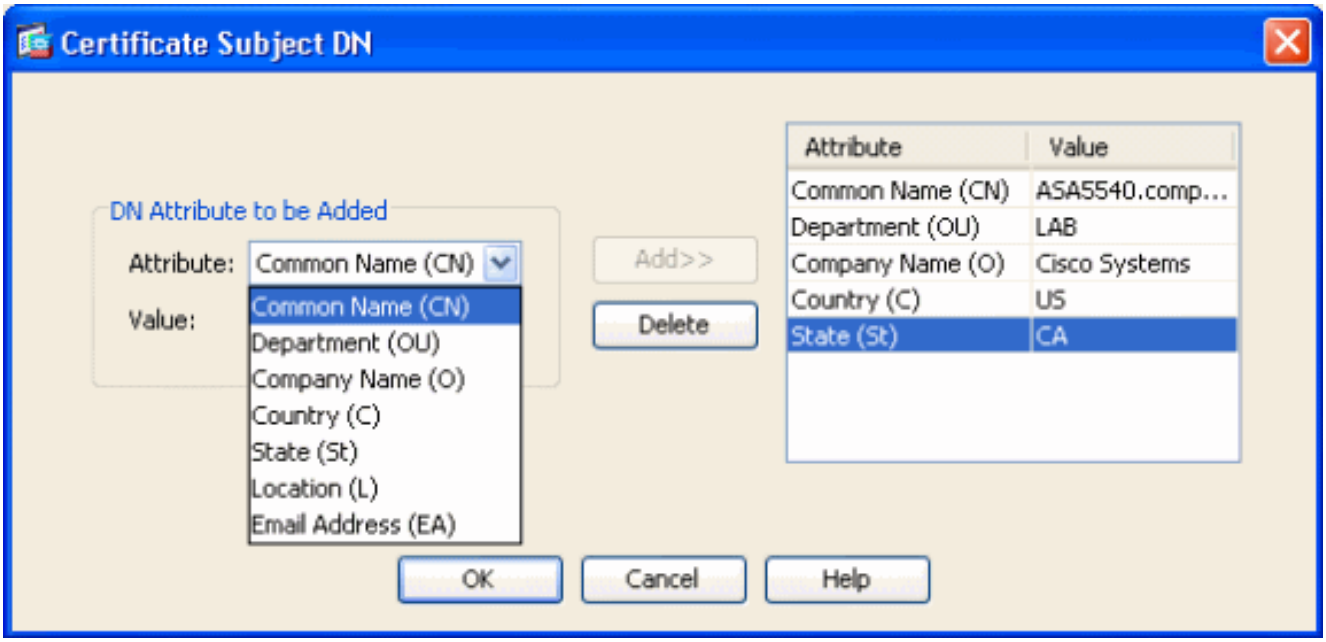
2. In Aggiungi certificato di identità selezionare il pulsante di opzione **Aggiungi nuovo certificato di identità** e scegliere la coppia di chiavi dal menu a discesa.**Nota:** si consiglia di non utilizzare <Default-RSA-Key> perché se si rigenera la chiave SSH, il certificato viene invalidato. Se non si dispone di una chiave RSA, completare i passaggi a e b. In caso contrario, passare al punto 3.**Figura 2**



(Facoltativo) Completare questi passaggi se non è ancora stata configurata una chiave RSA, in caso contrario andare al passaggio 3.Fare clic su **Nuovo...**.Immettere il nome della coppia di chiavi nel campo **Immettere il nuovo nome della coppia di chiavi** e fare clic su **Genera ora**.**Figura 3**



