Install and Renew the SSL Certificate with ASDM

Contents

Introduction

This document describes how to renew an SSL certificate and install it on ASA on a vendor or your own certificate server.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This procedure pertains to Adaptive Security Appliance (ASA) versions 8.x with Adaptive Security Device Manager (ASDM) version 6.0(2) or later.

The procedure in this document is based on a valid configuration with a certificate installed and used for SSL VPN access. The procedure does not impact your network as long as the current certificate is not deleted. This procedure is a step-by-step process on how to issue a new CSR for a current certificate with the same root certificate that issued the original root CA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

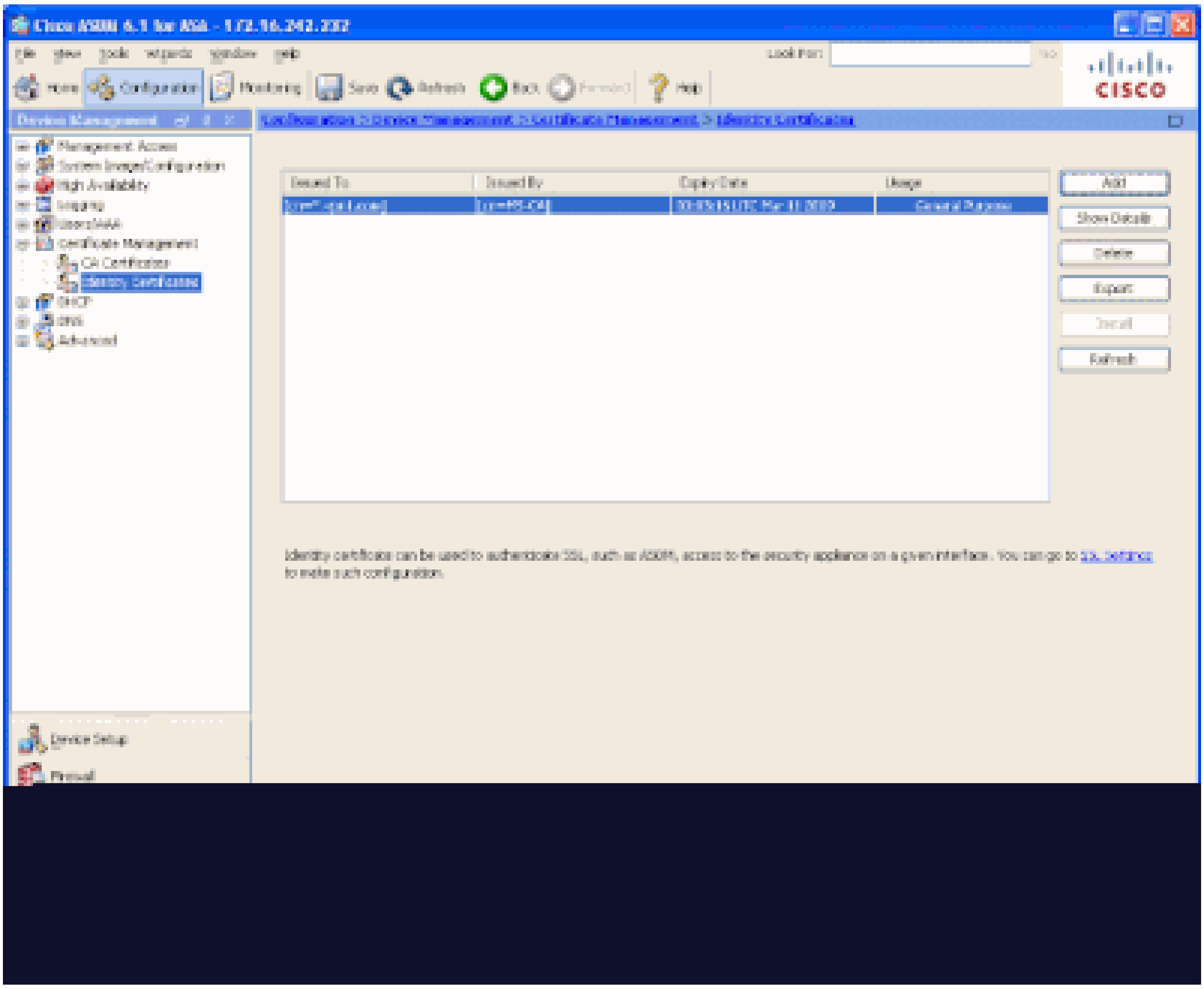
This document describes a procedure that can be used as a guideline with any certificate vendor or your own root certificate server. Special certificate parameter requirements are sometimes required by your certificate vendor, but this document is intended to provide the general steps required to renew an SSL certificate and install it on an ASA that uses 8.0 software.

Procedure

Complete these steps:

1. Select the certificate you want to renew beneath **Configuration** > **Device Management** > **Identity Certificates**, and then click **Add**.

