

# VPN 3000 Concentrator and VPN Client Authentication using SC2 (TM) Apollo OS Smart Card Configuration Example

Document ID: 62992

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Setup

- Windows 2003 Enterprise Certificate Authority Installation
- Windows 2003 Enterprise Certificate Authority Configuration
- User's Smart Card Digital Certificate Request
- VPN Client Setup
- VPN 3000 Concentrator Configuration
- VPN Concentrator Identity Certificate (VPN Certificate) Request
- VPN Client Configuration

#### Verify

#### Troubleshoot

#### Related Information

## Introduction

**Contributing Author:** Eyal Webber–Zvik, SCsquare Ltd.

This document describes how to use the SC<sup>2</sup>™ Ltd. Apollo OS Smart Card for a secured, smart card–based authentication between a Cisco VPN Client and a Cisco VPN 3000 Concentrator.

This document is based on a lab test completed with a Windows 2003 Enterprise Server and Certificate Authority (CA), a Windows XP Professional workstation, and a Cisco VPN 3000 Concentrator.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN 3000 Concentrator version 4.1.3 Released 12–Apr–2004
- Cisco VPN Client 4.0.3 (D)
- SC<sup>2</sup>™ Apollo OS Smart Card (contact interface) versions 2.3, 2.4, and 2.41
- SC<sup>2</sup>™ Apollo OS Smart Card (dual interface) version 3.01
- SC<sup>2</sup>™ Cryptographic Service Provider (CSP) version 3.11

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, make sure that you understand the potential impact of any command.

## Conventions

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

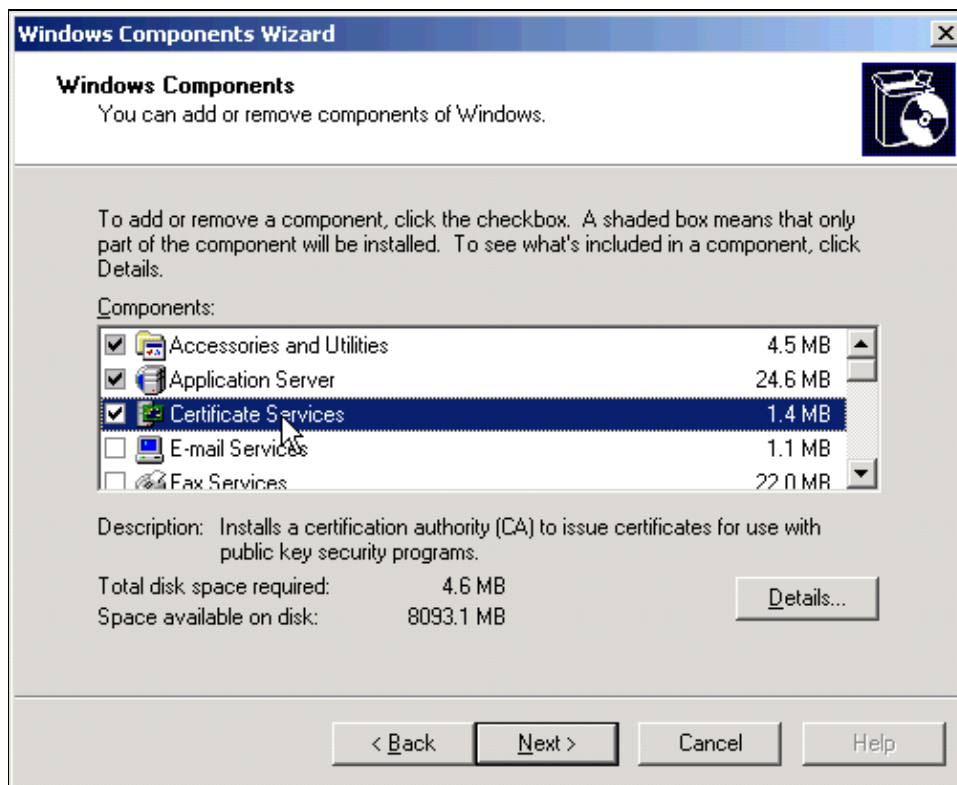
## Setup

Use the procedures in these sections to configure the VPN 3000 Concentrator and VPN Client Authentication with the use of the SC<sup>2</sup>™ Apollo OS Smart Card.

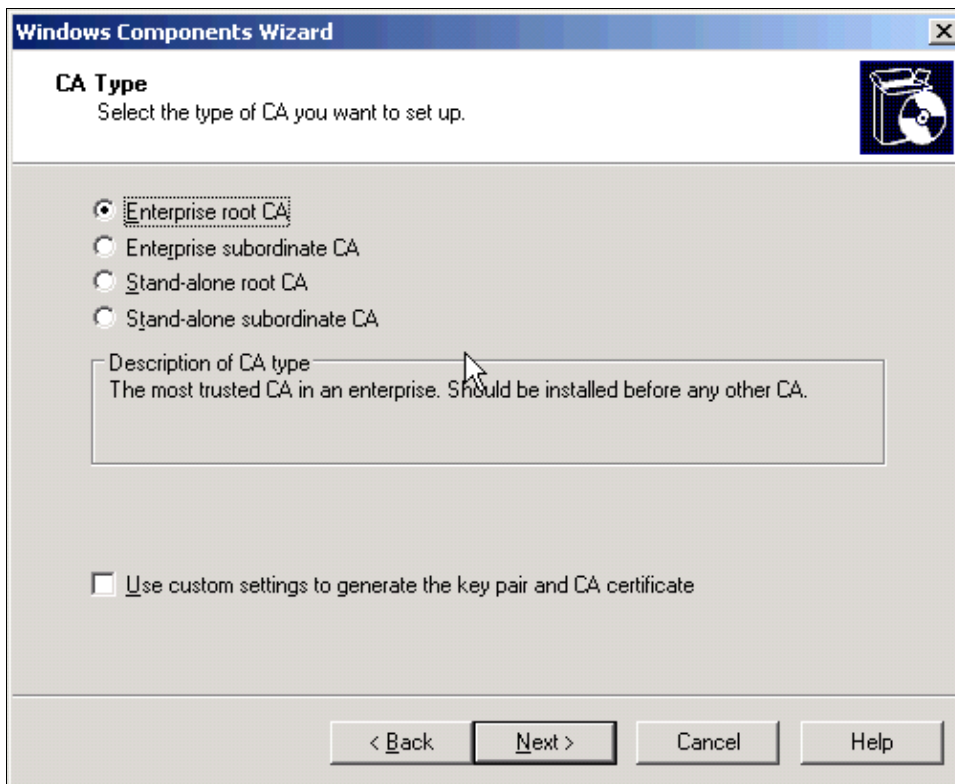
## Windows 2003 Enterprise Certificate Authority Installation

Complete these steps in order to install the Windows 2003 Enterprise Certificate Authority.

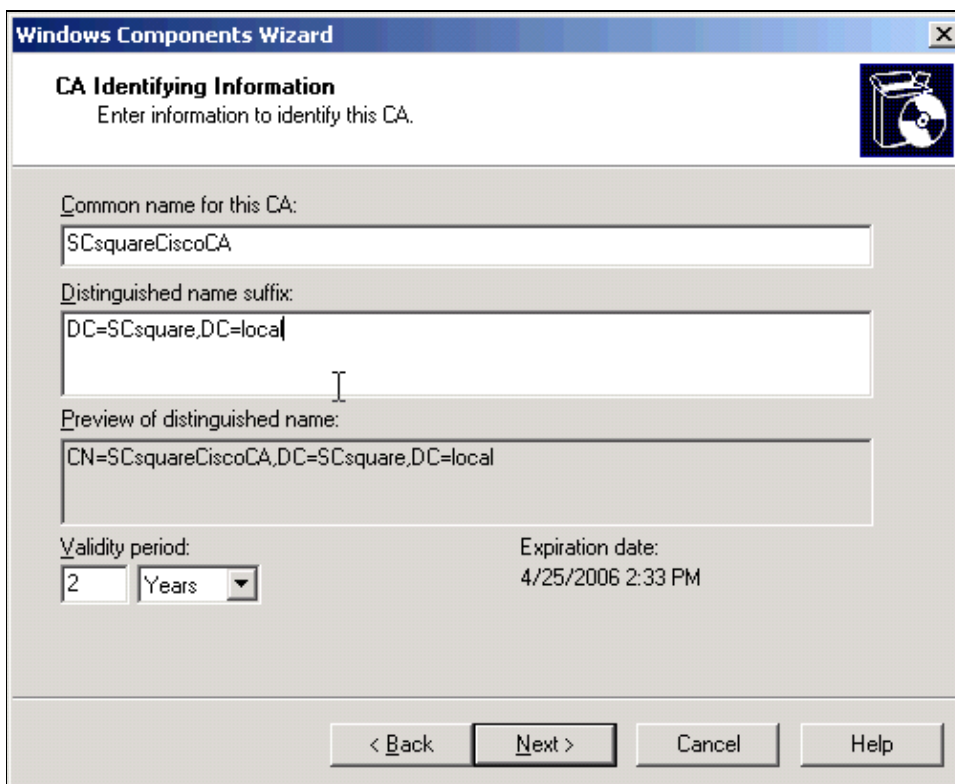
1. Choose **Control Panel > Add or Remove Programs > Add/Remove Windows Components**.
2. Check **Certificate Services** and click **Next**.



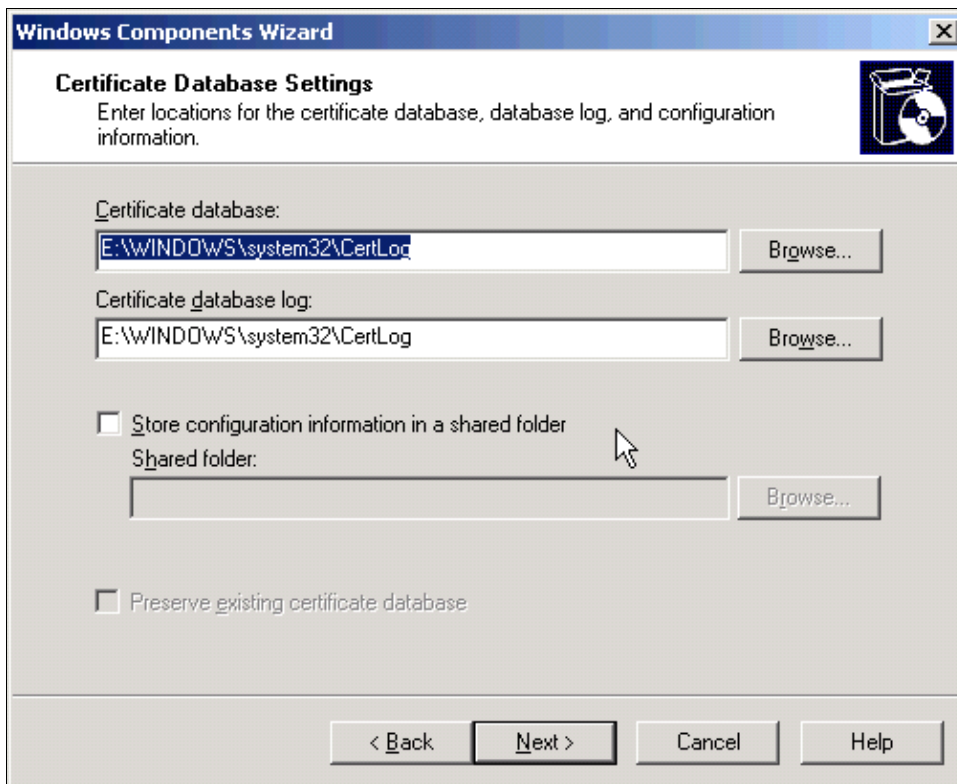
3. Choose **Enterprise root CA** or **Stand-alone root CA** (this depends on your PKI architecture) and click **Next**.



4. Enter the common name for your CA, set the validity period of its certificate, and click **Next**.



5. It is recommended to leave these fields with their default values and click **Next**.



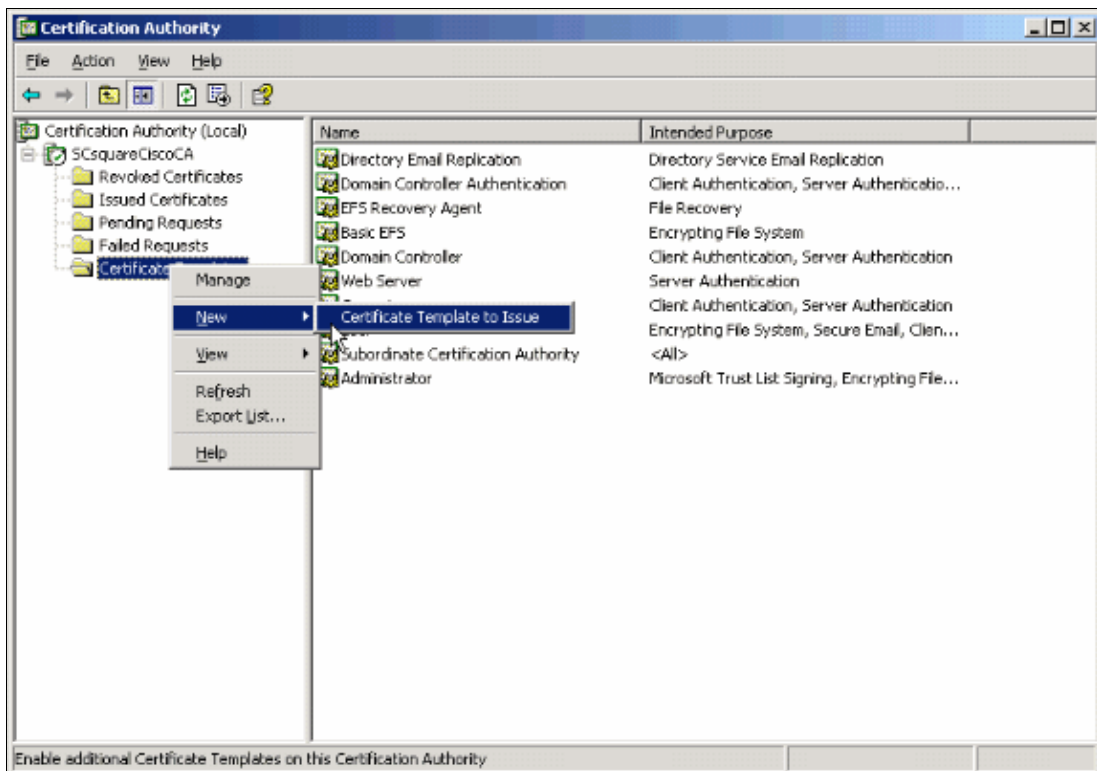
6. Click **Finish**.