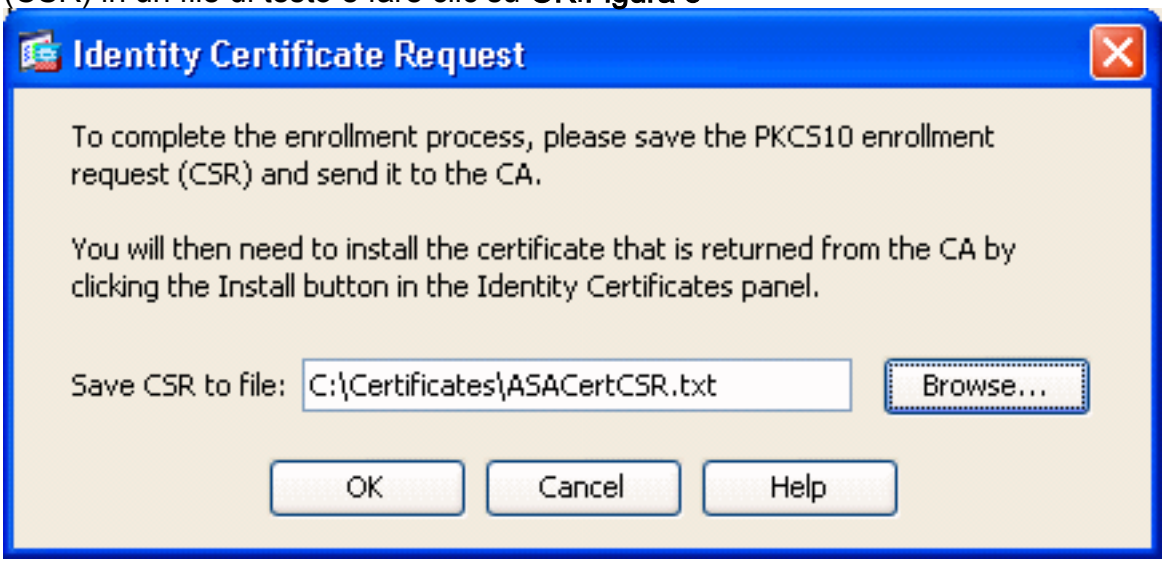
3. Fare clic su **Seleziona**.
4. Immettere gli attributi del certificato appropriati, come mostrato nella Figura 4. Una volta completato, fare clic su **OK**. Fare quindi clic su **Aggiungi certificato**.**Figura 4**



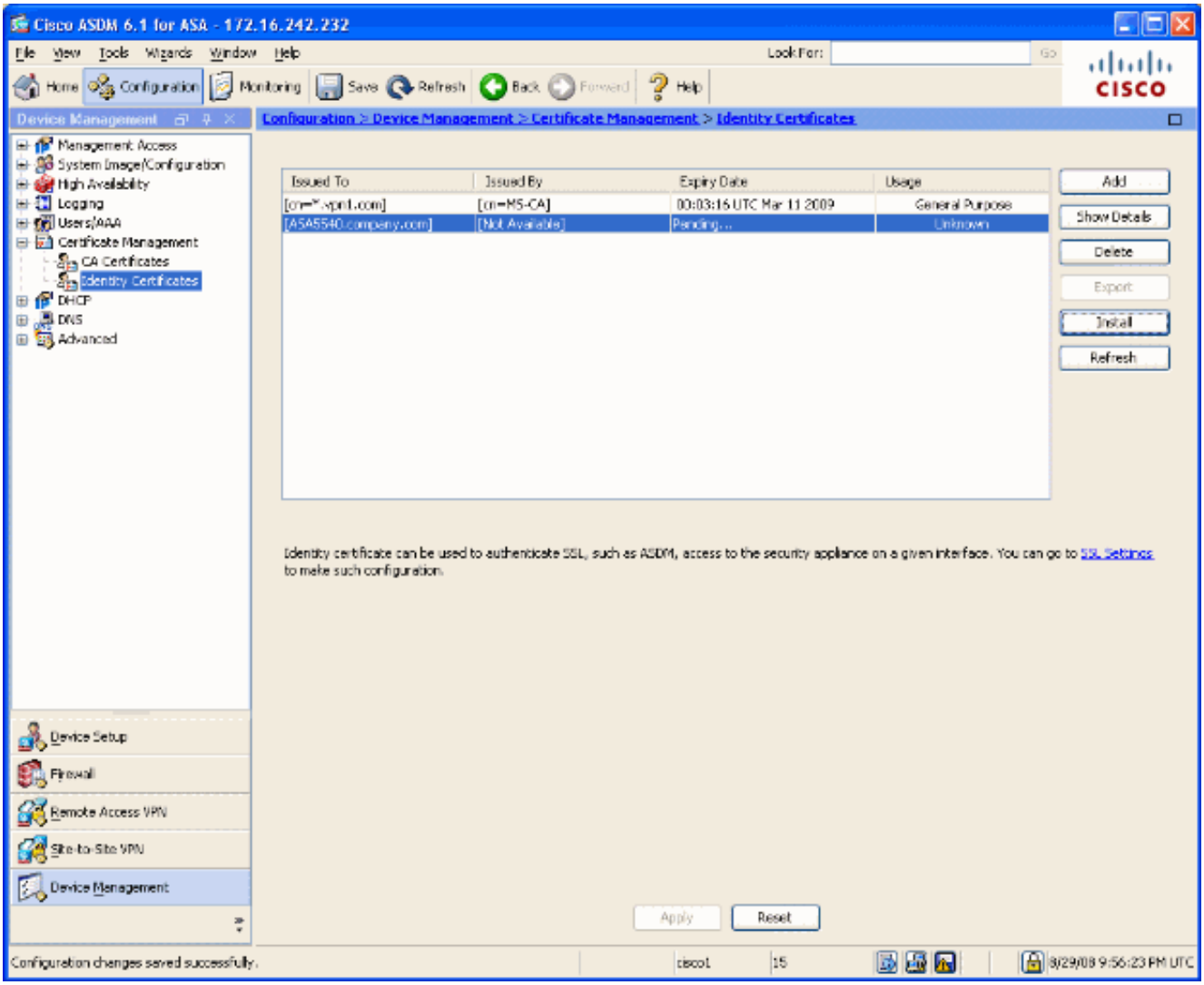
Output CLI:

```
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
```