   Figure 1

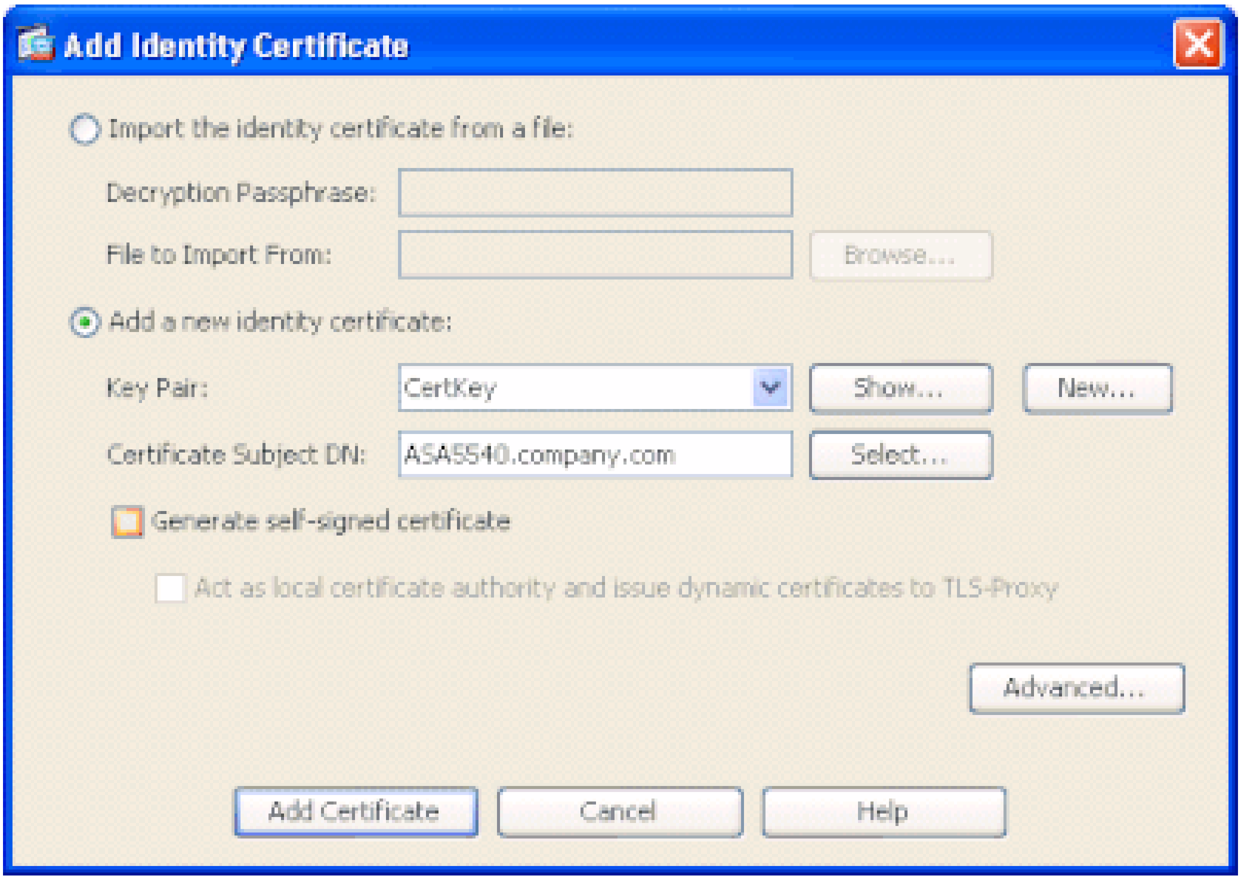
Issued To	Issued By	Expiry Date	Usage
[cn=*.vpn.local]	[cn=MS-CA]	00:05:15 UTC Mar 11 2010	General Purpose

   Identity certificates can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to SSL Settings to make such configuration.

2. Under Add Identity Certificate, select the **Add a new identity certificate** radio button, and choose your key pair from the drop-down menu.

Note: It is not recommended to use because if you regenerate your SSH key, you invalidate your certificate. If you do not have an RSA key, complete Steps a and b. Otherwise continue to Step 3.

Figure 2



Add Identity Certificate

○ Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: CertKey

Certificate Subject DN: ASA5540.company.com

□ Generate self-signed certificate

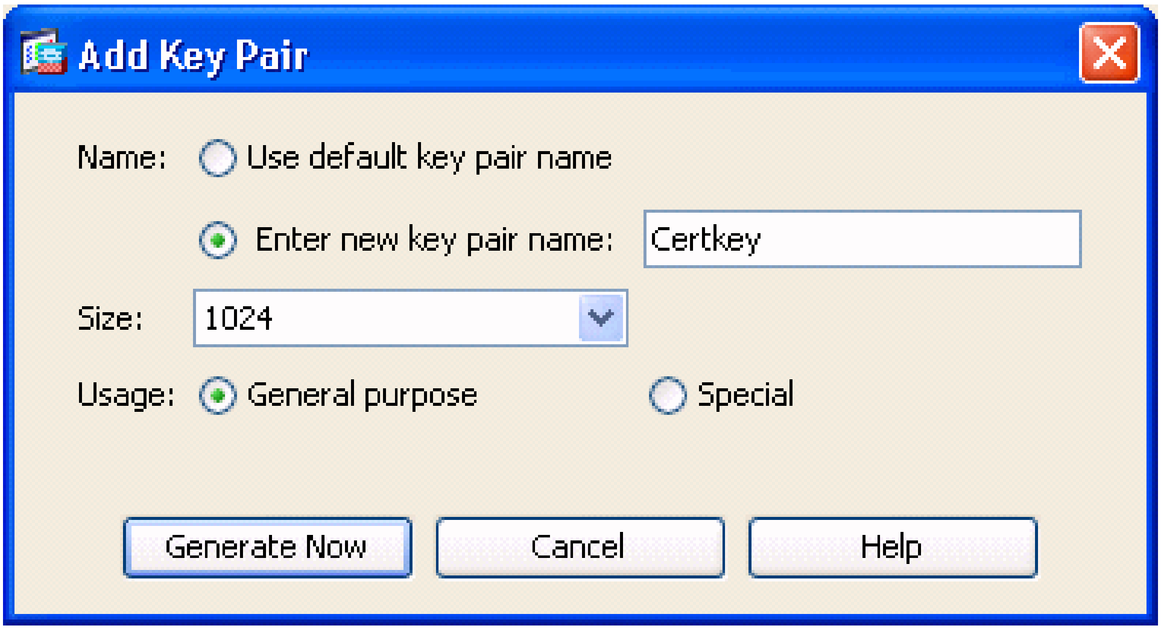
□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