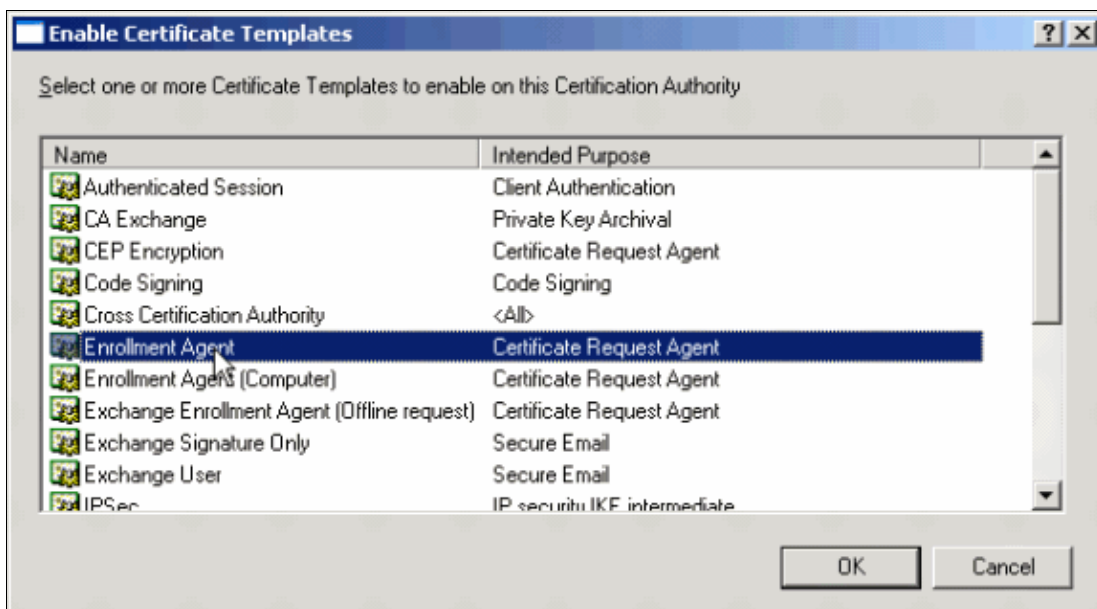
## Windows 2003 Enterprise Certificate Authority Configuration

Complete these steps in order to configure Windows 2003 Enterprise Certificate Authority.

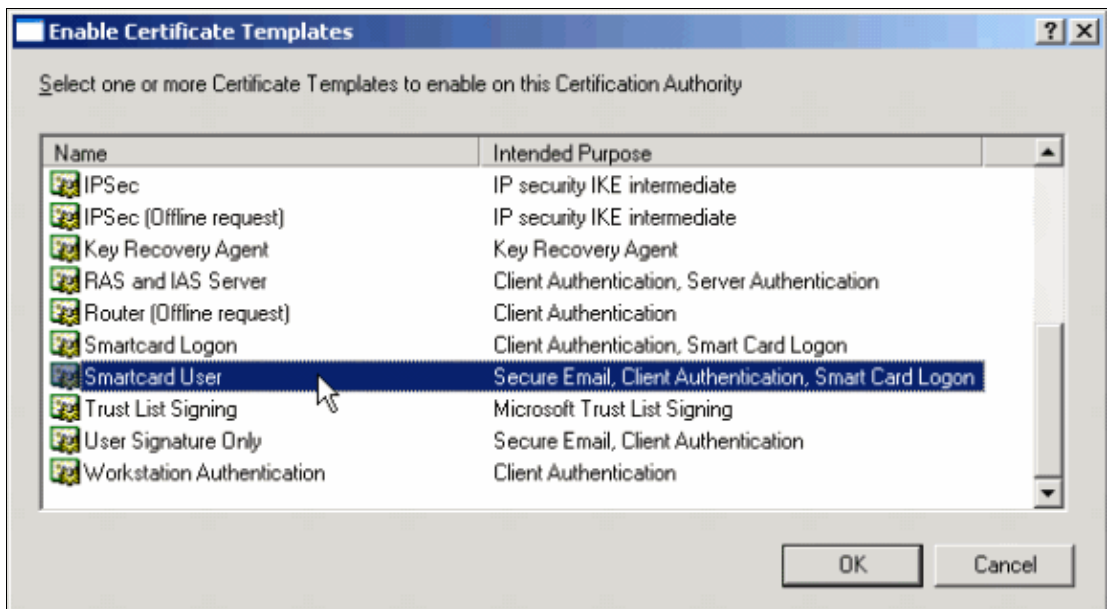
1. Choose **Control Panel > Administrative Tools > Certificate Authority**.
2. Right click on **Certificate Templates** and choose **New > Certificate Template to Issue**.



3. Choose the **Enrollment Agent** certificate template and click **OK**.



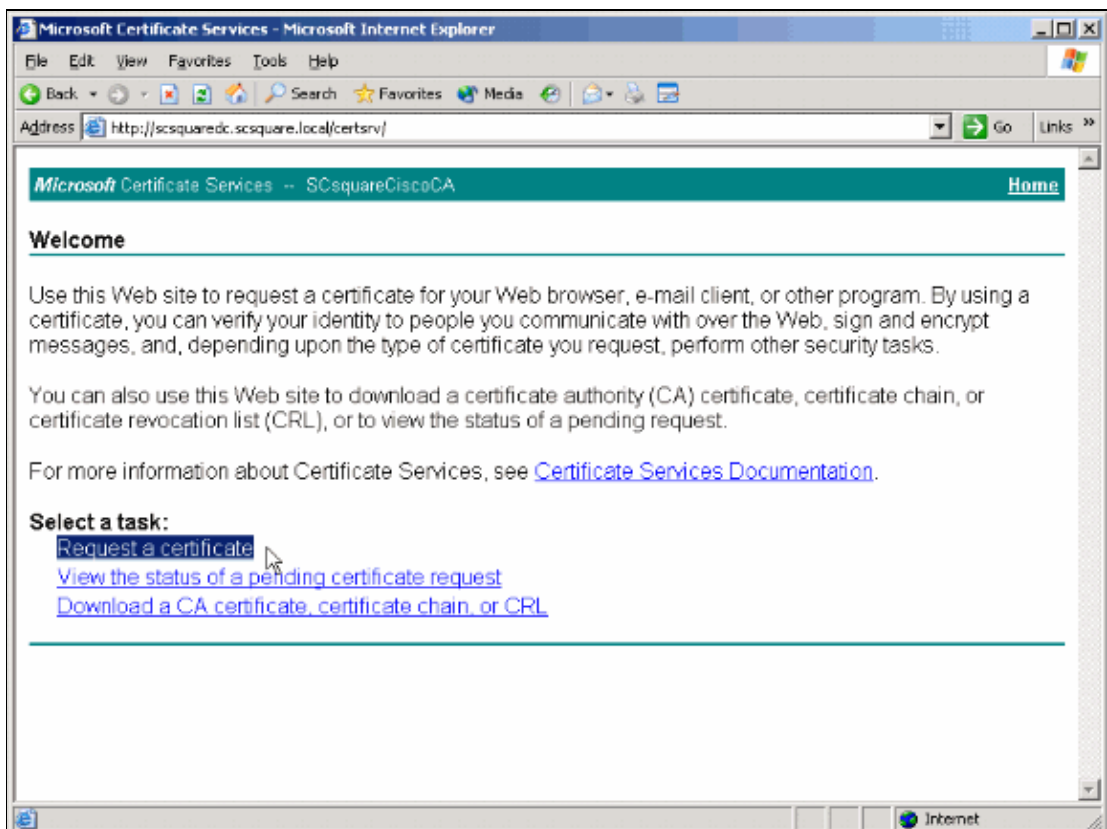
4. Repeat steps 1 through 3, choose the **Smartcard User** certificate template, and click **OK**.



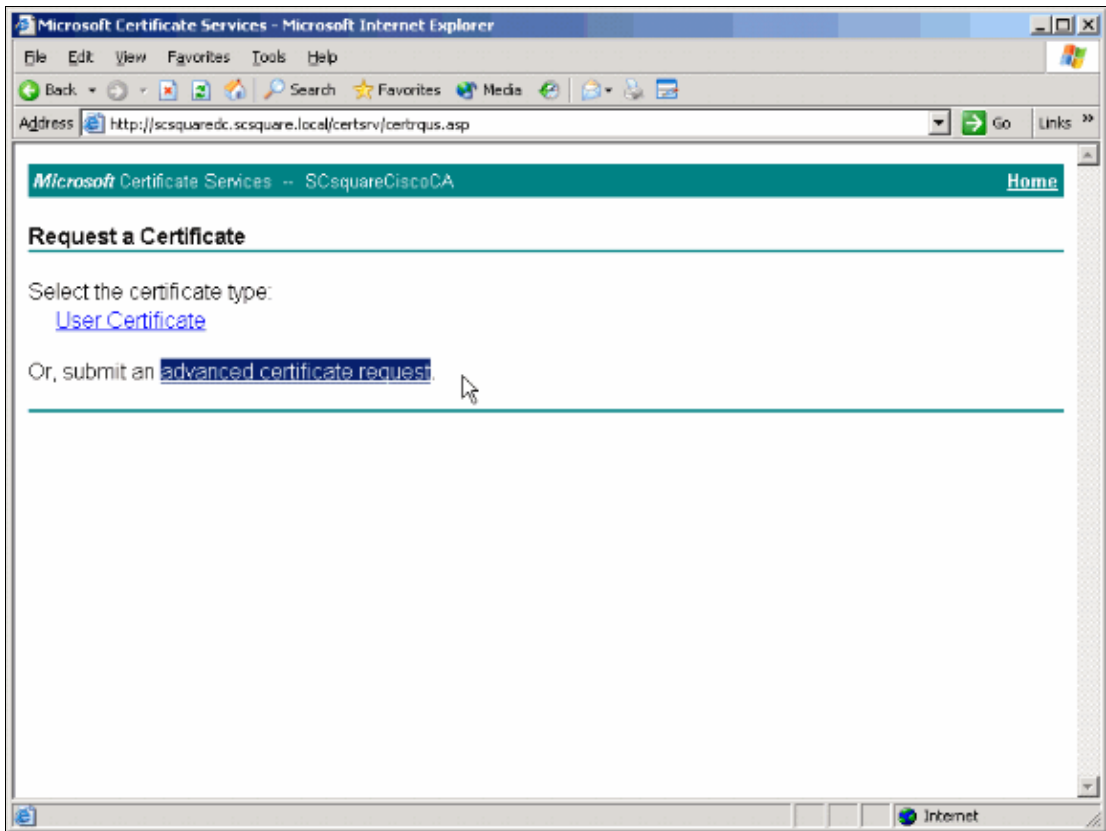
## User's Smart Card Digital Certificate Request

Complete these steps to request a user's smart card digital certificate.

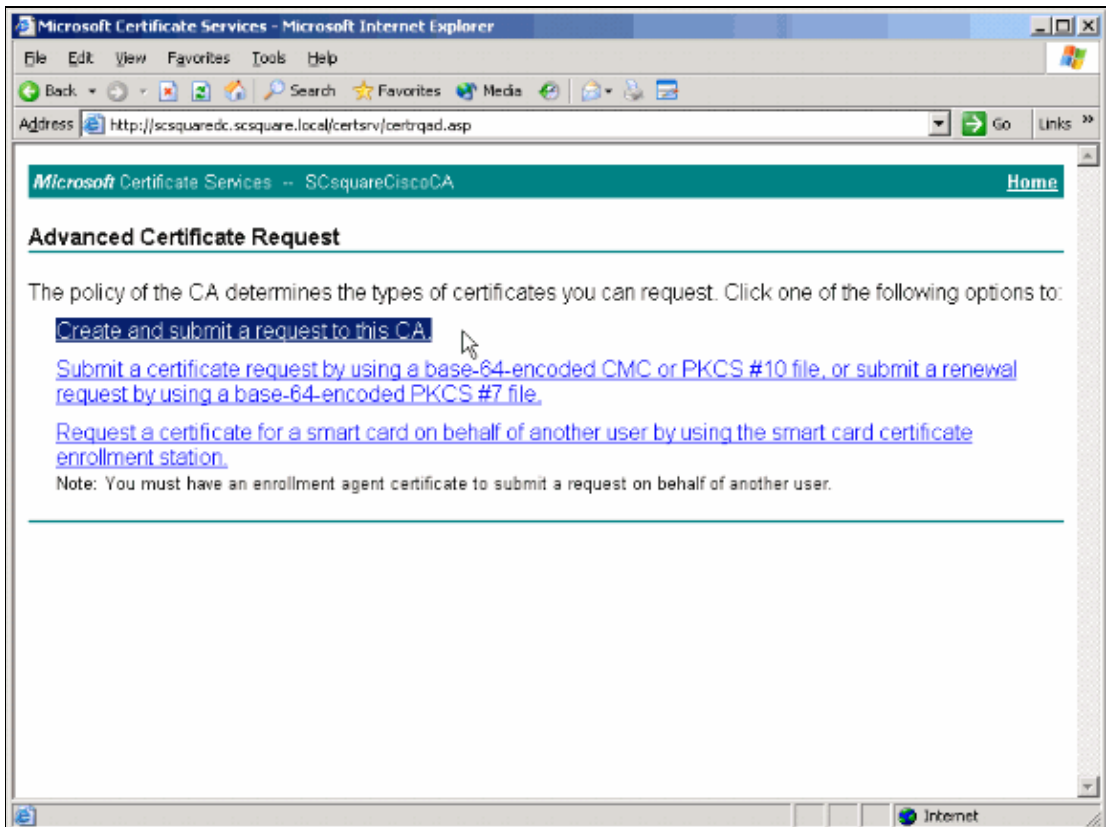
1. Go to the Certificate Authority web interface.
2. Choose **Request a certificate**.



3. Choose **advanced certificate request**.



4. Choose **Create** and submit a request to this CA.

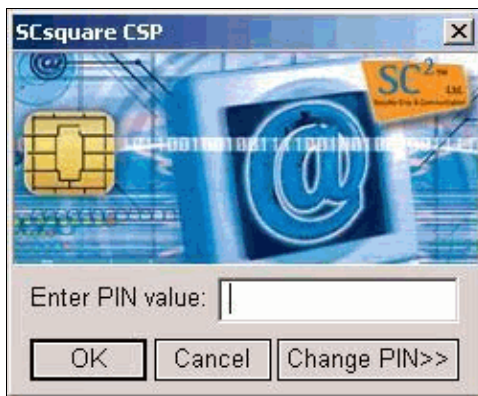
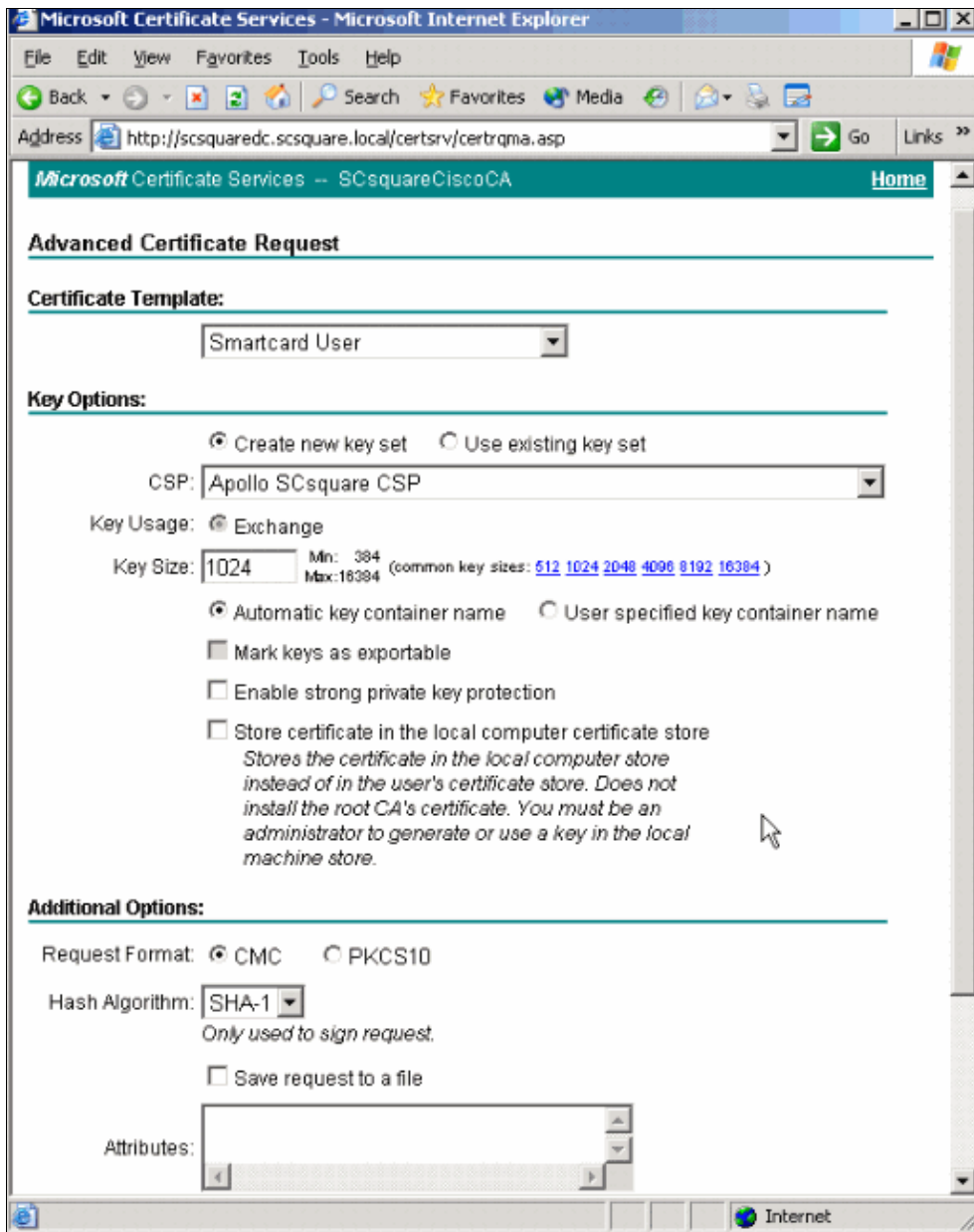