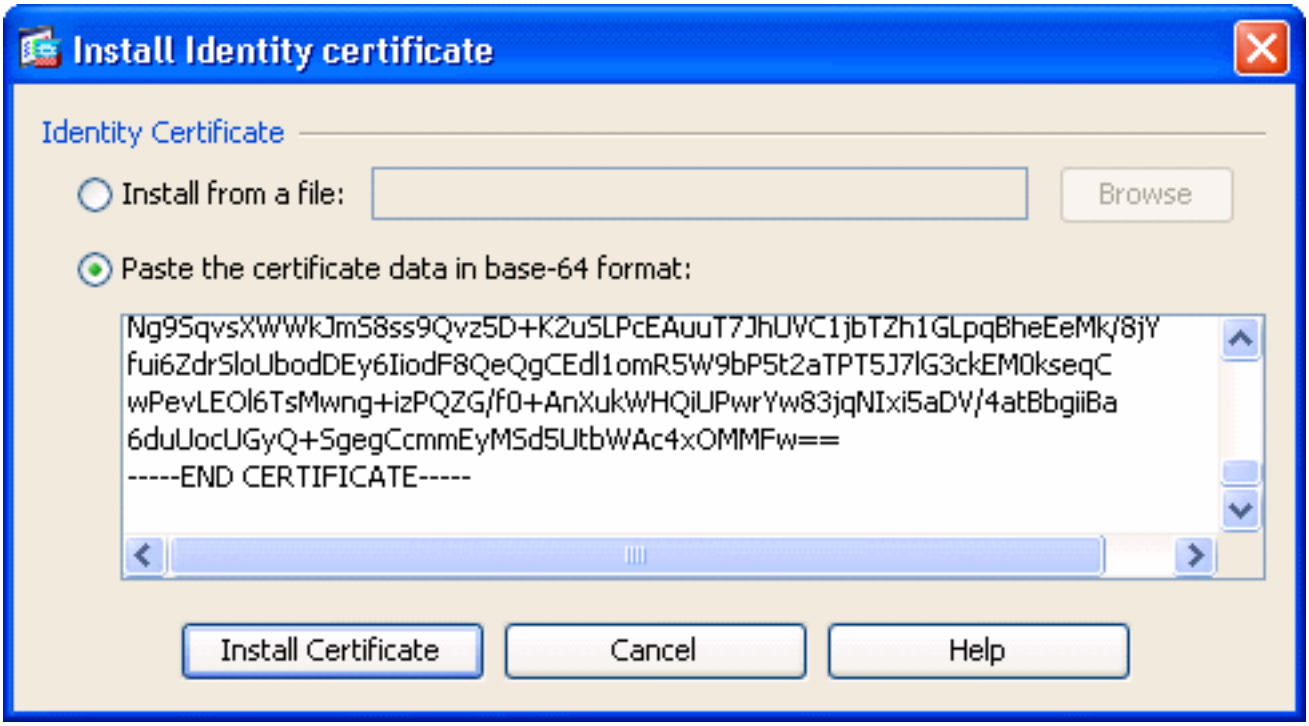
5. Nella finestra popup **Richiesta certificato di identità**, salvare la richiesta di firma del certificato (CSR) in un file di testo e fare clic su **OK**.**Figura 5**