a. (Optional) Complete these steps if you do not have an RSA key configured yet, otherwise skip to Step 3.

Click **New...** .

b. Enter the key pair name in the **Enter new key pair name** field, and click **Generate Now**.

Figure 3



Add Key Pair

Name: ○ Use default key pair name

● Enter new key pair name: Certkey

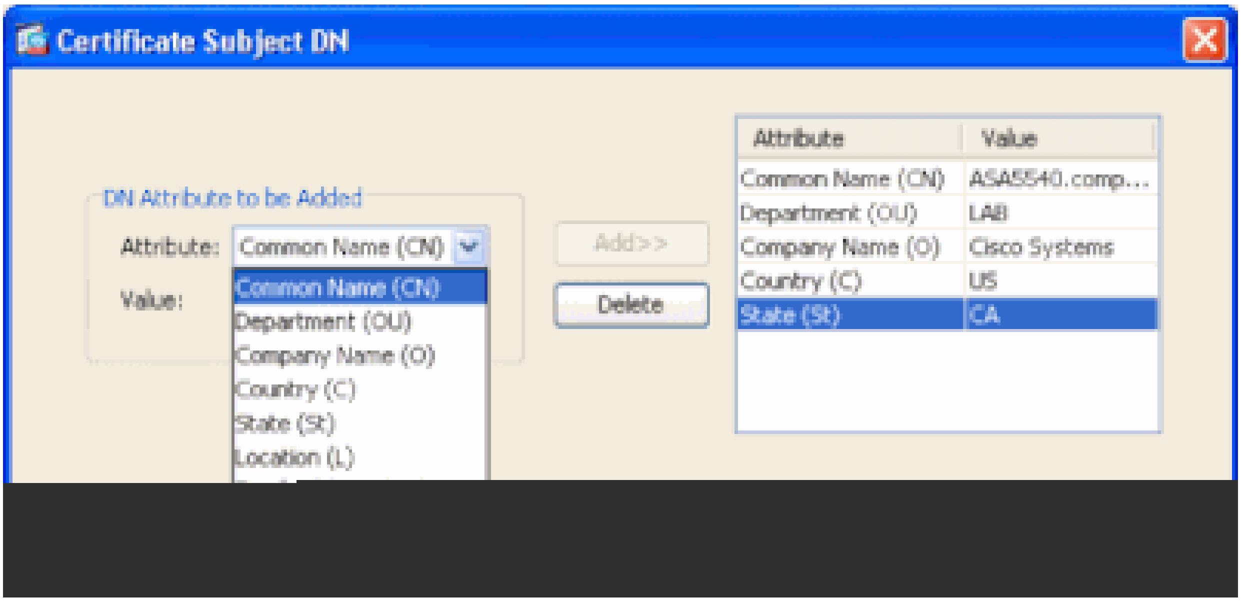
Size: 1024

Usage: ● General purpose ○ Special

3. Click **Select**.

4. Enter the appropriate certificate attributes as shown in Figure 4. Once completed, click **OK**. Then click **Add Certificate**.

Figure 4



Attribute: Common Name (CN)

Value:

Attribute	Value
Common Name (CN)	ASA5540.comp...
Department (OU)	LAB
Company Name (O)	Cisco Systems
Country (C)	US
State (St)	CA