5. Choose the **Smartcard User** certificate template.

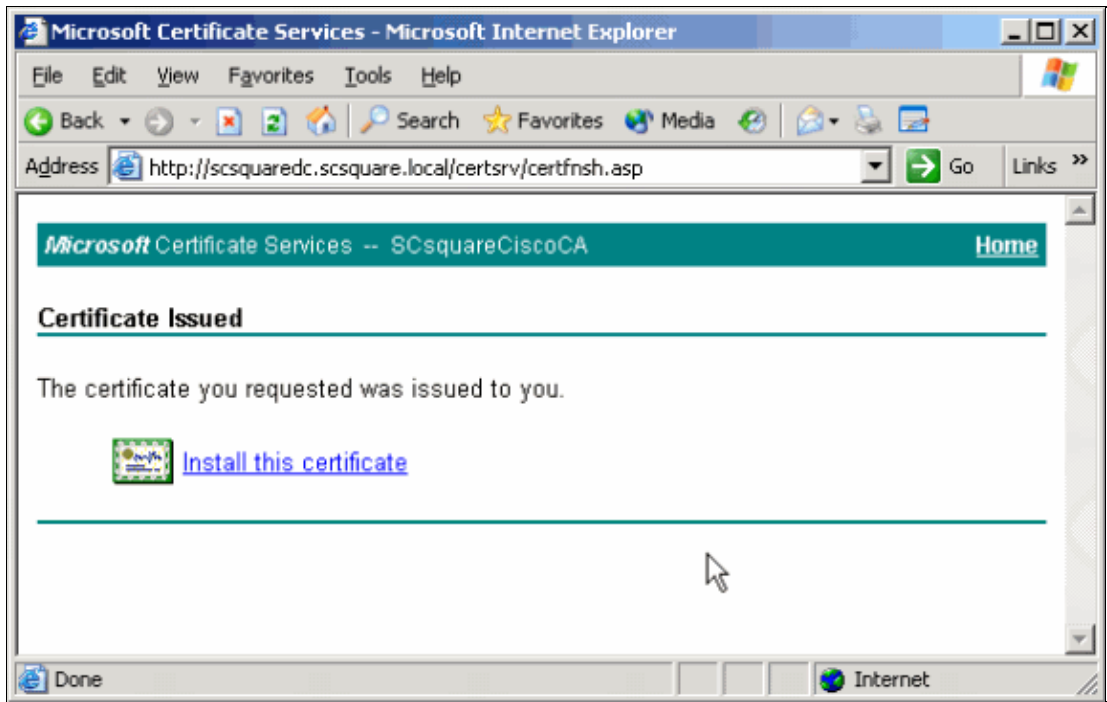
6. Choose **Apollo SC<sup>2</sup>™ CSP**.

7. Verify that all the selections in your form match the selections that the window in step 8 shows.

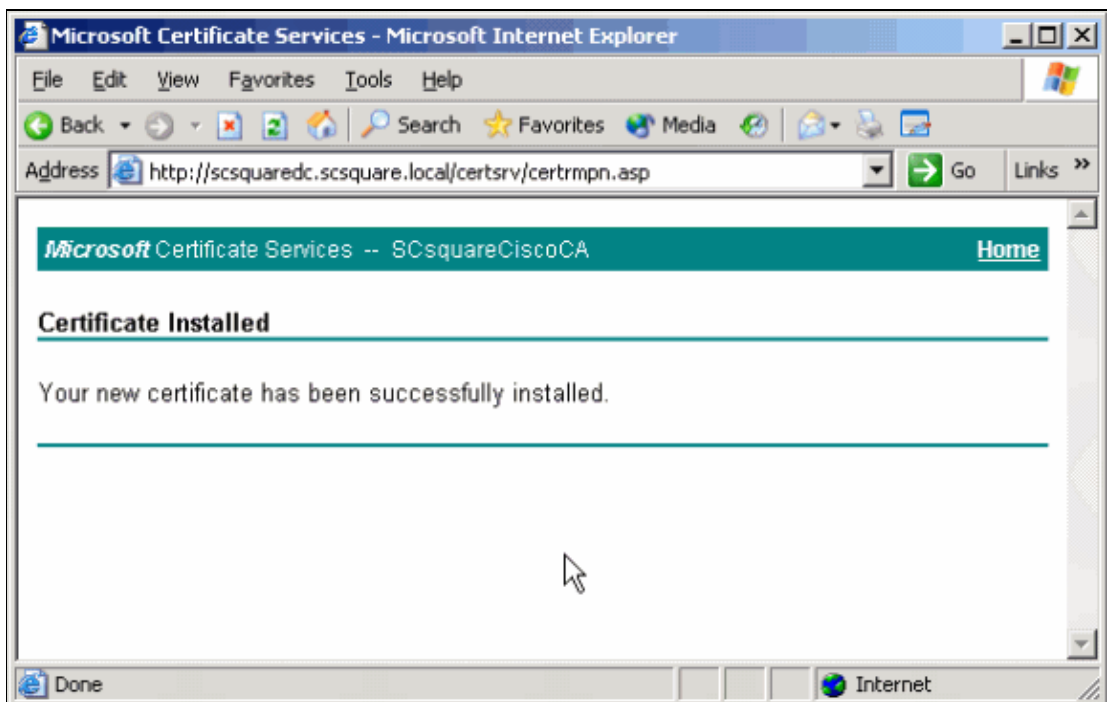
8. Click **Submit** and enter your PIN when requested.



9. Once the certificate is issued, click **Install this certificate** to have the certificate stored on your smart card.



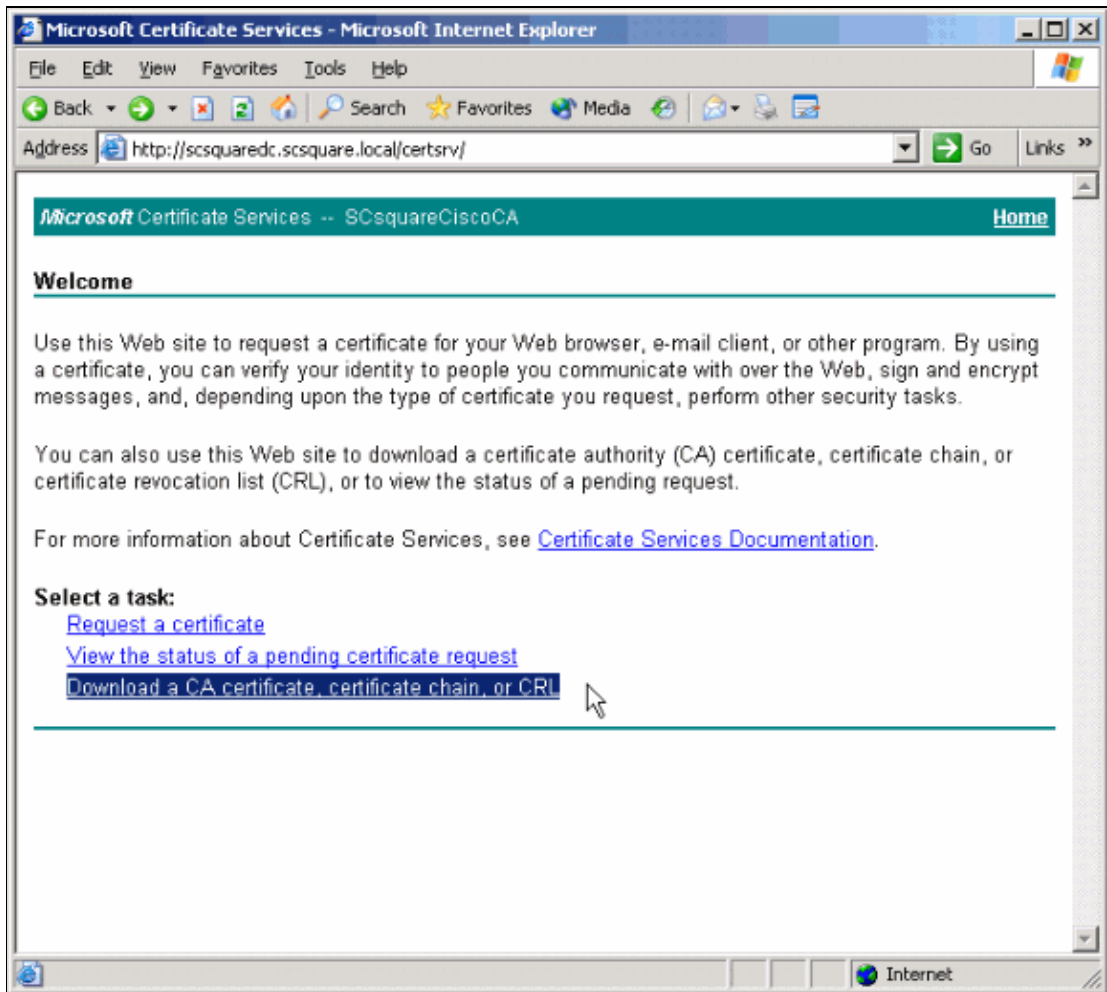
10. This message appears after a successful certificate installation.



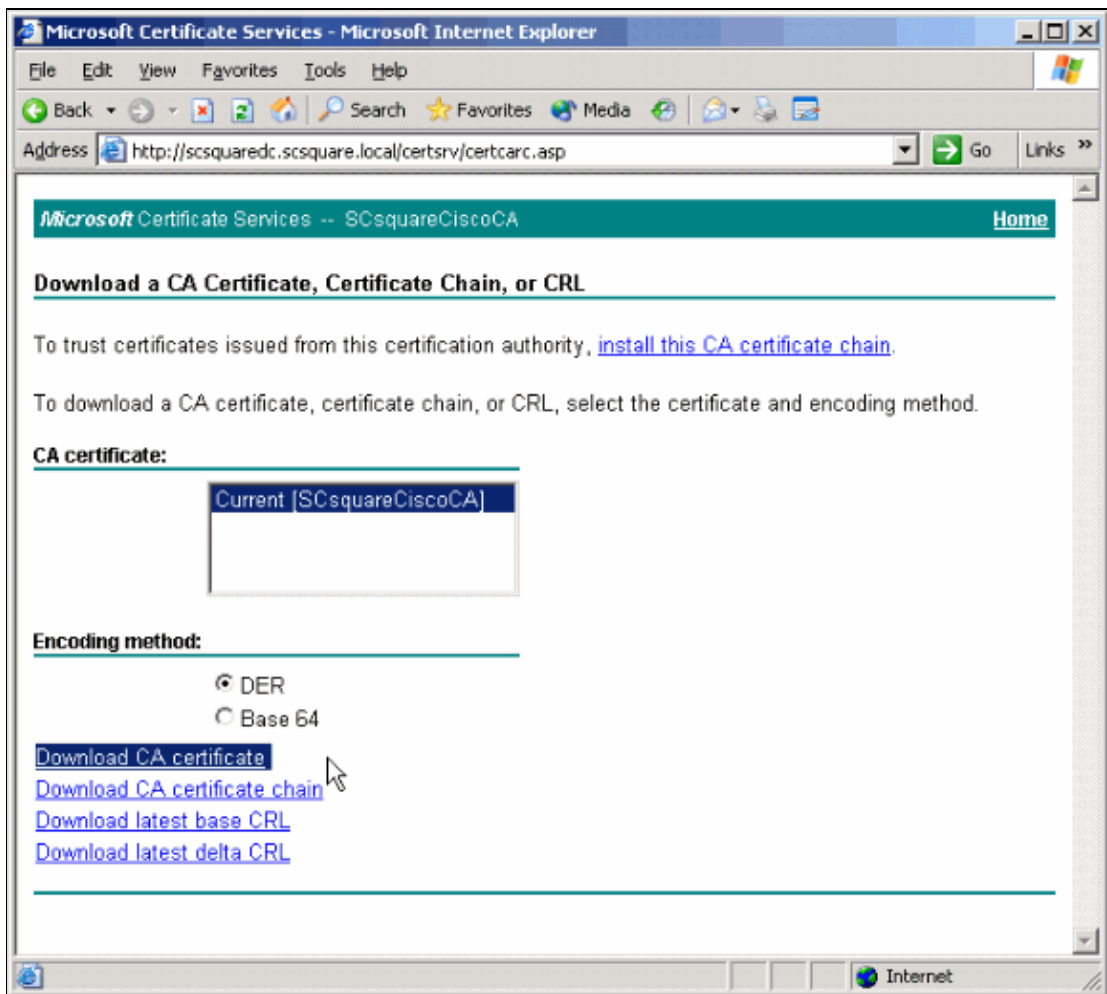
## VPN Client Setup

Complete these steps in order to setup the VPN Client.