6. (Facoltativo) Verificare in ASDM che il CSR sia in sospeso, come mostrato nella Figura 6.**Figura 6**



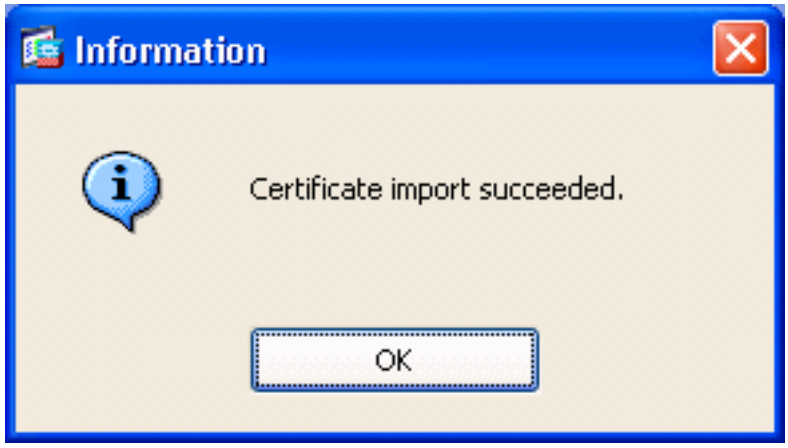
7. Inviare la richiesta di certificato all'amministratore del certificato che emette il certificato sul server. A tale scopo, è possibile utilizzare un'interfaccia Web, un messaggio di posta elettronica oppure accedere direttamente al server CA radice per l'elaborazione dei certificati.
8. Completare questa procedura per installare il certificato rinnovato.Selezionare la richiesta di certificato in sospeso in Configurazione > Gestione dispositivi > Certificati di identità, come mostrato nella Figura 6, e fare clic su **Installa**.Nella finestra Installa certificato di identità, selezionare il pulsante di opzione **Incolla i dati del certificato in formato base 64** e fare clic su **Installa certificato**.**Nota:** in alternativa, se il certificato viene emesso in un file con estensione cer anziché in un file di testo o in un messaggio di posta elettronica, è anche possibile selezionare **Installa da un file**, individuare il file appropriato nel PC, fare clic su **Installa file di certificato ID** e quindi su **Installa certificato**.**Figura 7**