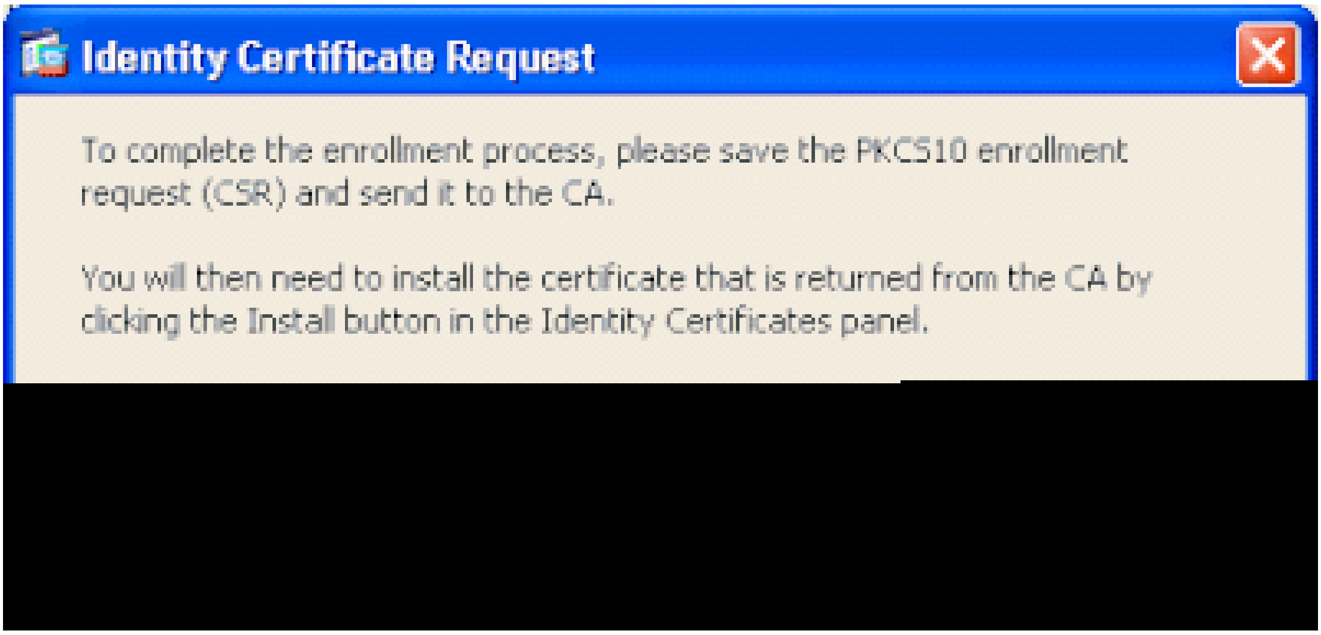
CLI output:

<#root>

```
crypto ca trustpoint ASDM_TrustPoint0

        keypair CertKey
        id-usage ssl-ipsec
        fqdn 5540-uwe
        subject-name CN=website address,OU=LAB,O=Cisco ystems,C=US,St=CA
        enrollment terminal


crypto ca enroll ASDM_TrustPoint0
```

1. In the **Identity Certificate Request** pop-up window, save your Certificate Signing Request (CSR) to a text file, and click **OK**.

Figure 5



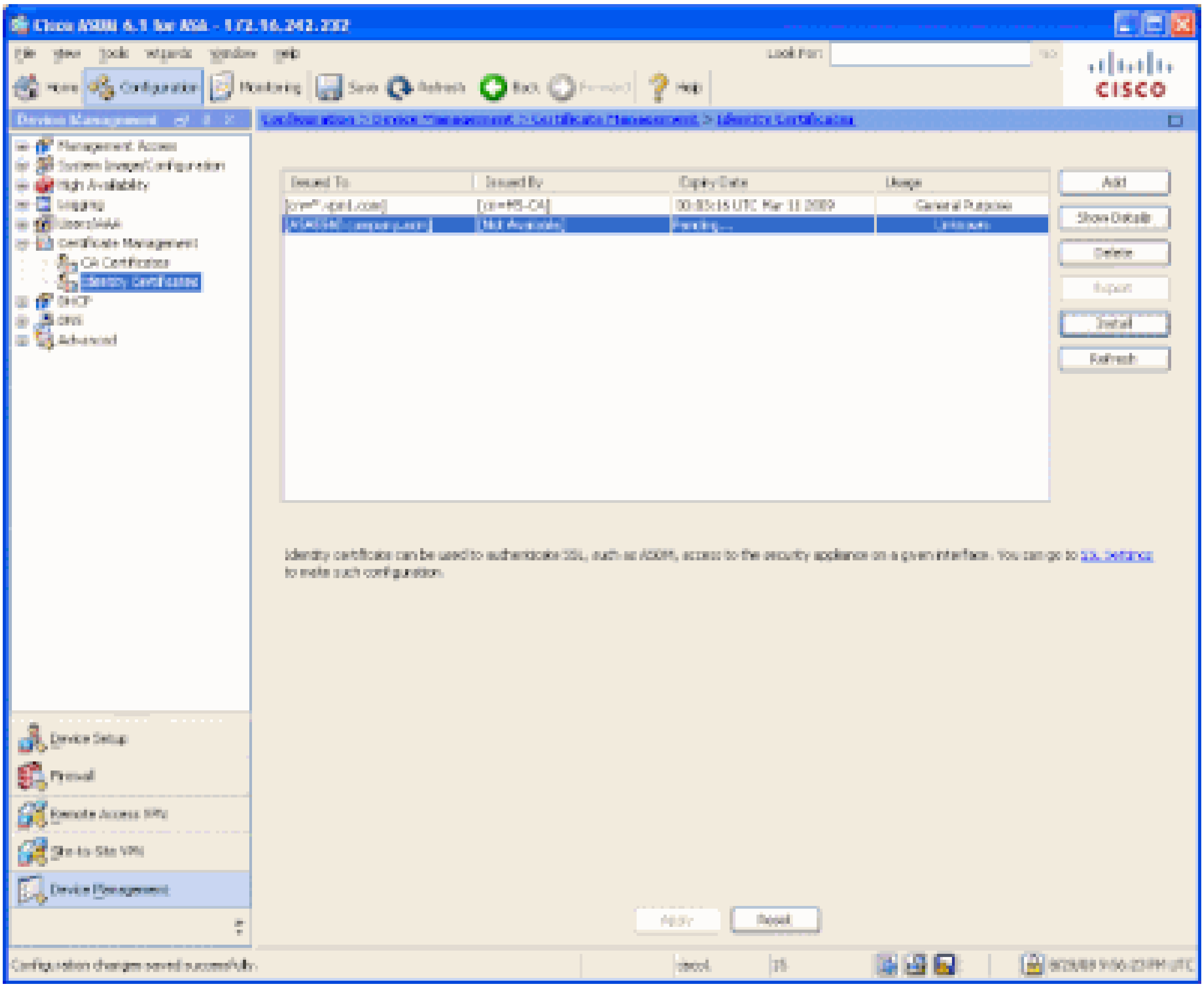
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

[redacted]

2. (Optional) Verify in ASDM that the CSR is pending.