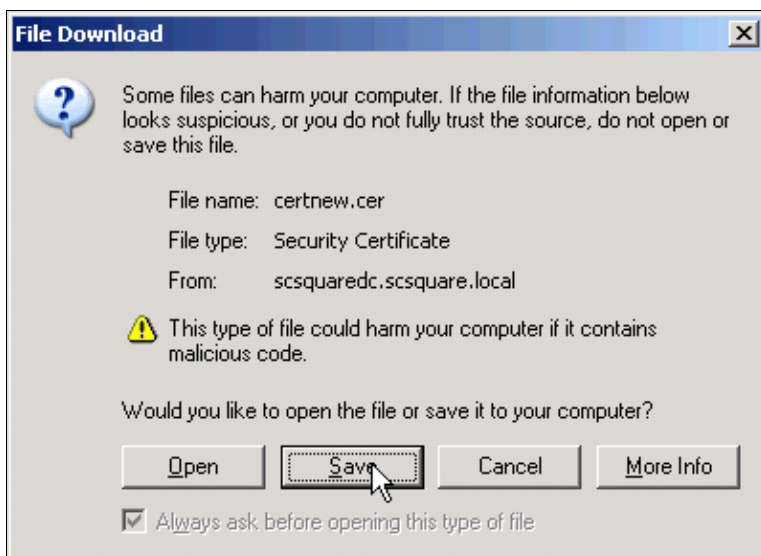
1. Open the browser and go to the CA's Certificate Services page.
2. Choose **Download a CA certificate, certificate chain, or CRL.**



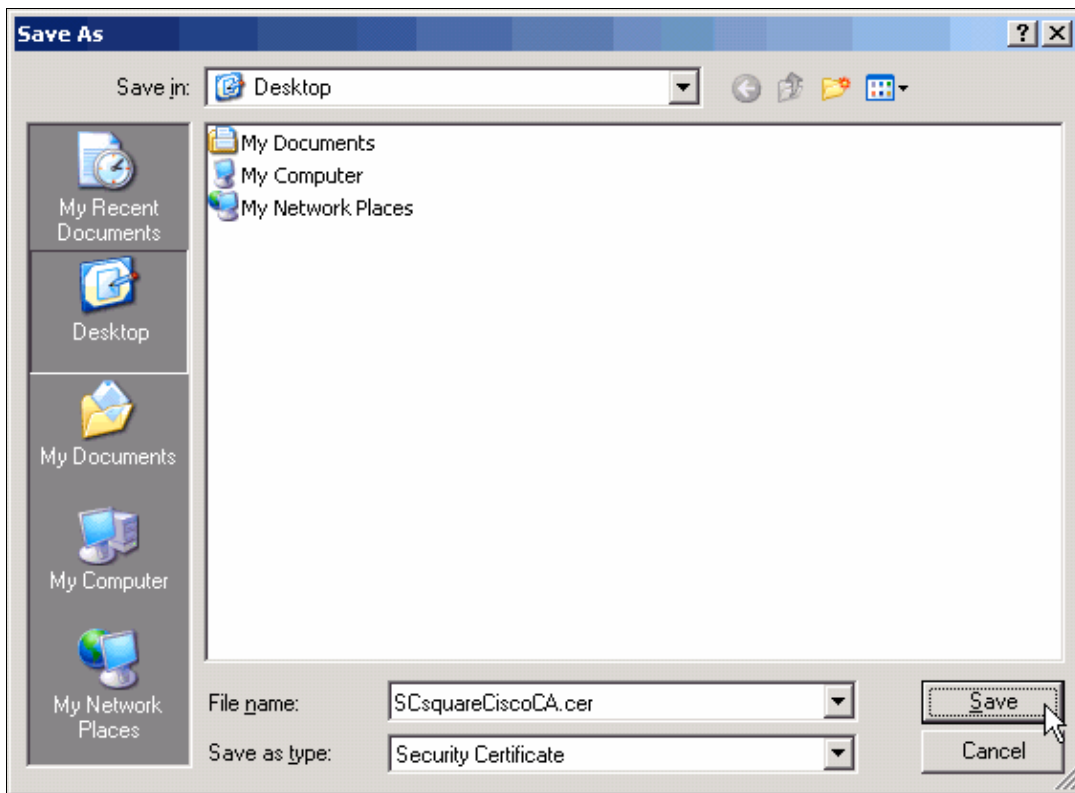
3. Verify that all the selections in your form match the selections that the window in step 4 shows.
4. Choose **Download CA certificate**.



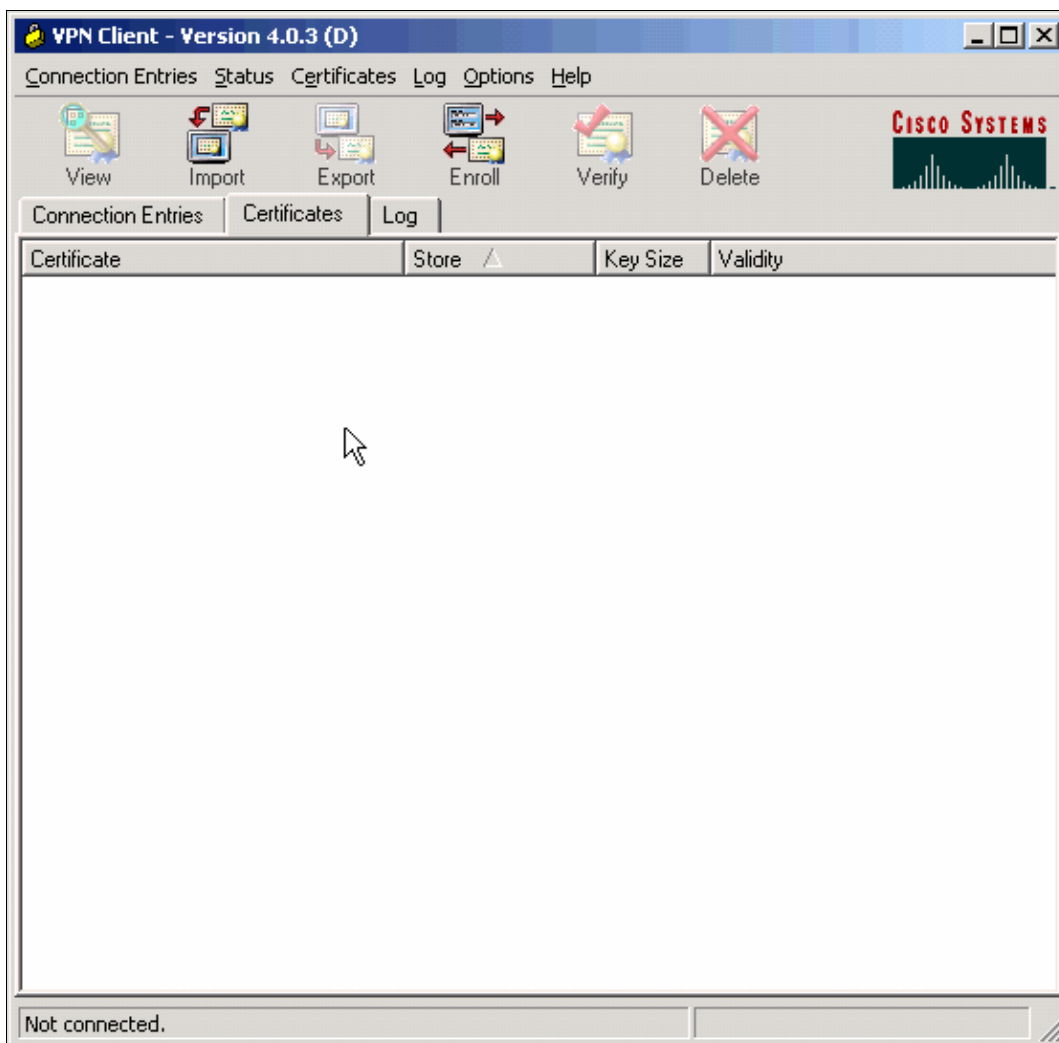
5. Click **Save** in order to save the downloaded certificate on your computer.



6. Choose the location on your computer to where you want to save the CA certificate.
7. Enter a name for the certificate and click **Save**.



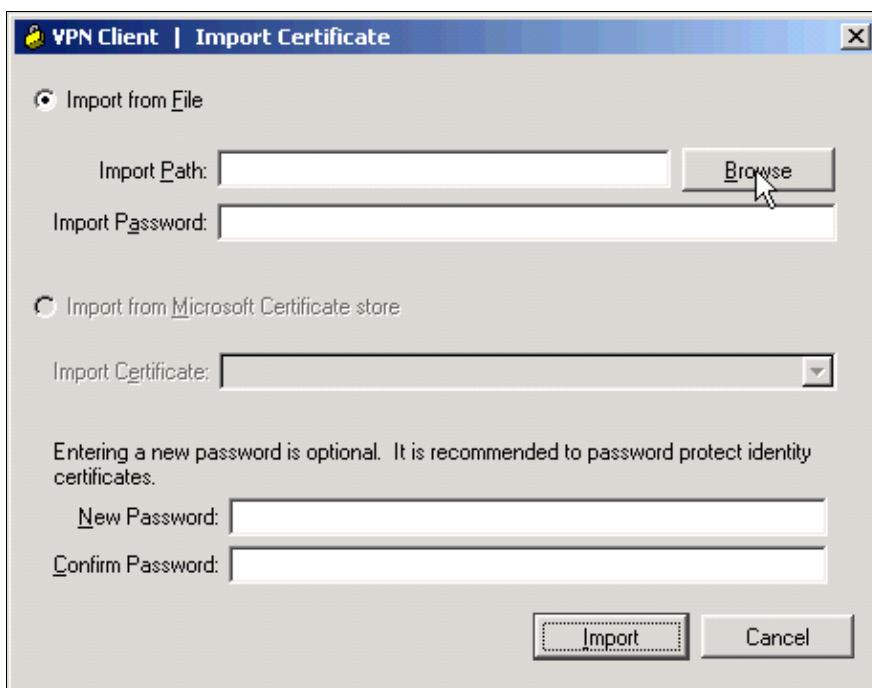
8. Start the VPN Client utility.



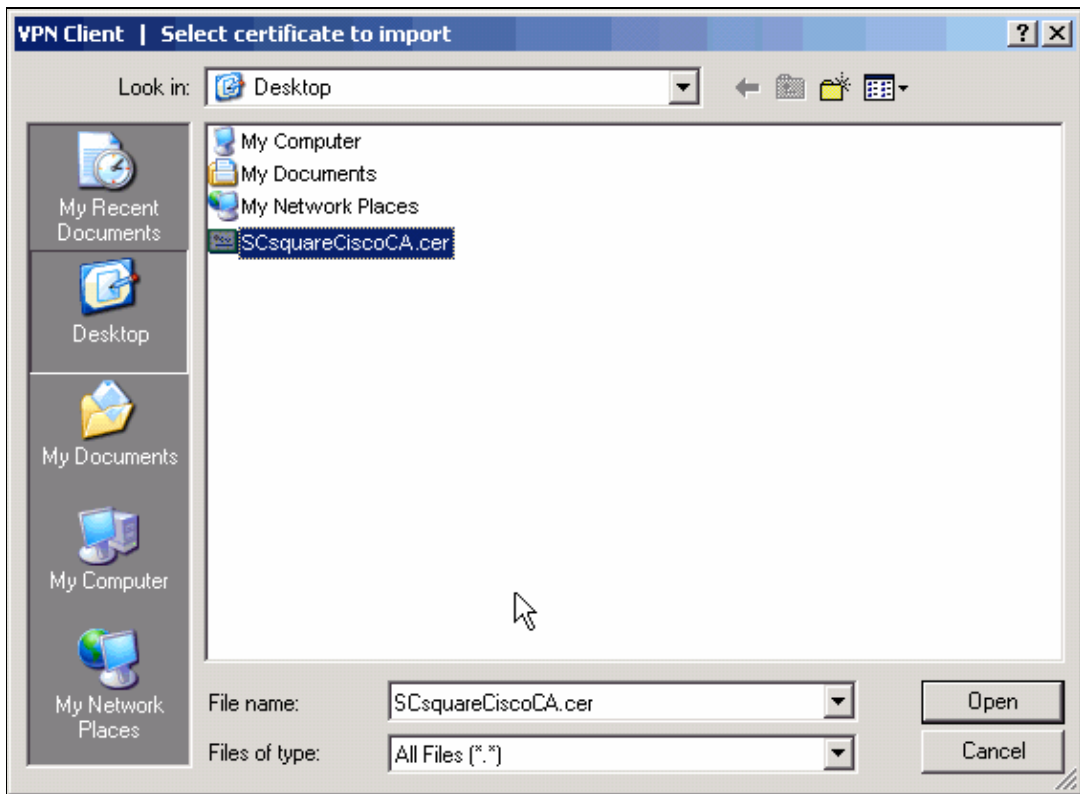
9. From the Certificates menu, enable the **Show CA/RA Certificate** option.
10. Click **Import**.



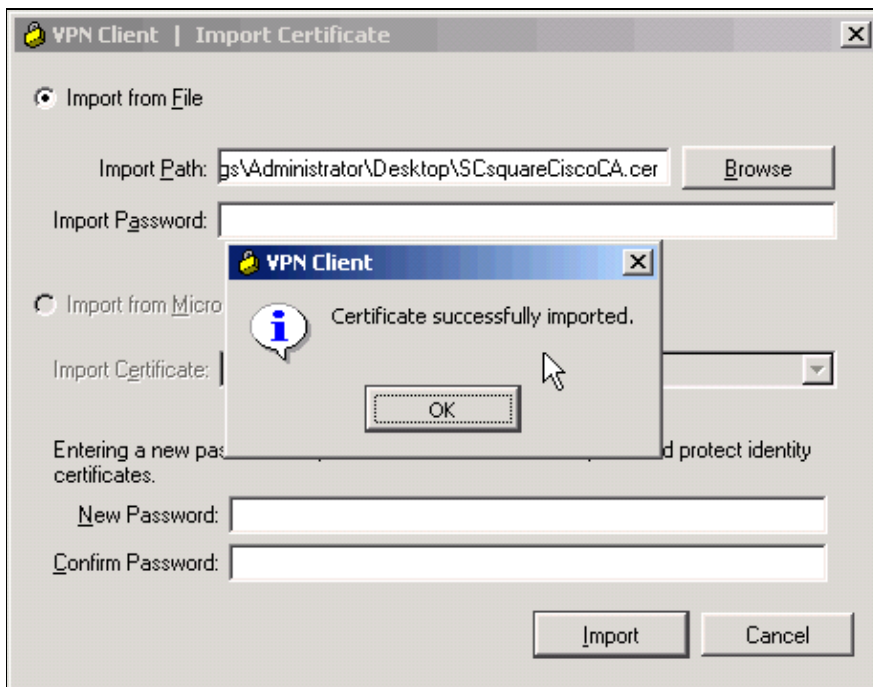
11. In the Import Certificate dialog, select **Import from file** and click **Browse**.



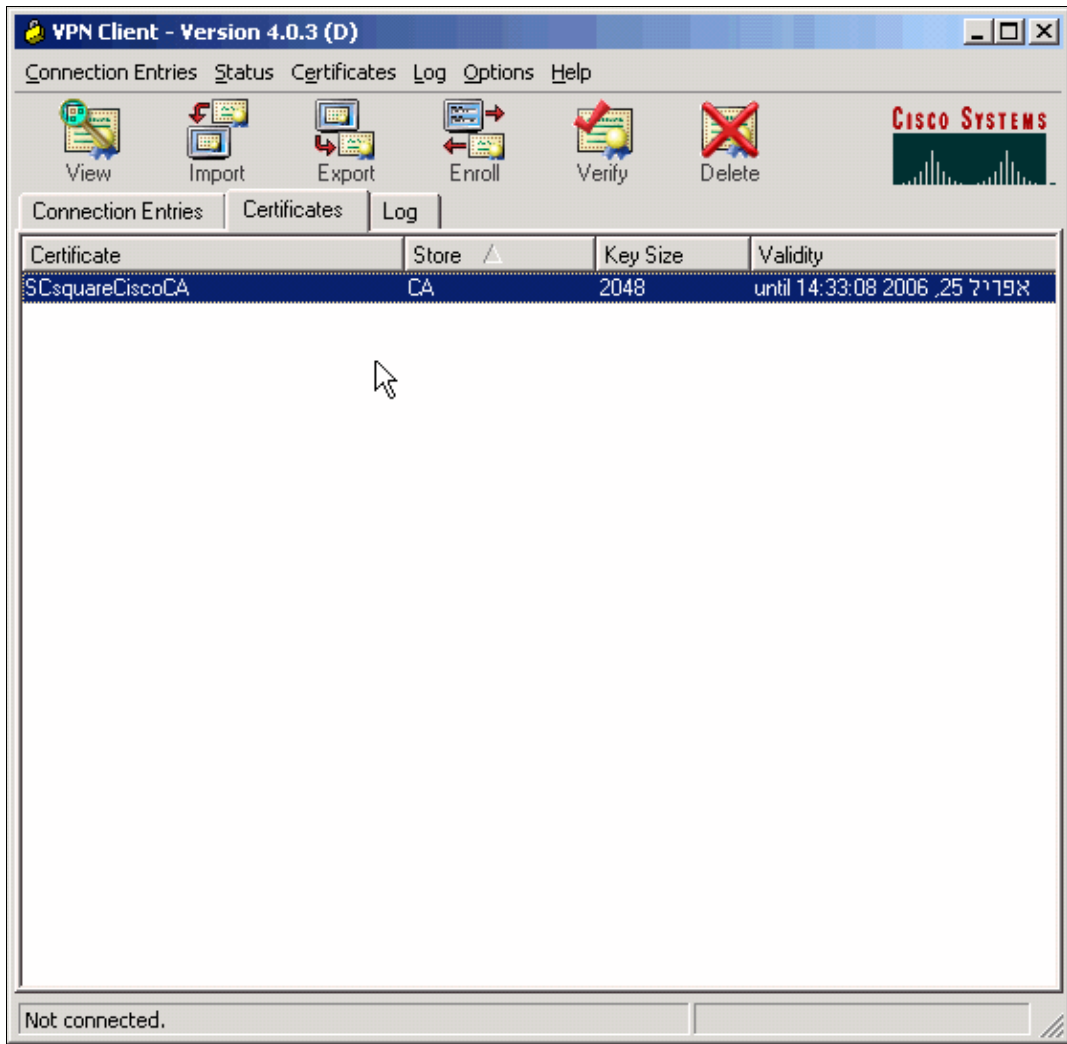
12. Choose the CA certificate you previously saved and click **Open**.