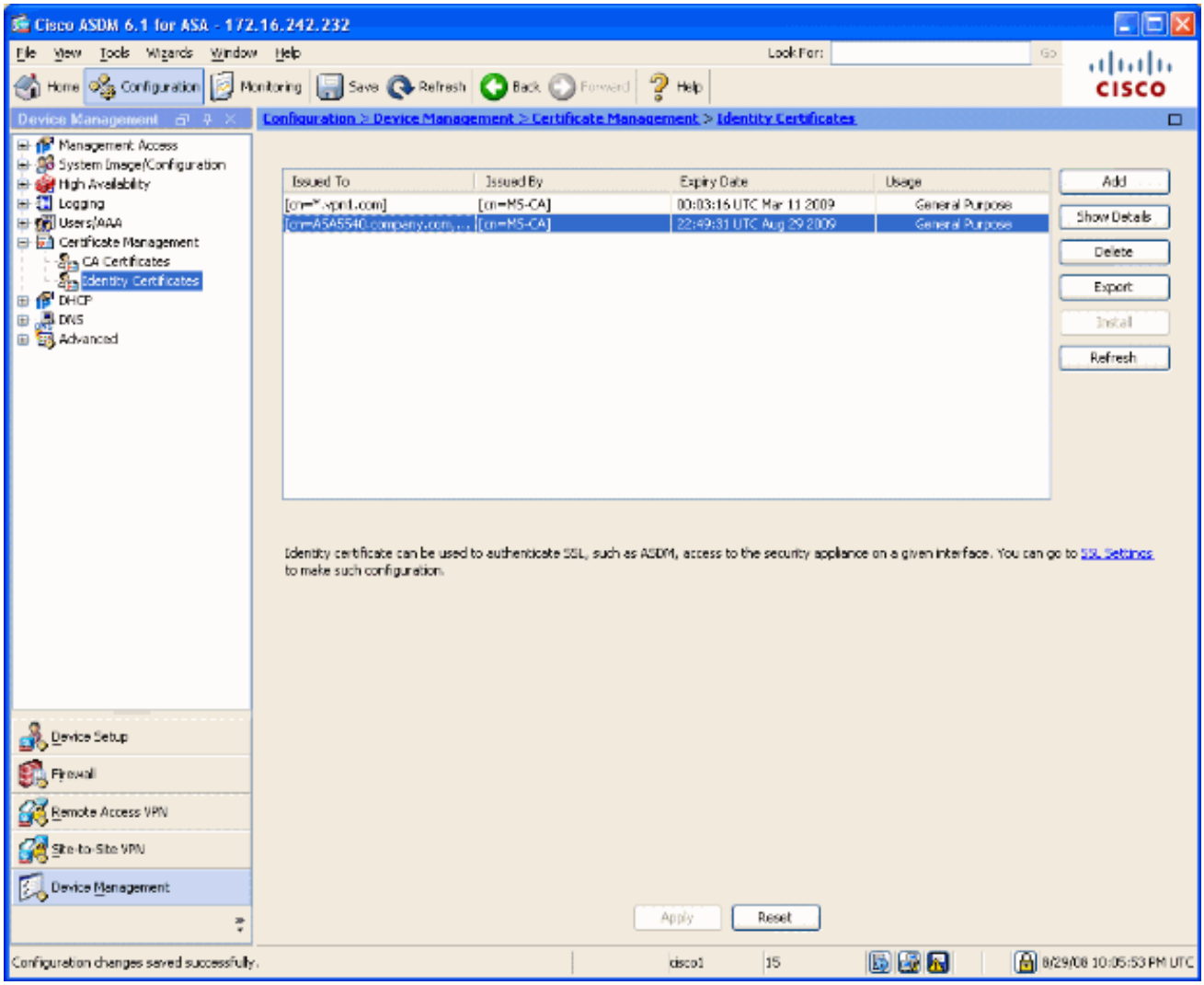
Output CLI:

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

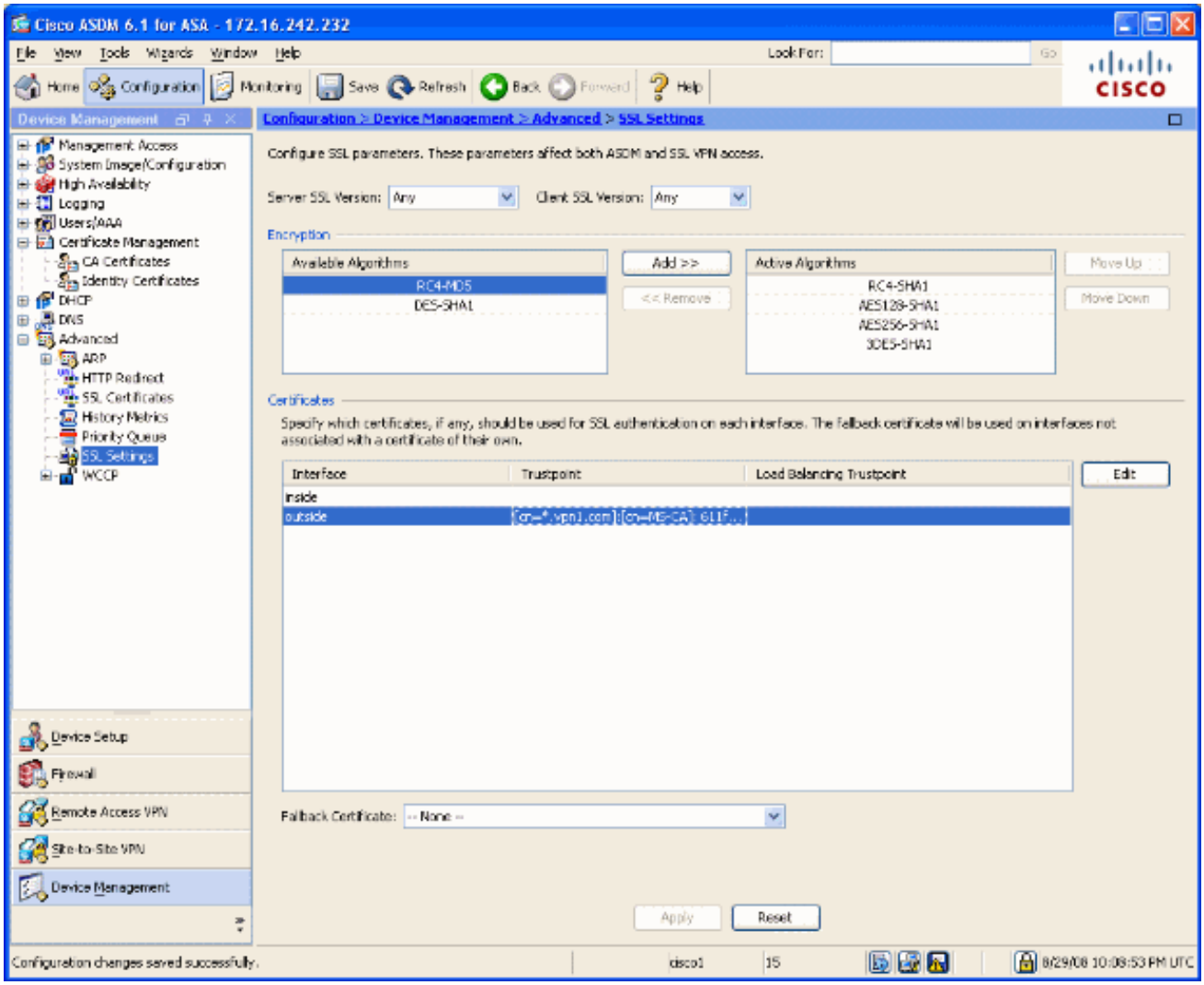
9. Verrà visualizzata una finestra che conferma l'installazione del certificato. Fare clic su "OK" per confermare.**Figura 8**