Figure 6



Issued To	Issued By	Expiry Date	Usage
[cn=*.vpn1.com]	[cn=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose
[ASA5540.company.com]	[Not Available]	Pending...	Unknown

Identity certificate can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to SSL Settings to make such configuration.

Configuration changes saved successfully.

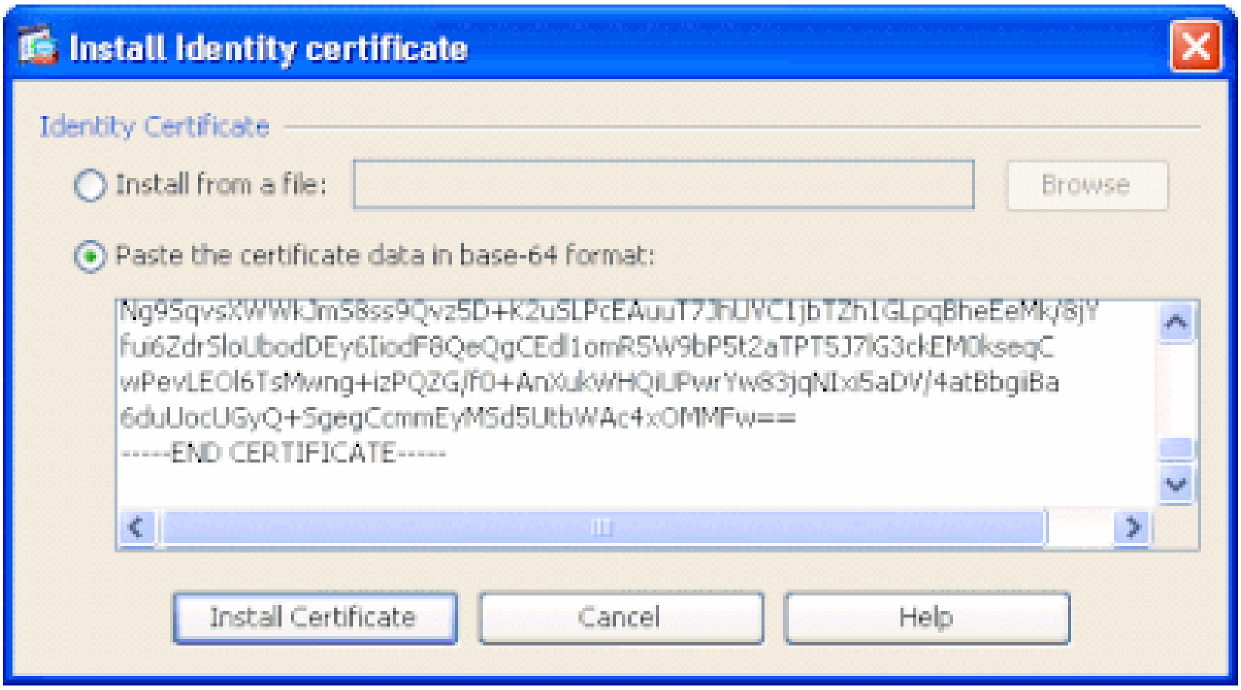
3. Submit the certificate request to the certificate administrator, who issues the certificate on the server.

This can either be through a web interface, e-mail, or directly to the root CA server for certificate issue process.

4. Complete these steps in order to install the renewed certificate.
    a. Select the certificate request under **Configuration > Device Management > Identity Certificates** , as shown in Figure 6, and click **Install**.
    b. In the **Install Identity Certificate** window, select the **Paste the certificate data in base-64 format** radio button, and click **Install Certificate**.

Note: Alternatively, if the certificate is issued in a .cer file rather then a text based file or e-mail, you can also select **Install** from a file, browse to the appropriate file on your PC, click **Install ID certificate file**, then click **Install Certificate**.

Figure 7



Install Identity certificate
Identity Certificate
○ Install from a file:
Browse
● Paste the certificate data in base-64 format:

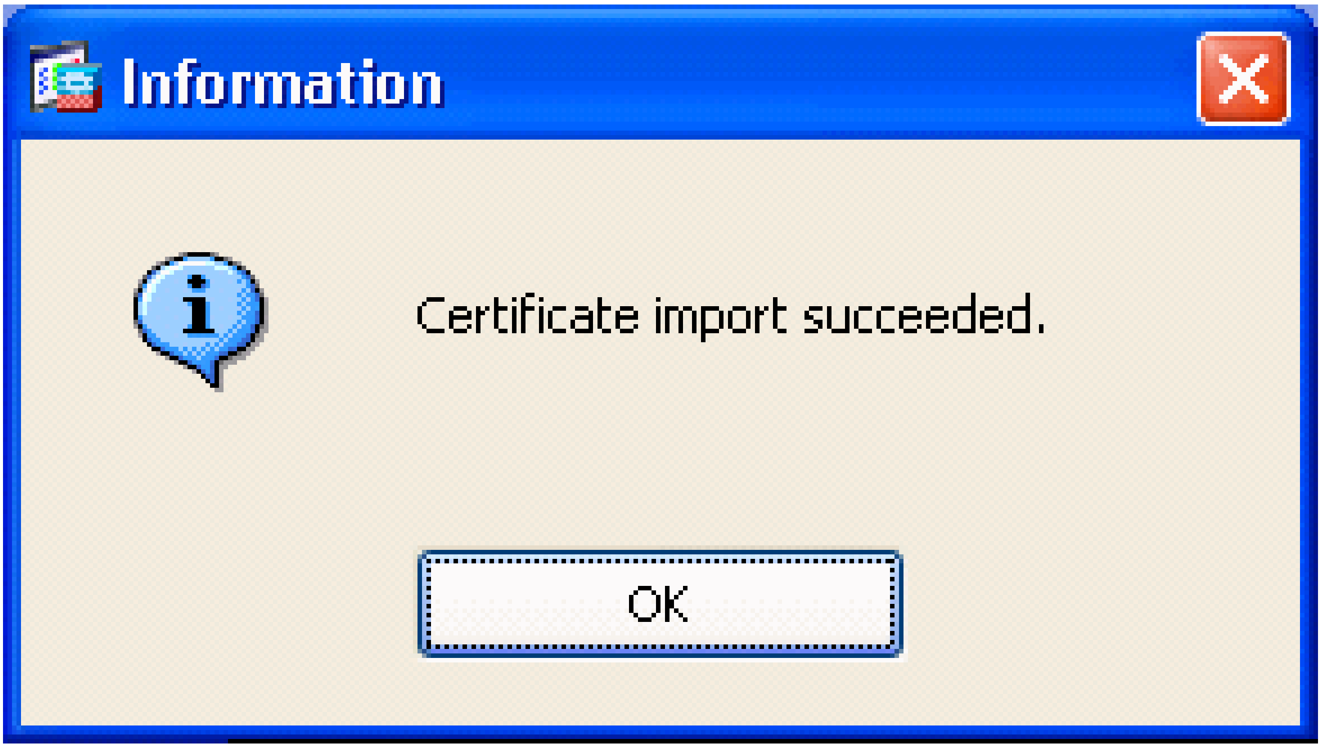
```
Ng9SqvsXWWkJm58ss9Qvz5D+K2uSLPcEAuuT7JhUVCIjbTZh1GLpqBheEeMk/8jY
fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw==
-----END CERTIFICATE-----
```

CLI output:

```
<#root>

crypto ca import ASDM_TrustPoint0 certificate

WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ

!--- output truncated

wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw==
        quit
```