13. This message appears when you successfully import the certificate.



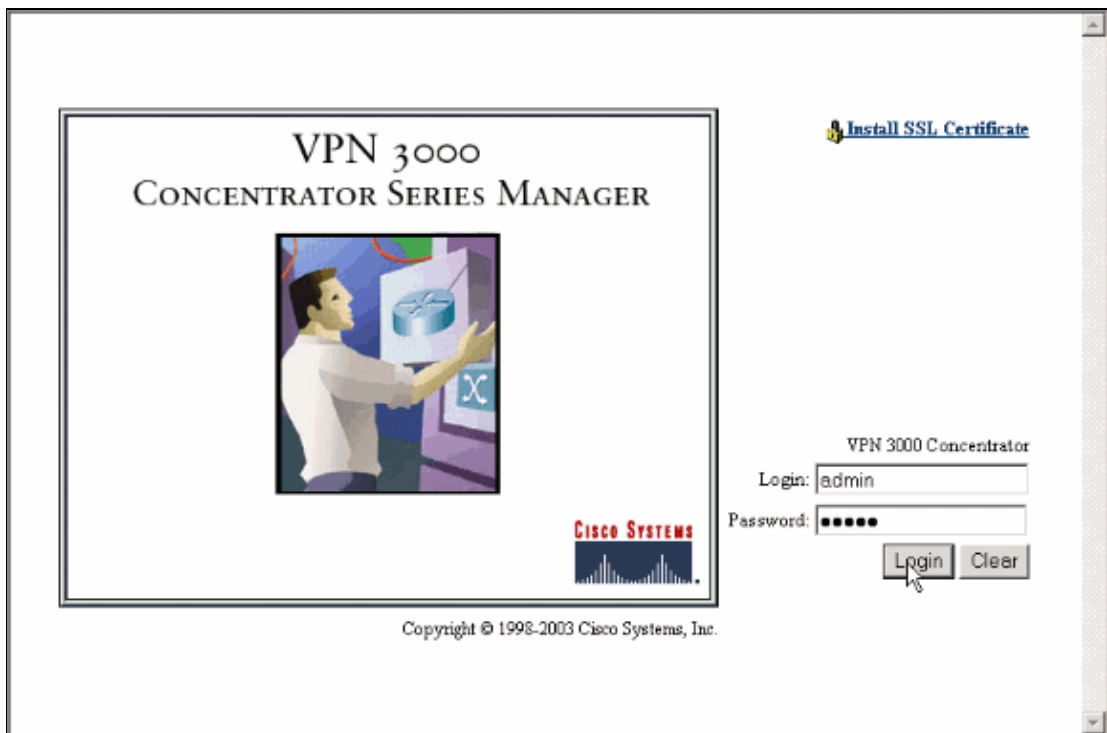
14. The CA certificate is now listed in the VPN Client application, under the Certificates tab.



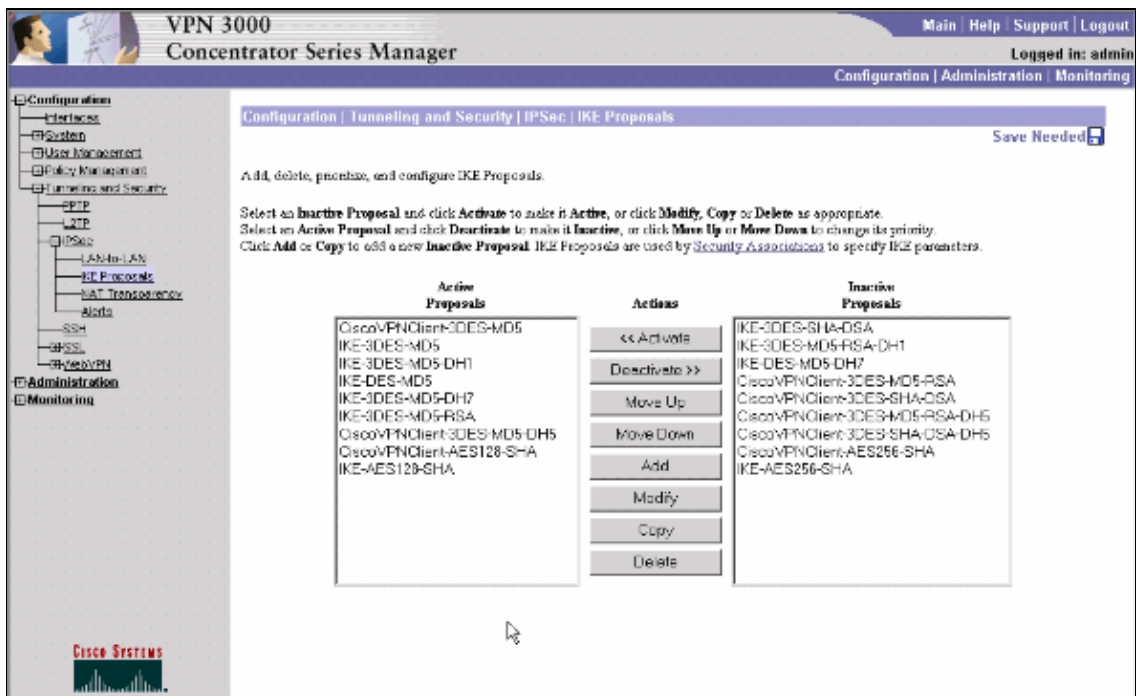
## VPN 3000 Concentrator Configuration

Complete these steps in order to configure the VPN 3000 Concentrator.

1. Enter the VPN 3000 Concentrator Series Manager administration web interface.
2. Login as Administrator.



3. On the left side of your screen select **Configuration > Tunneling and Security > IPSec > IKE Proposals**.
4. Click **Add** (in the middle of the screen) to add a new IKE proposal.



5. In the Add form, fill the required fields as this window shows.

Configuration | Tunneling and Security | IPsec | IKE Proposals | Add

Configure and add a new IKE Proposal.

Proposal Name  Specify the name of this IKE Proposal.

Authentication Mode  Select the authentication mode to use.

Authentication Algorithm  Select the packet authentication algorithm to use.

Encryption Algorithm  Select the encryption algorithm to use.

Diffie-Hellman Group  Select the Diffie Hellman Group to use.

Lifetime Measurement  Select the lifetime measurement of the IKE keys.

Data Lifetime  Specify the data lifetime in kilobytes (KB).

Time Lifetime  Specify the time lifetime in seconds.

- Click **Add** when you are done.
- Verify that the new IKE proposal is listed in the Active Proposals list, and click the **Save Needed** link on the upper right corner of the form.

Configuration | Tunneling and Security | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority. Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient	<< Activate	IKE-3DES-SHA-DSA
CiscoVPNClient3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5	Move Up	IKE-DES-MD5-DH7
IKE-3DES-MD5-DH1	Move Down	CiscoVPNClient-3DES-MD5-RSA
IKE-DES-MD5	Add	CiscoVPNClient-3DES-SHA-DSA
IKE-3DES-MD5-DH7	Modify	CiscoVPNClient-3DES-MD5-RSA-DH5
IKE-3DES-MD5-RSA	Copy	CiscoVPNClient-3DES-SHA-DSA-DH5
CiscoVPNClient-3DES-MD5-DH5	Delete	CiscoVPNClient-AES256-SHA
CiscoVPNClient-AES128-SHA		IKE-AES256-SHA
IKE-AES128-SHA		

- On the left side of your screen, select **Administration > Certificate Management > Installation**.
- Choose **Install CA certificate**.

Administration | Certificate Management | Install

Choose the type of certificate to install:

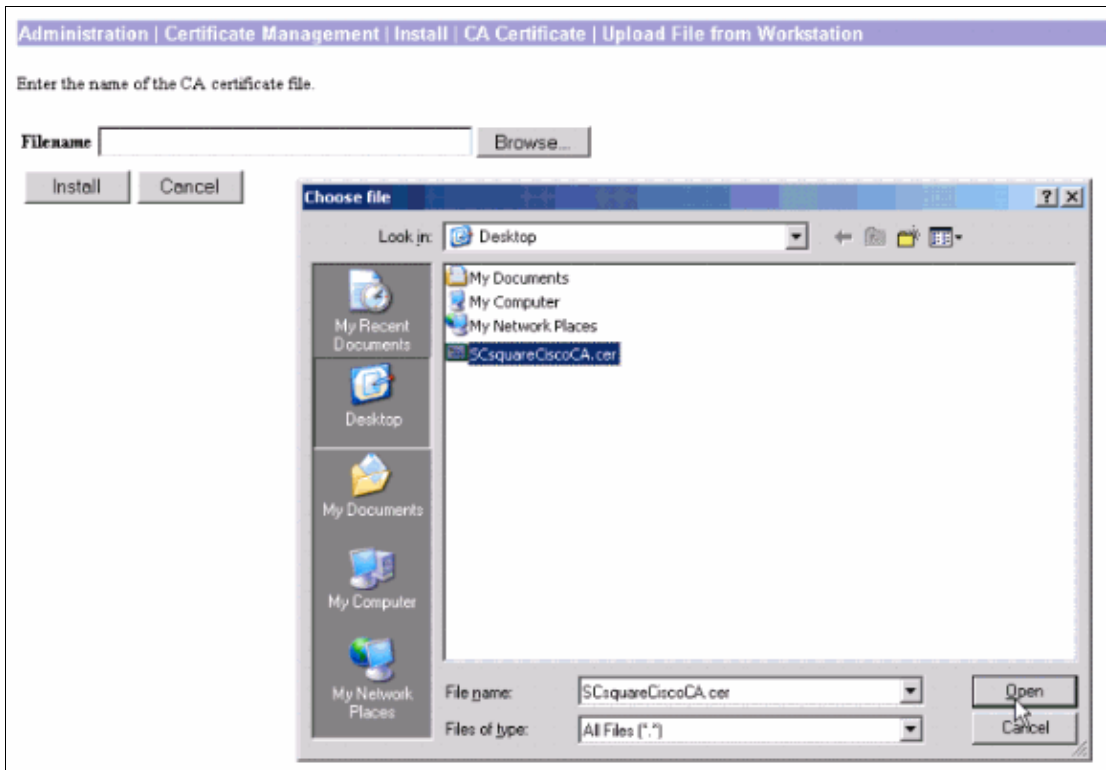
- Install CA certificate**
- Install SSL certificate with private key
- Install certificate obtained via enrollment

[<< Go back to Certificate Management](#)

- Choose **Upload File from Workstation**.



11. Click **Browse** and select your CA certificate file (the one you previously saved).



12. On the left side of your screen select **Administration > Certificate Management**.

13. Verify that the CA certificate is listed in the Certificate Authorities certificates table.

Administration | Certificate Management Monday, 26 April 2004 11:52:01  
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
SCsquareCiscoCA	SCsquareCiscoCA	04/25/2006	No	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>

**Identity Certificates** (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

**SSL Certificate** [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
192.168.10.195 at Cisco Systems, Inc.	192.168.10.195 at Cisco Systems, Inc.	04/26/2007	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>

**Enrollment Status** [[Remove All](#): [Enrolled](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

- On the left side of your screen select **Administration > Certificate Management > Enrollment > Identity Certificate > PKCS10**.
- Complete the form fields as this window shows and click **Enroll** when you are done.

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Common Name (CN)  Enter the common name for the VPN 3000 Concentrator to be used in this PKI.

Organizational Unit (OU)  Enter the department.

Organization (O)  Enter the Organization or company.

Locality (L)  Enter the city or town.

State/Province (SP)  Enter the State or Province.

Country (C)  Enter the two-letter country abbreviation (e.g. United States = US).

Subject AlternativeName (FQDN)  Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.

Subject AlternativeName (E-Mail Address)  Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.

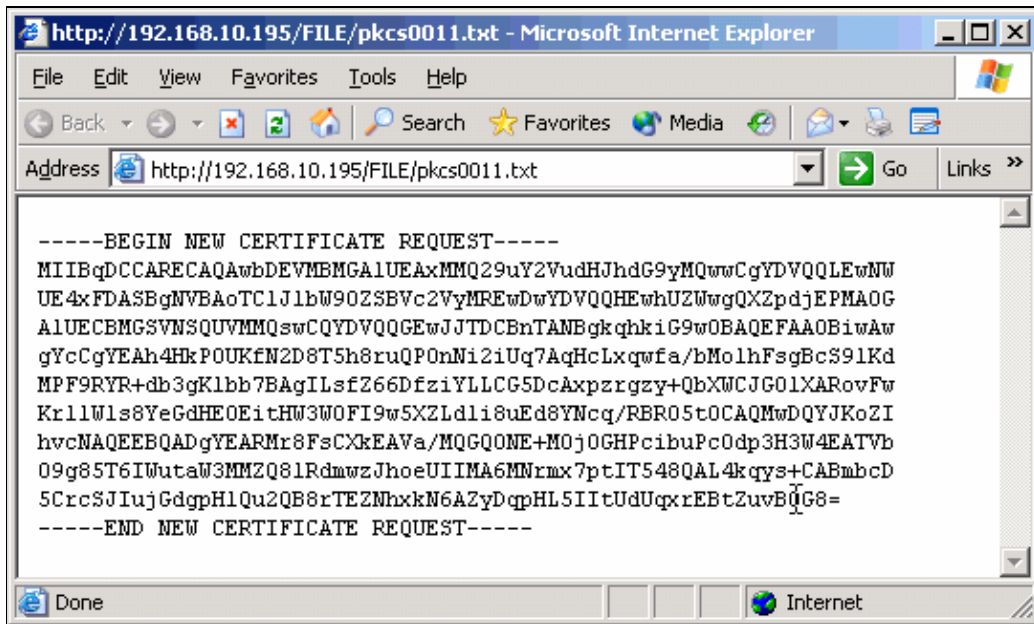
Key Size  Select the key size for the generated RSA/DSA key pair.

- A new window opens with the PKCS#10 certificate request in it.