10. Assicurarsi che il nuovo certificato venga visualizzato in Certificati di identità.**Figura 9**



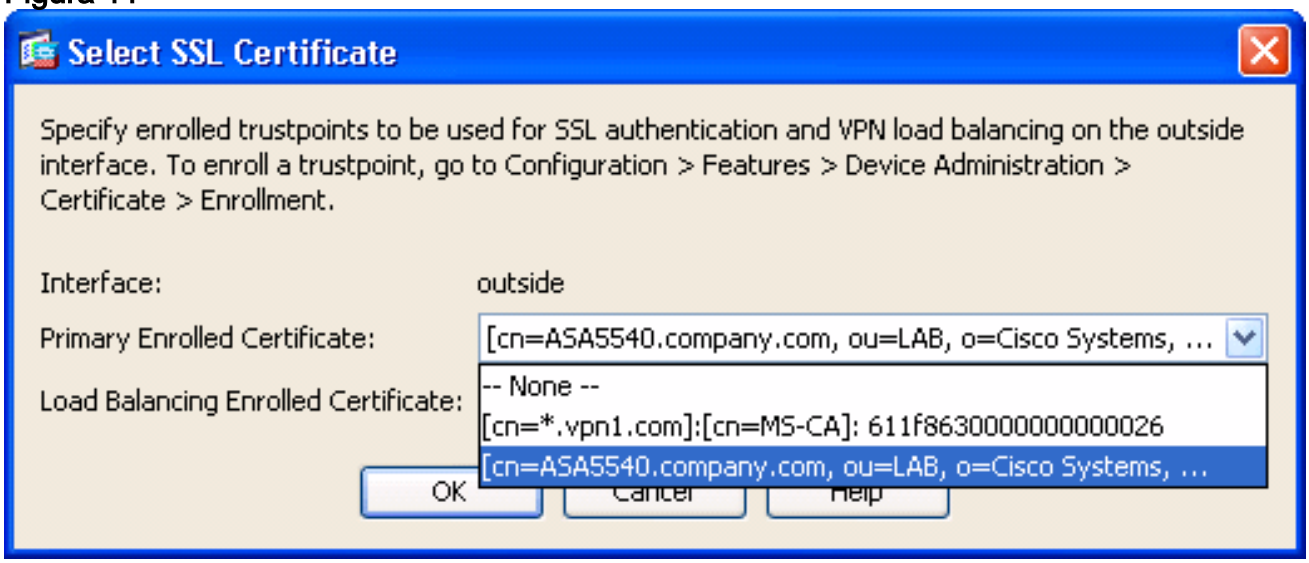
11. Completare questa procedura per associare il nuovo certificato all'interfaccia:Scegliere **Configurazione > Gestione dispositivi > Avanzate > Impostazioni SSL**, come mostrato nella Figura 10.Selezionare l'interfaccia in Certificati e fare clic su **Modifica**.**Figura 10**



12. Scegliere il nuovo certificato dal menu a discesa, fare clic su **OK**, quindi su **Applica**.

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

Figura 11



13. Salvare la configurazione in ASDM o nella CLI.

Verifica

Èpossibile usare l'interfaccia CLI per verificare che il nuovo certificato sia installato correttamente sull'ASA, come mostrato nell'output di esempio:

```
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)#
```

Risoluzione dei problemi

(Facoltativo) Verificare sulla CLI che all'interfaccia sia applicato il certificato corretto:

```
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)#
```

Come copiare i certificati SSL da un'appliance ASA a un'altra

Questa operazione può essere eseguita se sono state generate chiavi esportabili. È necessario esportare il certificato in un file PKCS. Ciò include l'esportazione di tutte le chiavi associate.

Utilizzare questo comando per esportare il certificato dalla CLI:

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

Nota: passphrase - utilizzata per proteggere il file pkcs12.

Utilizzare questo comando per importare il certificato tramite CLI:

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

Nota: questa passphrase deve essere uguale a quella utilizzata per l'esportazione del file.

Questa operazione può essere eseguita anche tramite ASDM per una coppia di failover ASA. Per effettuare questa operazione, effettuare le seguenti operazioni:

1. Accedere all'ASA principale tramite ASDM e scegliere **Strumenti—> Configurazione di backup**.
2. Èpossibile eseguire il backup di tutti i dati o solo dei certificati.
3. In standby, aprire ASDM e scegliere **Strumenti —> Ripristina configurazione**.

Informazioni correlate

- Pagina di supporto per Cisco Adaptive Security Appliance (ASA)
- Esempio di installazione manuale di certificati di terze parti per ASA 8.x da utilizzare con la configurazione di WebVPN
- Documentazione e supporto tecnico – Cisco Systems