5. A window appears that confirms the certificate is successfully installed. Click **OK** to confirm.

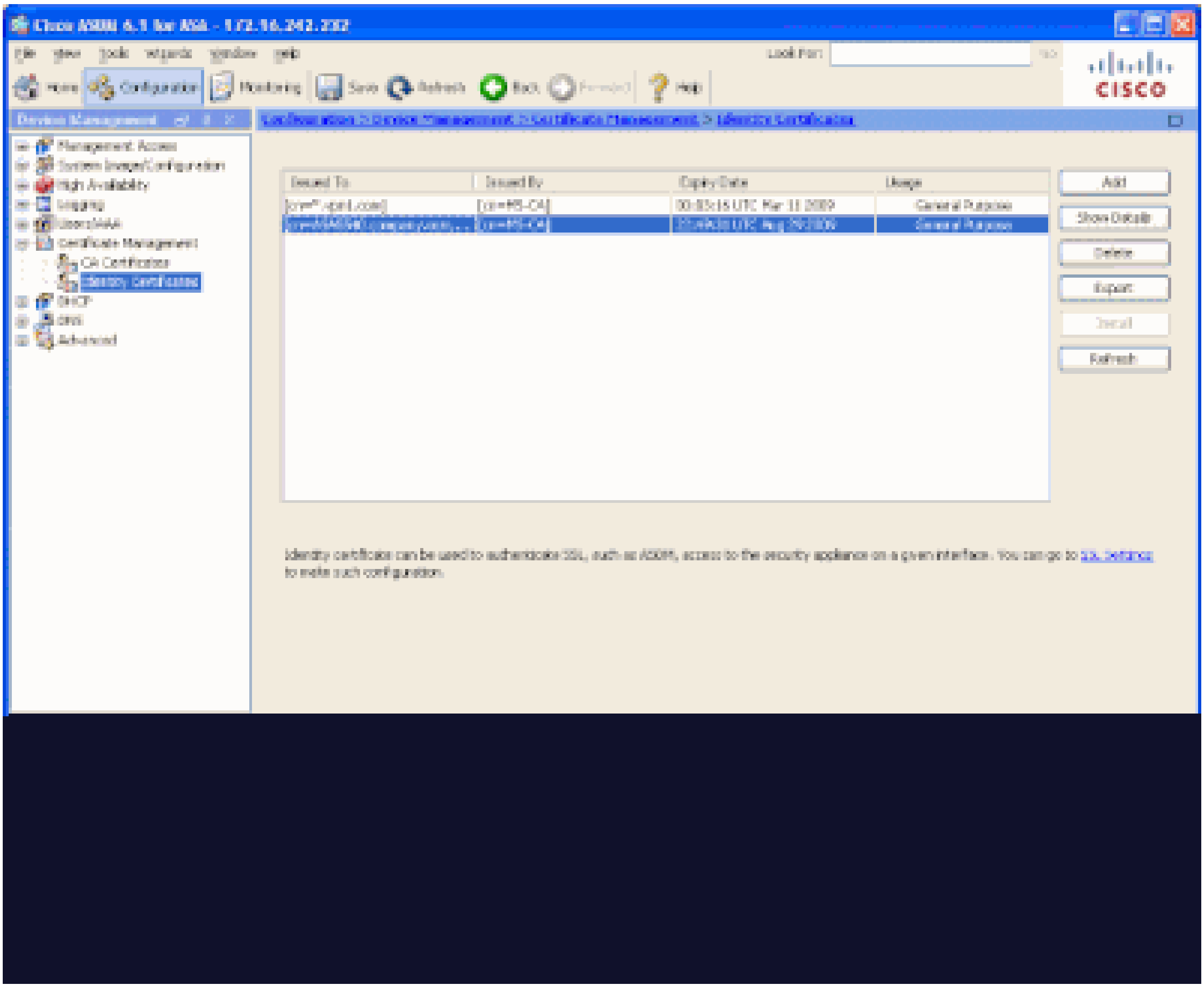
Figure 8



Certificate import succeeded.

6. Ensure your new certificate appears under **Identity Certificates**.

Figure 9



Issued To	Issued By	Expiry Date	Usage
[cn=*.vpnl.com]	[cn=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose
[cn=ASA5540.company.com,...	[cn=MS-CA]	[illegible] UTC Aug 29 2009	General Purpose

Identity certificate can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to SSL Settings to make such configuration.

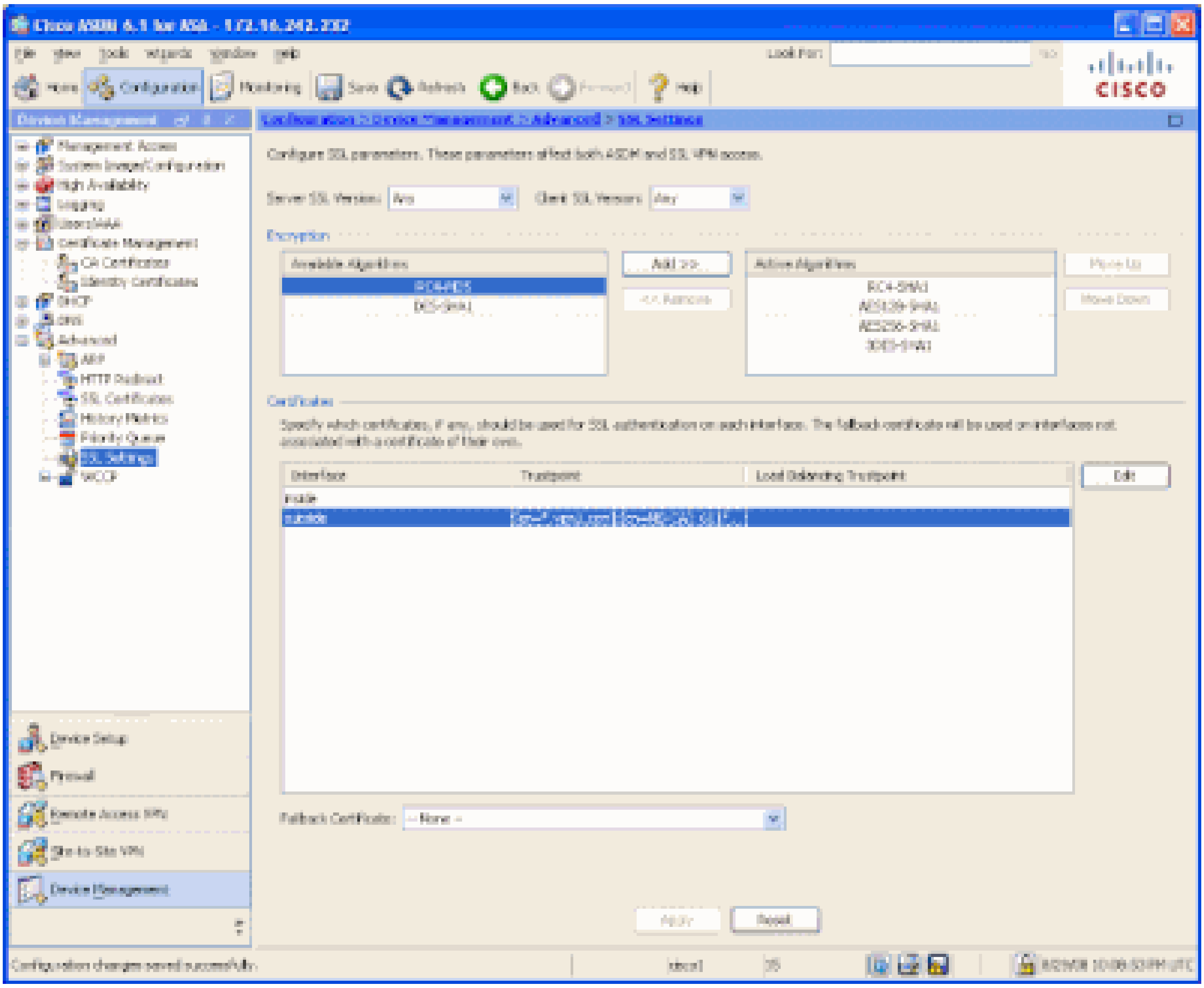
Cisco ASDM 6.1 for ASA - 172.16.242.232
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Device Management
Configuration > Device Management > Certificate Management > Identity Certificates
Management Access
System Image/Configuration
High Availability
Logging
Users/AAA
Certificate Management
CA Certificates
Identity Certificates
DHCP
DNS
Advanced
Add
Show Details
Delete
Export
Install
Refresh

7. Complete these steps in order to bind the new certificate to the interface:

   a. Choose **Configuration > Device Management > Advanced > SSL Settings** , as shown in Figure 10.

   b. Select your interface under **Certificates**. Click **Edit**.