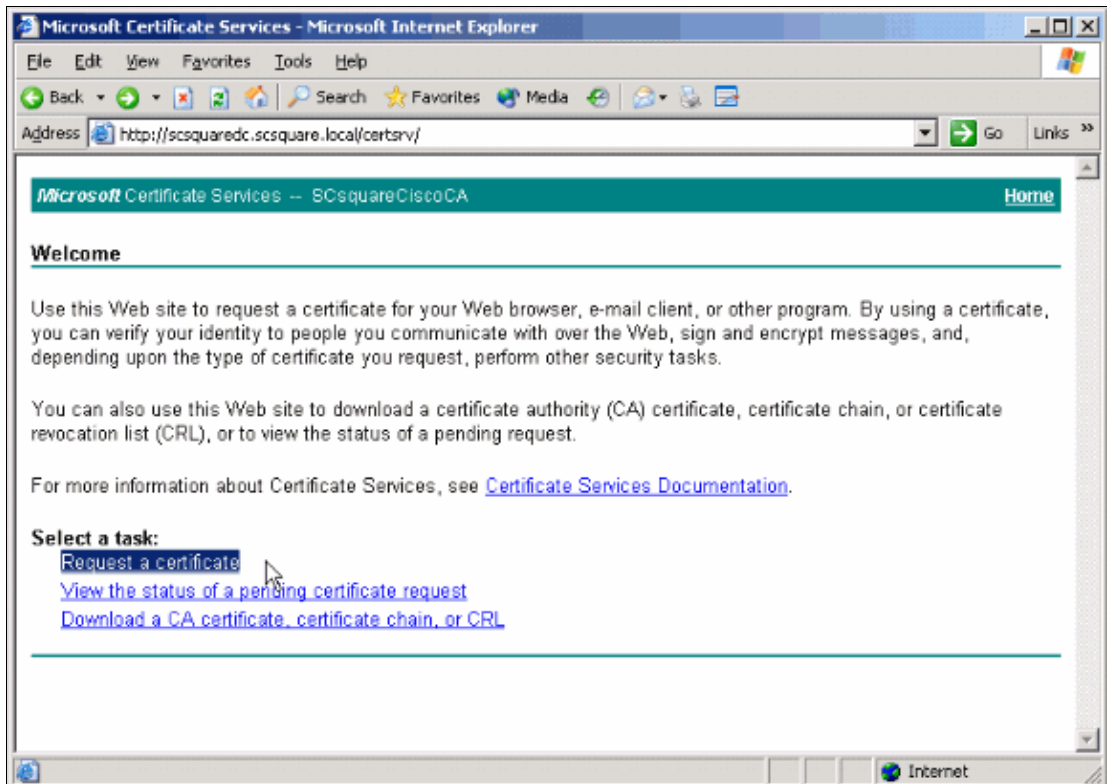
## VPN Concentrator Identity Certificate (VPN Certificate) Request

Complete these steps in order to request a VPN Concentrator identity certificate (VPN Certificate).

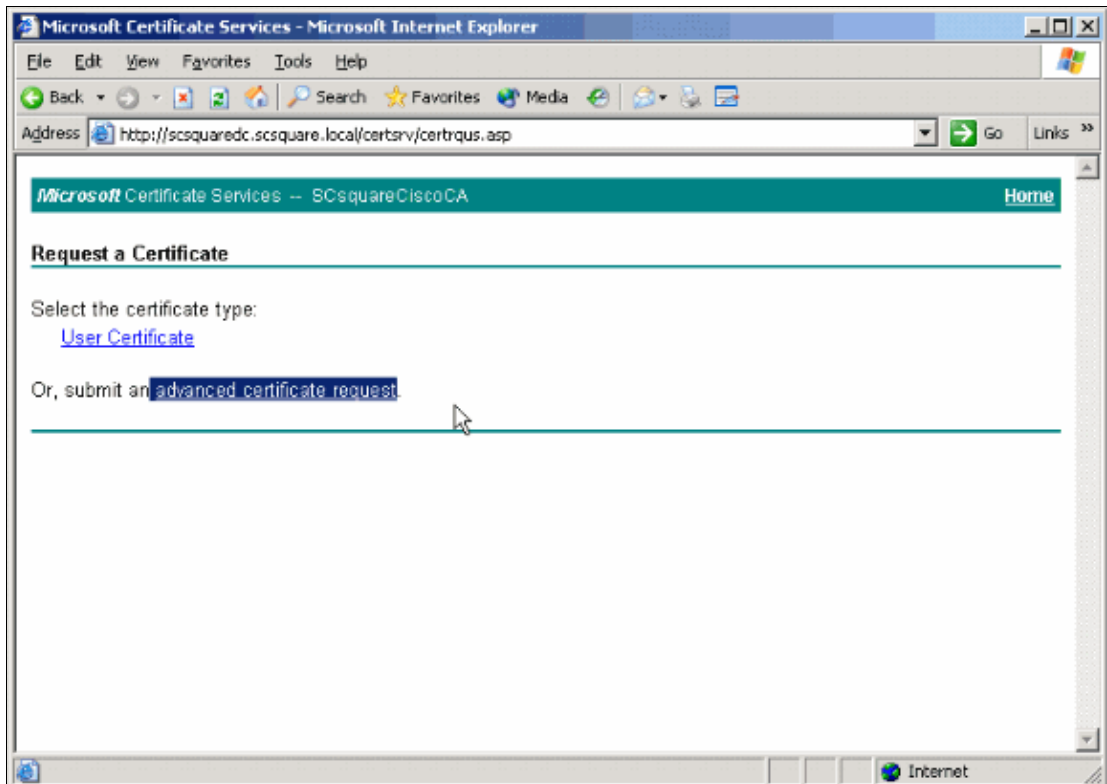
- Copy the entire contents of the certificate request to the clipboard.



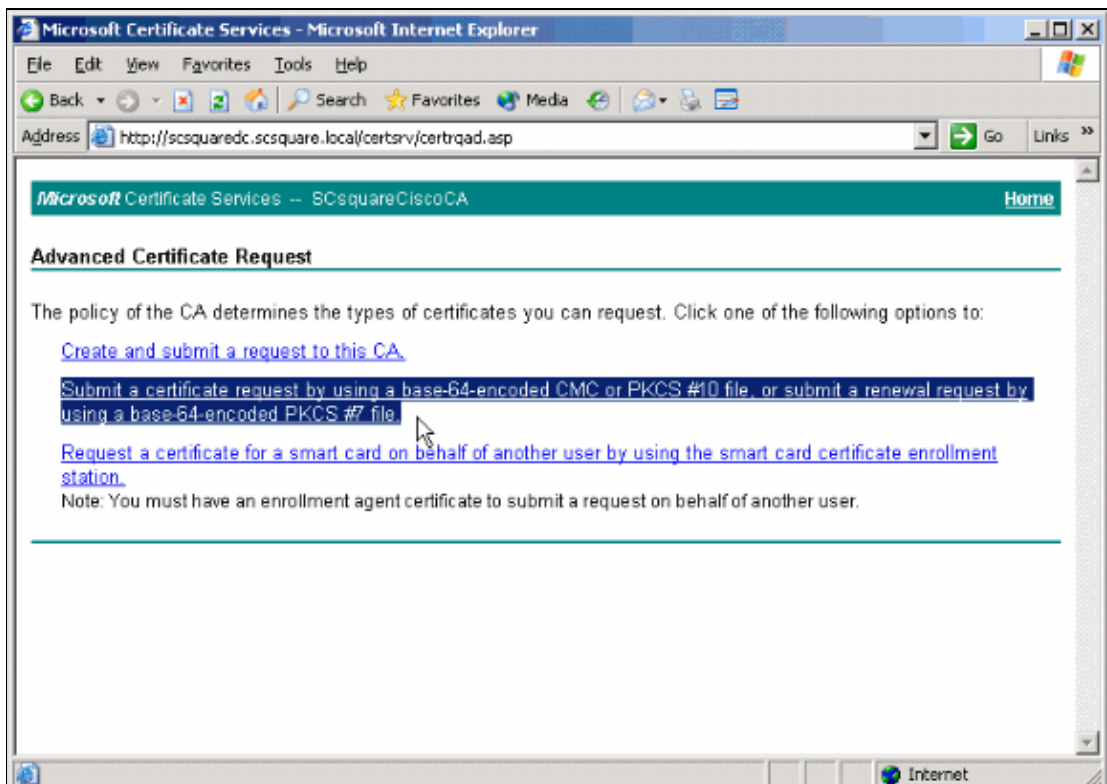
2. Go to the Certificate Authority web interface and select **Request a certificate**.



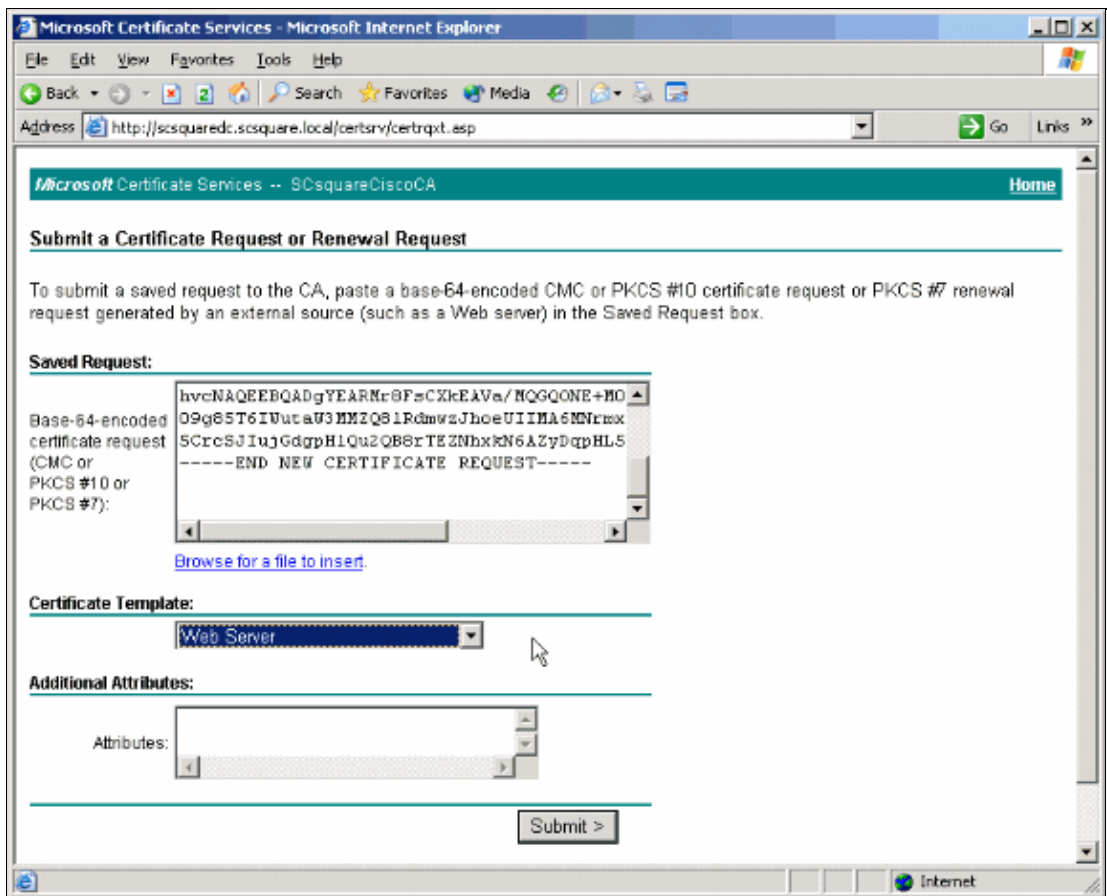
3. Choose **advanced certificate request**.



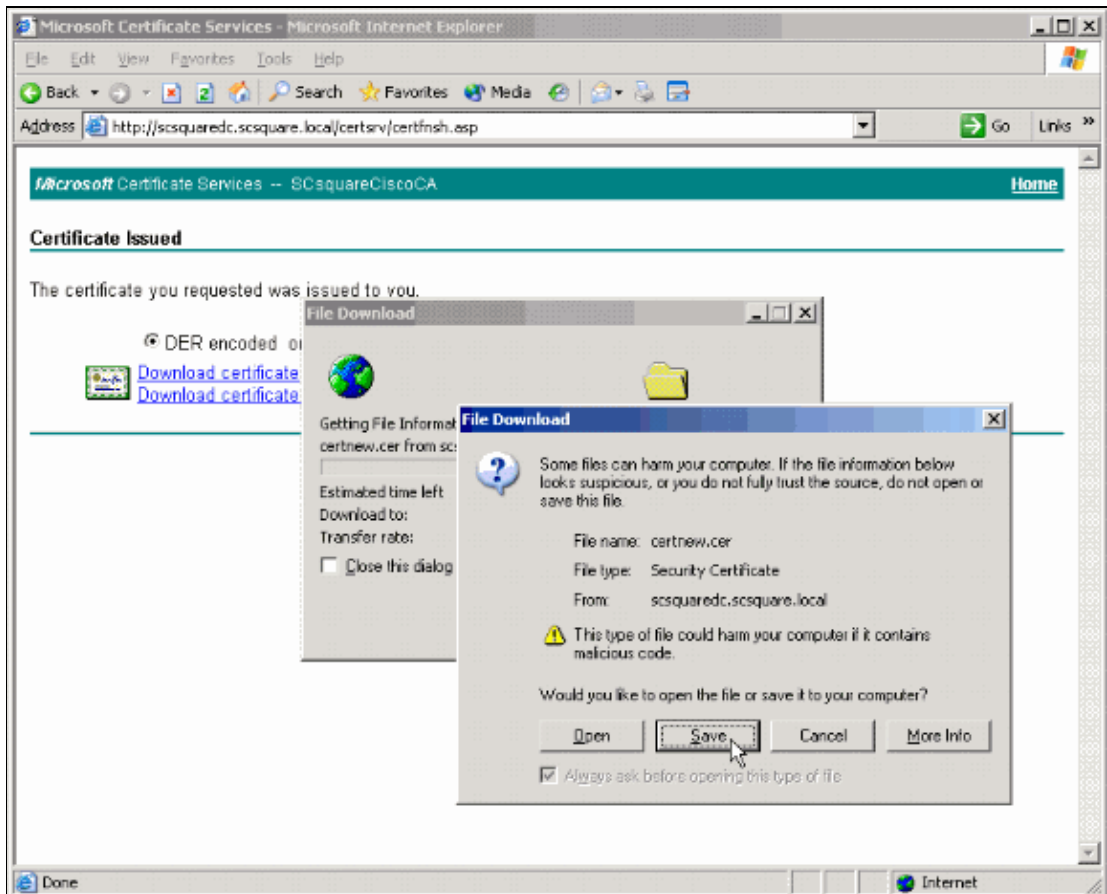
4. Choose **Submit a certificate request by using a base-64-encoded...**



5. Paste the request you previously copied to the clipboard into the Saved Request edit box.
6. In the Certificate Template, select **Web Server**.
7. Click **Submit**.



