ASA/PIX 7.x and VPN Client IPSec Authentication Using Digital Certificates with Microsoft CA Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Related Products
Conventions
Configure
Network Diagram
Configurations
ASA Configuration
ASA Configuration Summary
VPN Client Configuration
Verify
Troubleshoot
Related Information

Introduction

This document describes how to manually install a 3rd party vendor digital certificate on the Cisco Security Appliance (ASA/PIX) 7.x, as well as VPN clients, in order to authenticate the IPSec peers with Microsoft Certificate Authority (CA) server.

Prerequisites

Requirements

This document requires that you have access to a certificate authority (CA) for certificate enrollment. Supported 3rd party CA vendors include Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign.

Note: This document uses Windows 2003 Server as a CA server for the scenario.

Note: This document assumes that there is no pre-existing VPN configuration in the ASA/PIX.

Components Used

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

- ASA 5510 that runs software version 7.2(2) and ASDM version 5.2(2).
- VPN Client that runs software version 4.x and later.

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.

Related Products

The ASA configuration can also be used with the Cisco 500 Series PIX that runs software version 7.x.

Conventions

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

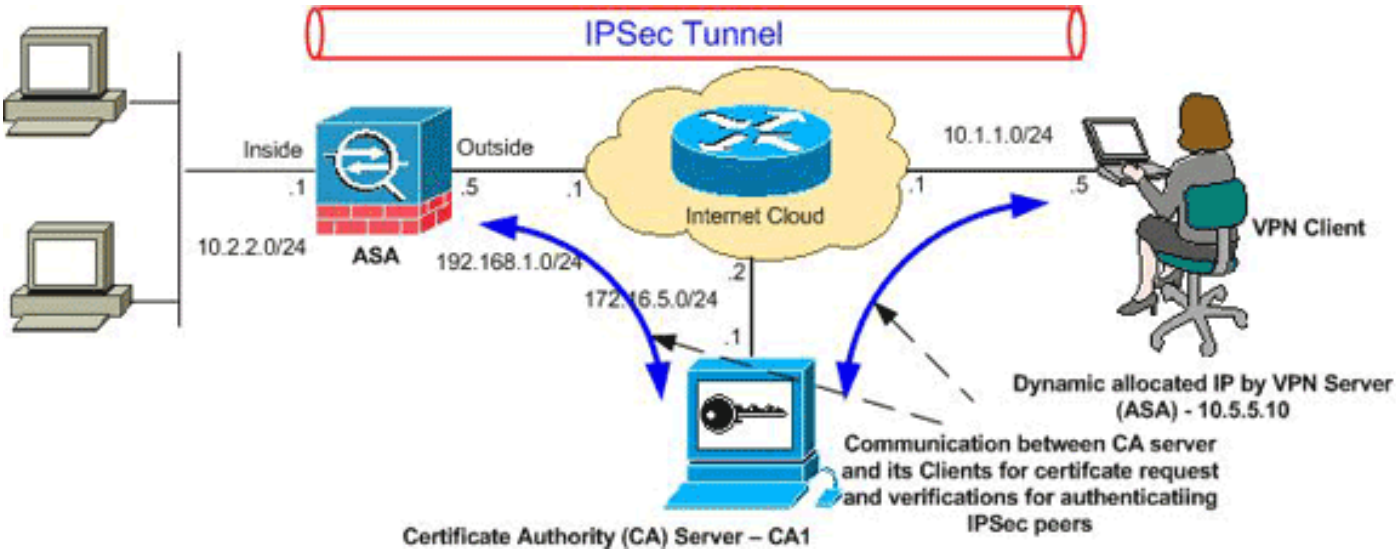
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Configurations

This document uses these configurations:

- ASA Configuration
- ASA Configuration Summary
- VPN Client Configuration

ASA Configuration

Complete these steps in order to install a 3rd party vendor digital certificate on the ASA:

Step 1. Verify that the Date, Time, and Time Zone Values are Accurate

Step 2. Generate the RSA Key Pair

Step 3. Create the Trustpoint.

Step 4. Generate the Certificate Enrollment.