Figure 10



Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

Server SSL Version: Any

Client SSL Version: Any

Available Algorithms: RC4-MD5, DES-SHA1

Active Algorithms: RC4-SHA1, AES128-SHA1, AES256-SHA1, 3DES-SHA1

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Trustpoint	Load Balancing Trustpoint
inside		
outside	[illegible]	

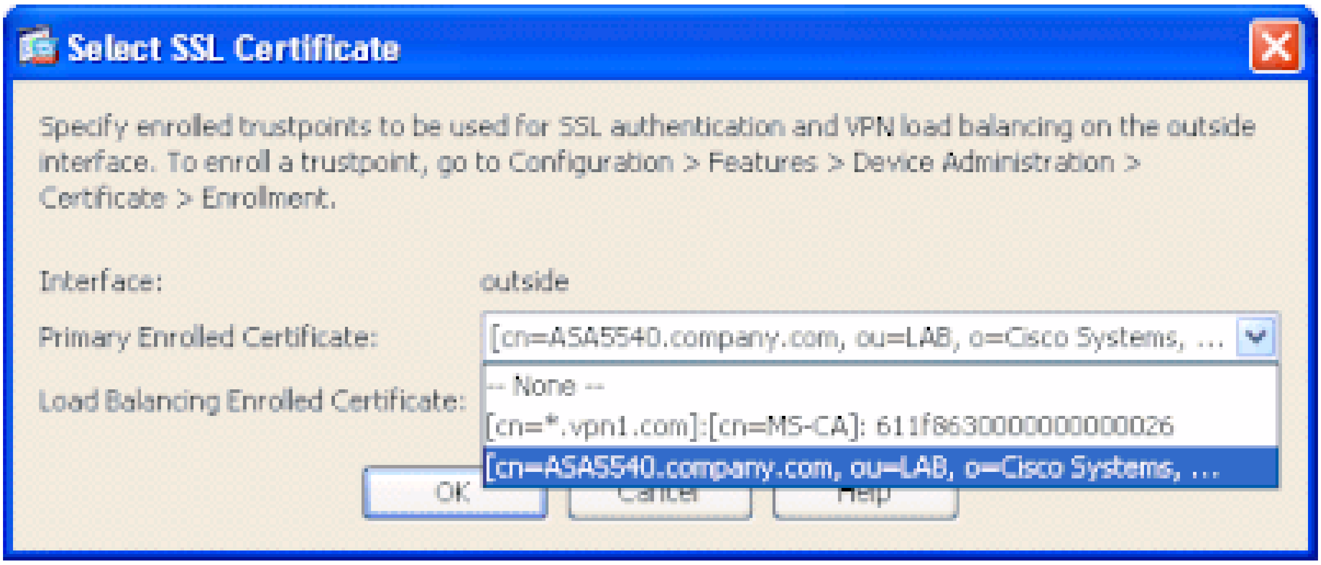
Fallback Certificate: -- None --

Configuration changes saved successfully.

8. Choose your new certificate from the drop-down menu, click **OK**, then click **Apply**.

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

Figure 11



Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.

Interface: outside

Primary Enrolled Certificate: [cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, ...

Load Balancing Enrolled Certificate:

-- None --
[cn=*.vpn1.com]:[cn=MS-CA]: 611f8630000000000026
[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, ...

9. Save your configuration in either ASDM or on the CLI.

Verify

You can use the CLI interface in order to verify that the new certificate is installed to the ASA correctly, as shown in this sample output:

<#root>

```
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=websiteaddress
!---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)#
```

Troubleshoot

(Optional) Verify on the CLI that the correct certificate is applied to the interface:

```
<#root>

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)#
```

How to Copy SSL Certificates from One ASA to Another

This can be done if you had generated exportable keys. You need to export the certificate to a PKCS file. This includes export of all of the associated keys.

Use this command to export your certificate via CLI:

```
<#root>

ASA(config)#

crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Note: A Passphrase is used to protect pkcs12 file.

Use this command to import your certificate in the CLI:

```
<#root>
```

```
SA(config)#

crypto ca import <trust-point-name> pkcs12 <passphrase>
```

Note: This passphrase must be the same as the one used when the file is exported.

This can also be done through ASDM for an ASA failover pair. Complete these steps to perform this:

1. Log into the primary ASA via ASDM and choose **Tools** > **Backup Configuration**.
2. You can backup everything or just the certificates.
3. On the standby, open ASDM and choose **Tools** > **Restore Configuration**.

Related Information

- Cisco Adaptive Security Appliance (ASA) Support Page

- **Technical Support & Documentation - Cisco Systems**