8. When you are done, click **Save** to save the issued certificate to your computer.



9. Return to the VPN 3000 Concentrator administration web interface.

10. Login as Administrator.
11. On the left side of your screen, select **Administration > Certificate Management > Installation.**
12. Choose **Installed certificate obtained via enrollment.**



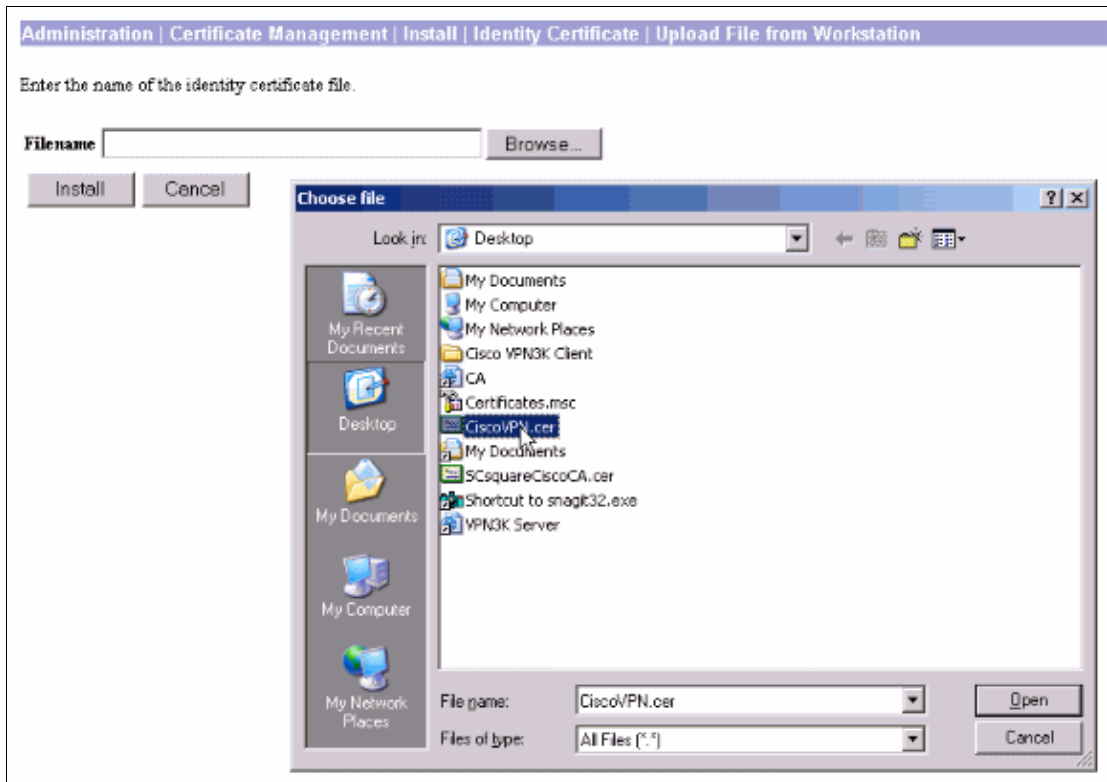
13. Click the **Install** link.



14. Choose **Upload File from Workstation.**



15. Click **Browse** and select the saved certificate.



16. Verify that the certificate is listed in the Identity Certificates table.

Administration | Certificate Management Monday, 26 April 2004 12:06:52  
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [ [View All CRL Caches](#) | [Clear All CRL Caches](#) ] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
SCsquareCiscoCA	SCsquareCiscoCA	04/25/2006	No	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>

**Identity Certificates** (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Concentrator at Remote User	SCsquareCiscoCA	04/25/2006	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>

**SSL Certificate** [ [Generate](#) ] *Note: The public key in the SSL certificate is also used for the SSH host key.*

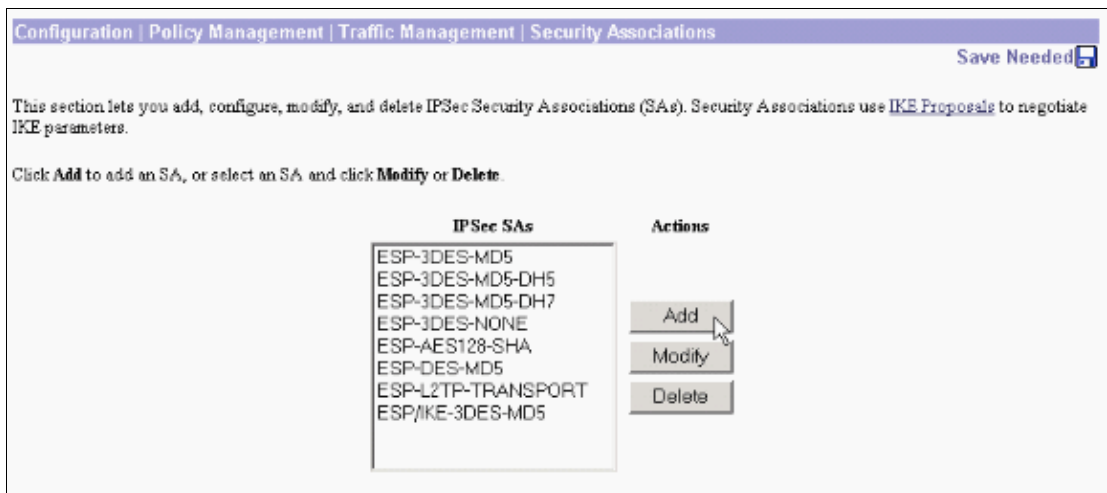
Subject	Issuer	Expiration	Actions
192.168.10.195 at Cisco Systems, Inc.	192.168.10.195 at Cisco Systems, Inc.	04/26/2007	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>

**Enrollment Status** [ [Remove All: Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#) ] (current: 0 available: 19)

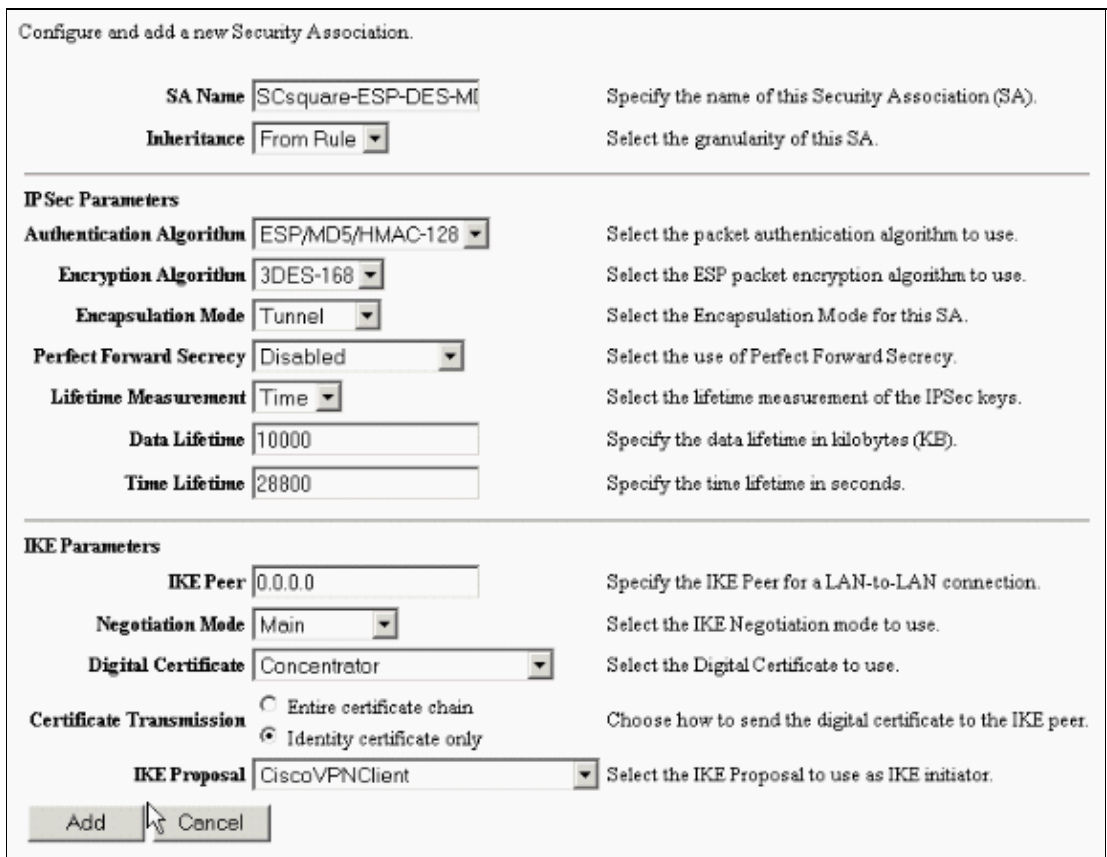
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
<b>No Enrollment Requests</b>							

17. On the left side of your screen, select **Configuration > Policy Management > Traffic Management > SAs**.

18. Click **Add** to add a new SA.

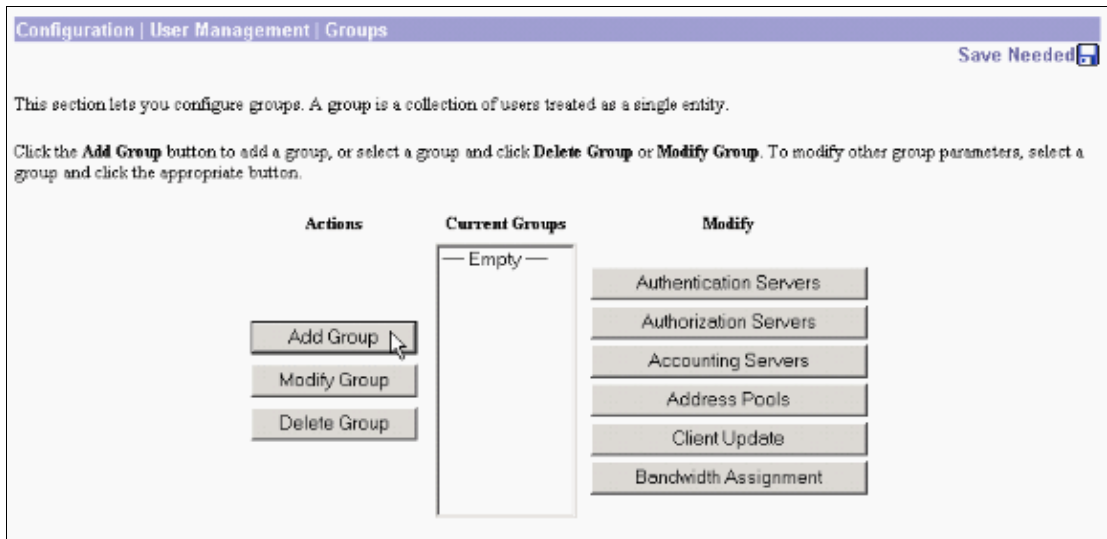


19. In the Add page, complete the form fields as this window shows and click **Add**.

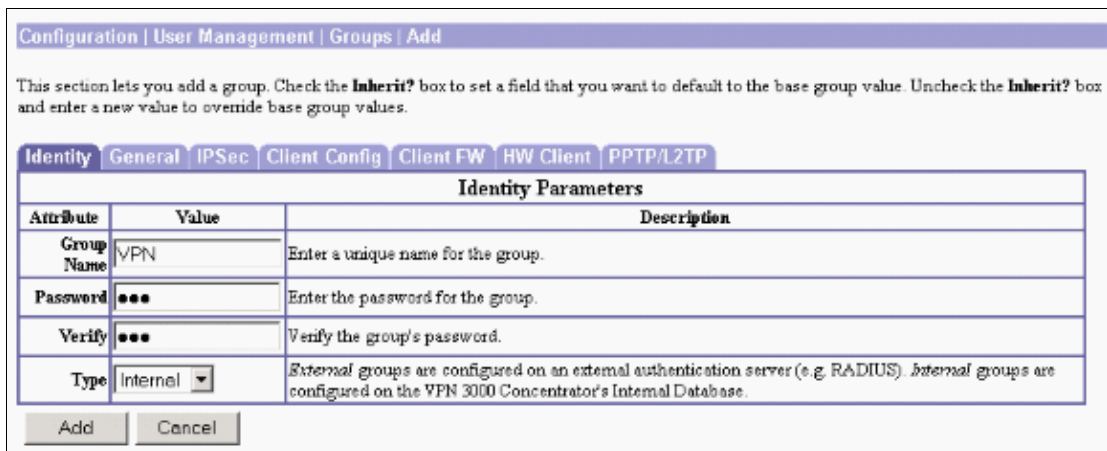


20. On the left side of your screen, select **Configuration > User Management > Groups**.

21. Click **Add Group** to add a new group.



22. In the Identity tab of the group add page, fill the form fields as this window shows and go to the General tab when you are done.



23. In the General tab, complete the form fields as this window shows and go to the IPSec tab when you are done.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP

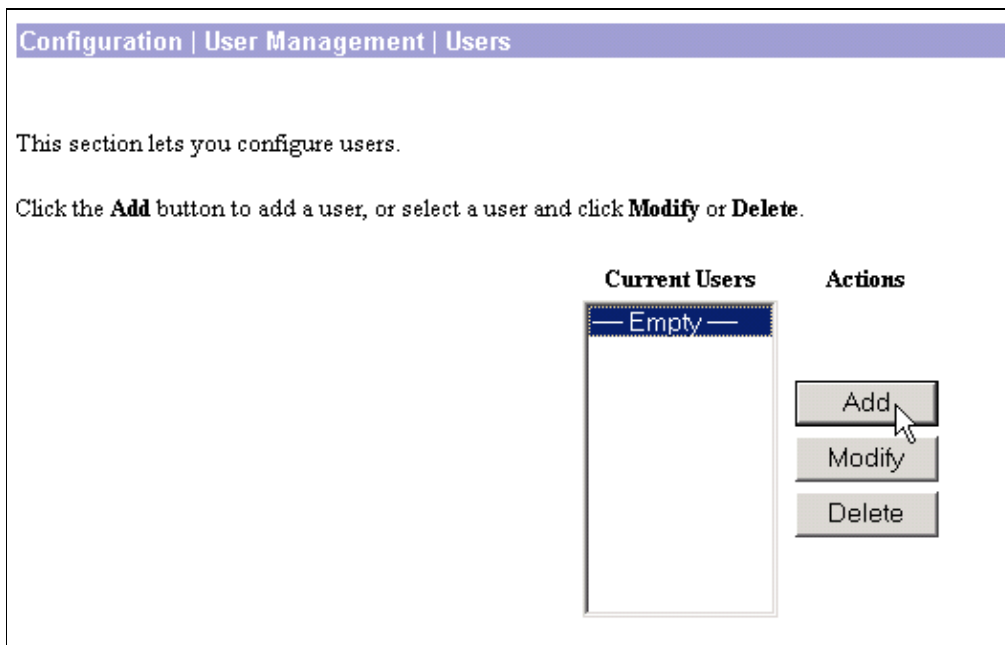
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		<input checked="" type="checkbox"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

24. In the IPsec tab, complete the form fields as this window shows and click **Add**.

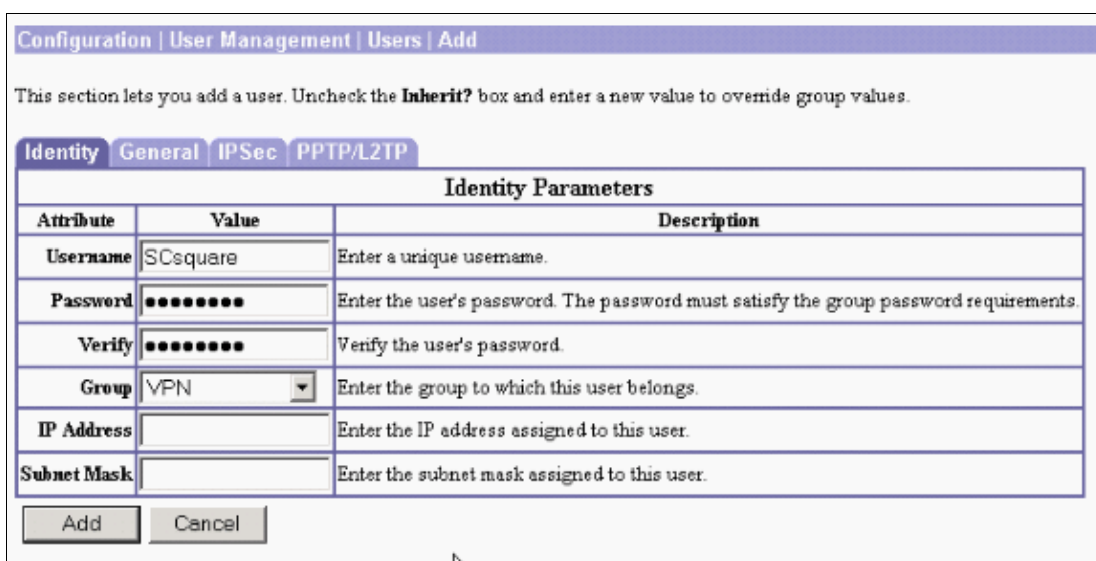
Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN

IPsec Parameters			
Attribute	Value	Inherit?	Description
IPsec SA	SCsquare-ESP-DES-MD5	<input type="checkbox"/>	Select the group's IPsec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User Authentication</b> .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IP Comp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Permit or deny VPN Clients according to their type and			

25. On the left side of your screen, select **Configuration > User Management > Users** and click **Add** to add a new user.