Step 5. Authenticate the Trustpoint

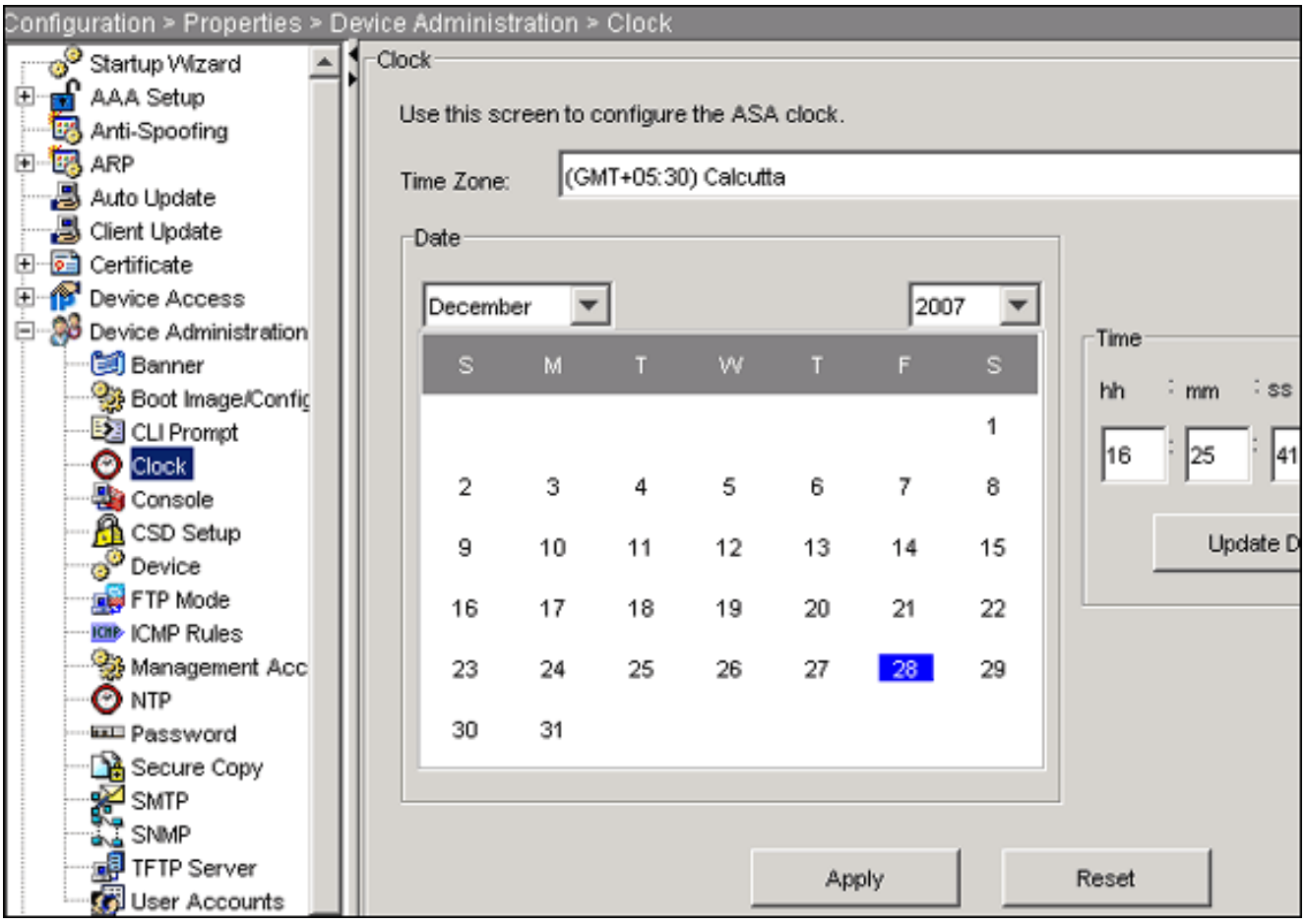
Step 6. Install the Certificate

Step 7. Configure Remote Access VPN (IPSec) to Use the Newly Installed Certificate

Step 1. Verify that the Date, Time, and Time Zone Values are Accurate

ASDM Procedure

1. Click **Configuration**, and then click **Properties**.
2. Expand **Device Administration**, and choose **Clock**.
3. Verify that the information listed is accurate.The values for Date, Time, and Time Zone must be accurate in order for proper certificate validation to occur.