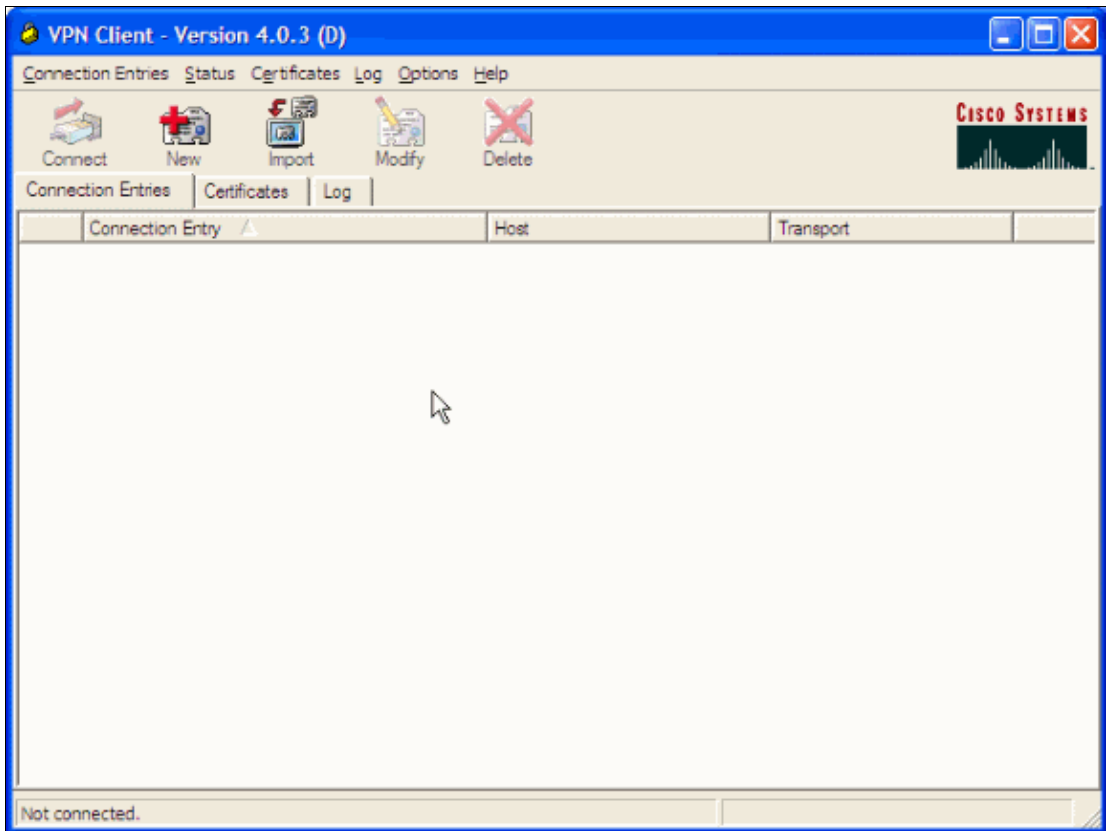
26. In the Identity tab of the add user page, complete the form fields as this window shows and click **Add**.



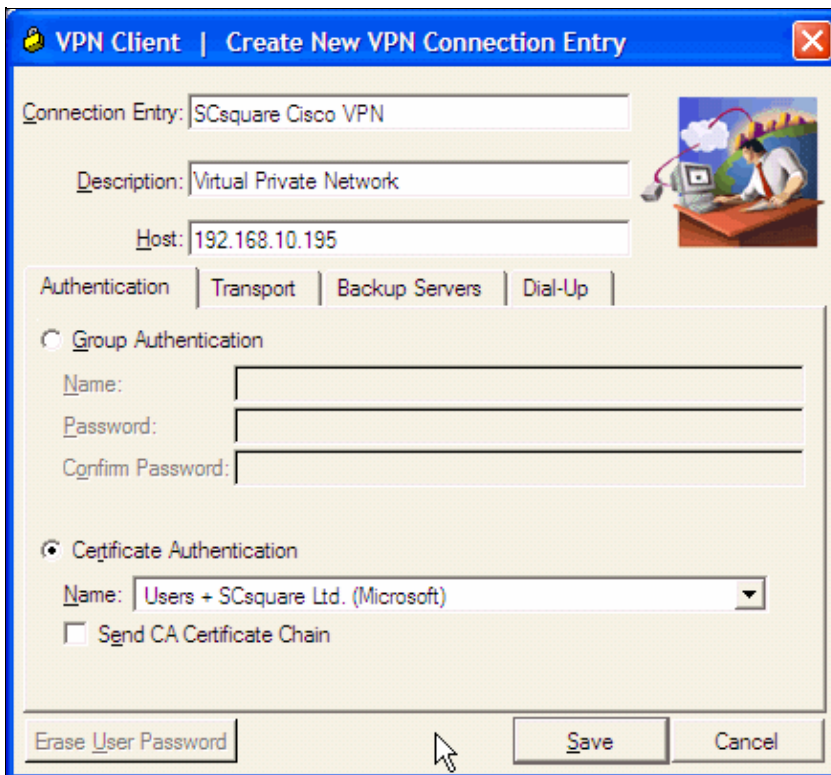
## VPN Client Configuration

Complete these steps in order to configure the VPN Client.

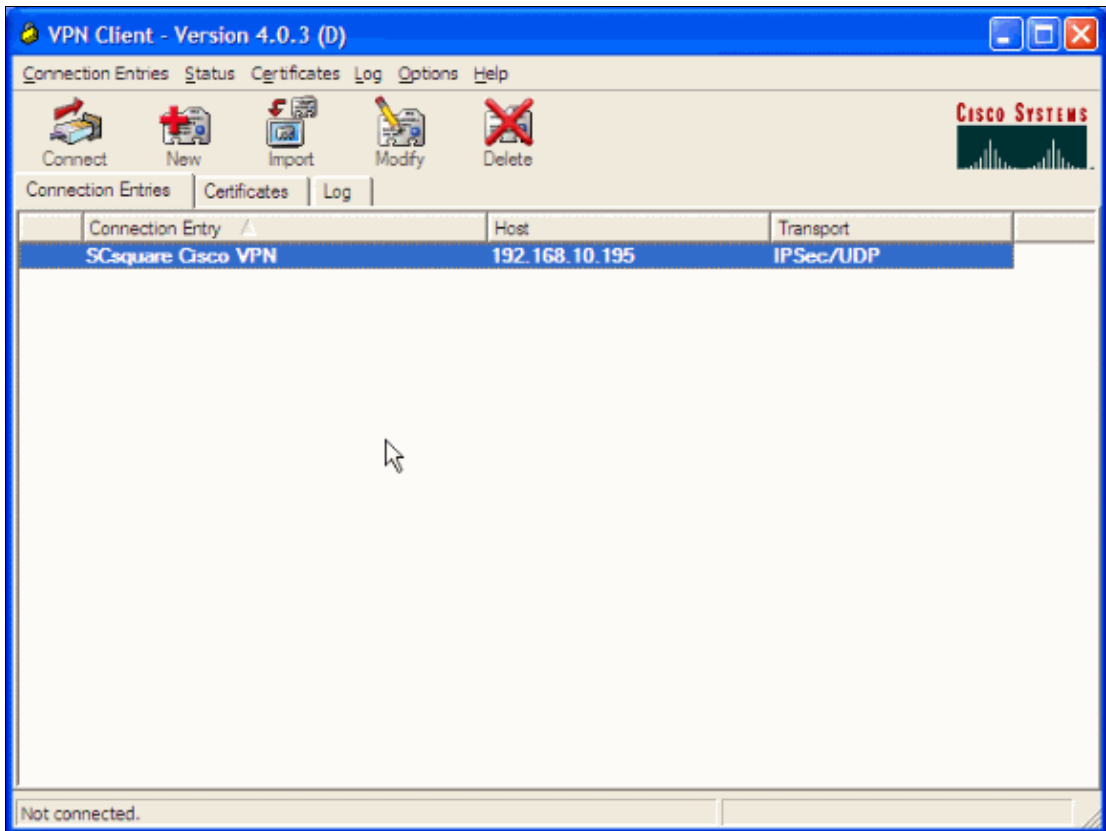
1. Start the VPN Client application.



2. Go to the Connection Entries tab and click **New** to add a new connection entry.
3. In the Create New VPN Connection Entry dialog, complete the form fields as this window shows and click **Save**.



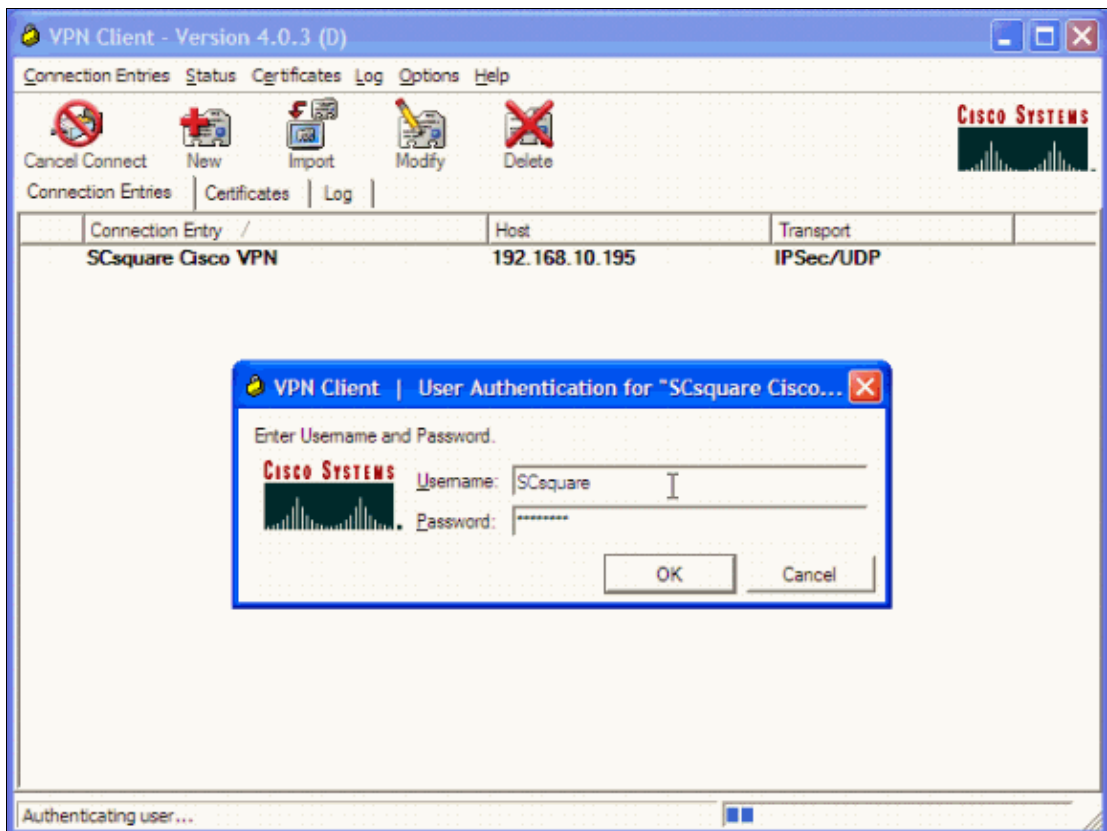
4. Choose the new connection you have just created and click **Connect**.



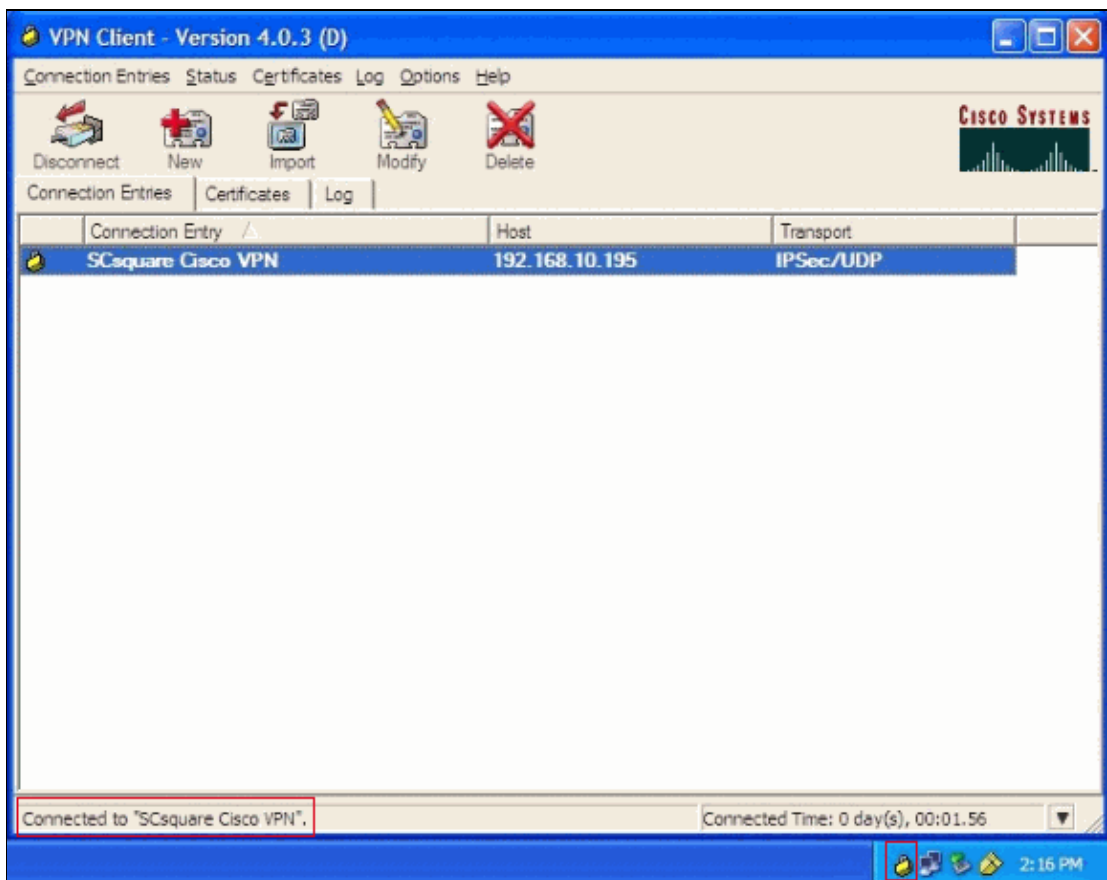
5. When the SC<sup>2</sup>™ CSP popup dialog appears, enter the PIN code to your smart card.



6. When the VPN Client application popup dialog appears, enter the Username and Password to your VPN account.



7. You are now connected to the VPN. The active connection is indicated in the VPN Client application status bar as well as in the system tray as a closed lock.



# Verify

There is currently no verification procedure available for this configuration.

# Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- [VPN Client Troubleshooting and Programmer Notes Version 4.6](#)
- [Troubleshooting Connection Problems on the VPN 3000 Concentrator](#)
- [VPN Client GUI Error Lookup Tool](#)

# Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 23, 2006

Document ID: 62992

---