Command Line Example

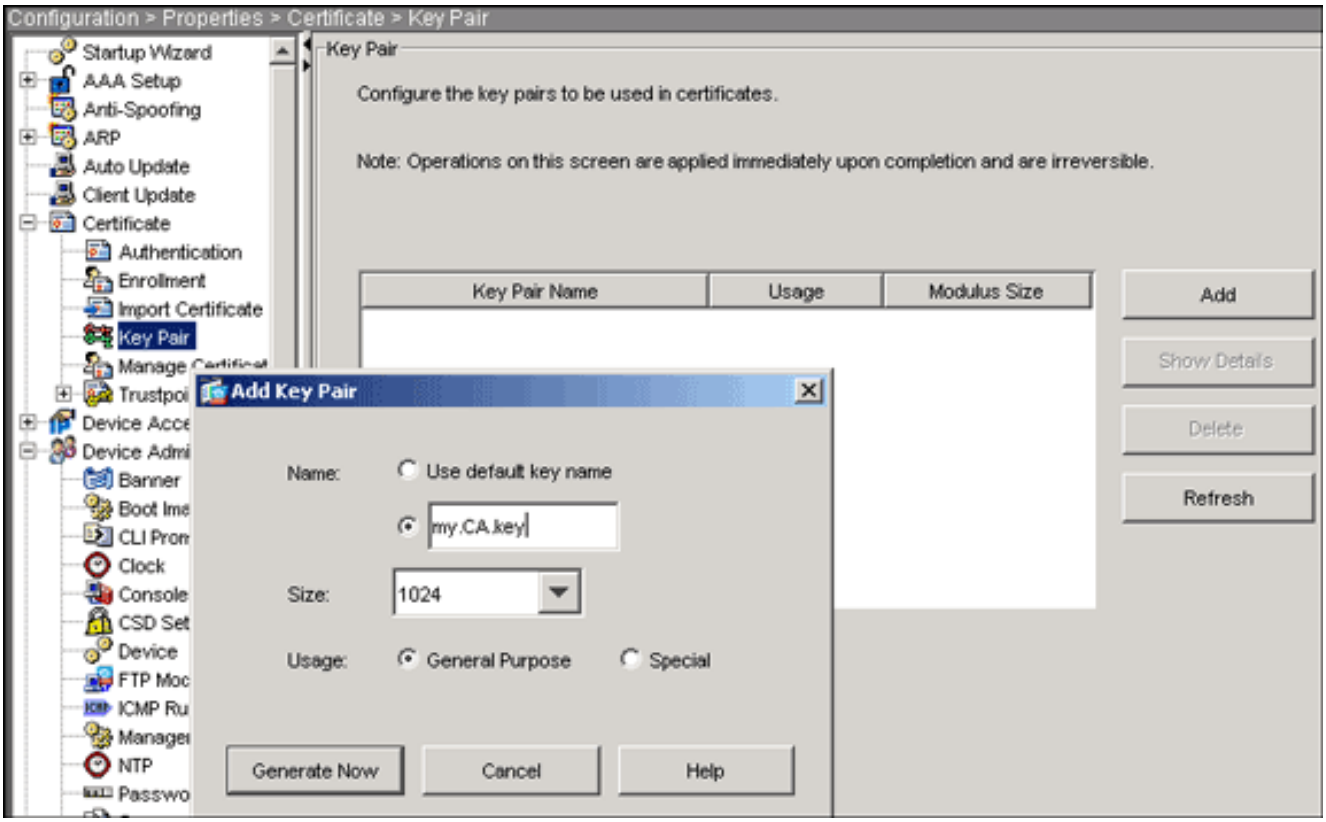
CiscoASA
CiscoASA#**show clock** 16:25:49.580 IST Fri Dec 28 2007

Step 2. Generate the RSA Key Pair

The generated RSA public key is combined with the identity information from the ASA to form a PKCS#10 certificate request. You should distinctly identify the key name with the Trustpoint for which you create the key pair.

ASDM Procedure

1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and choose **Key Pair**.
3. Click
   Add.



4. Enter the key name, choose the modulus size, and select the usage type.**Note:** The recommended key pair size is 1024.
5. Click **Generate Now**.The key pair you created should be listed in the Key Pair Name column.

Command Line Example

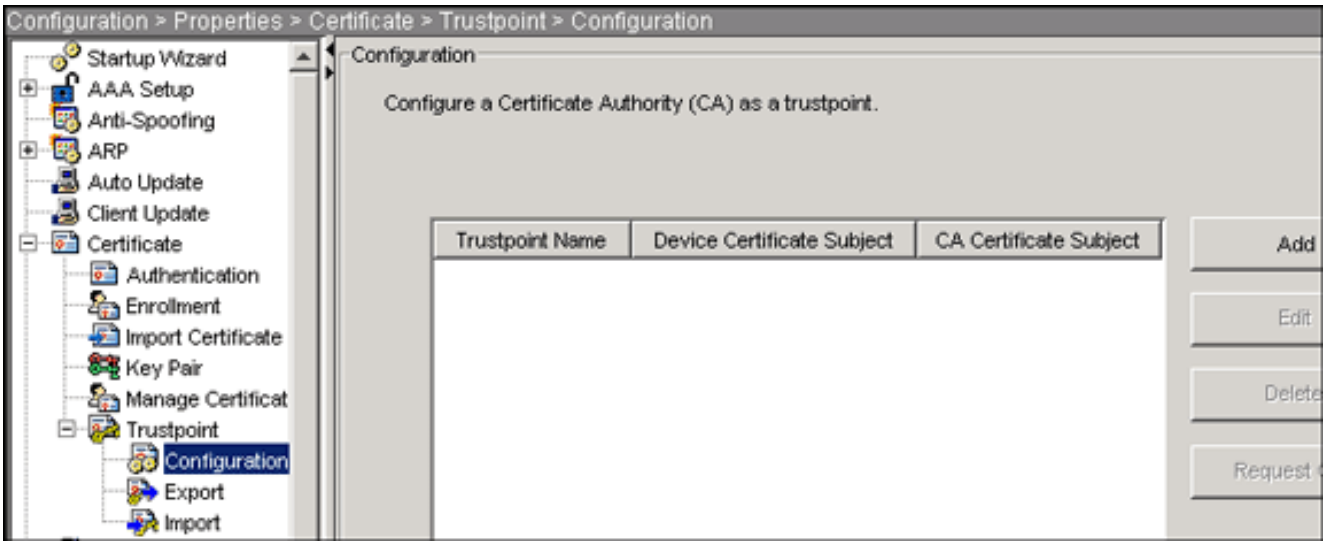
CiscoASA
CiscoASA#**configure terminal** CiscoASA(config)#**crypto key generate rsa label my.CA.key modulus 1024** *!--- Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.CA.key Keypair generation process begin. Please wait... ciscoasa(config)#

Step 3. Create the Trustpoint

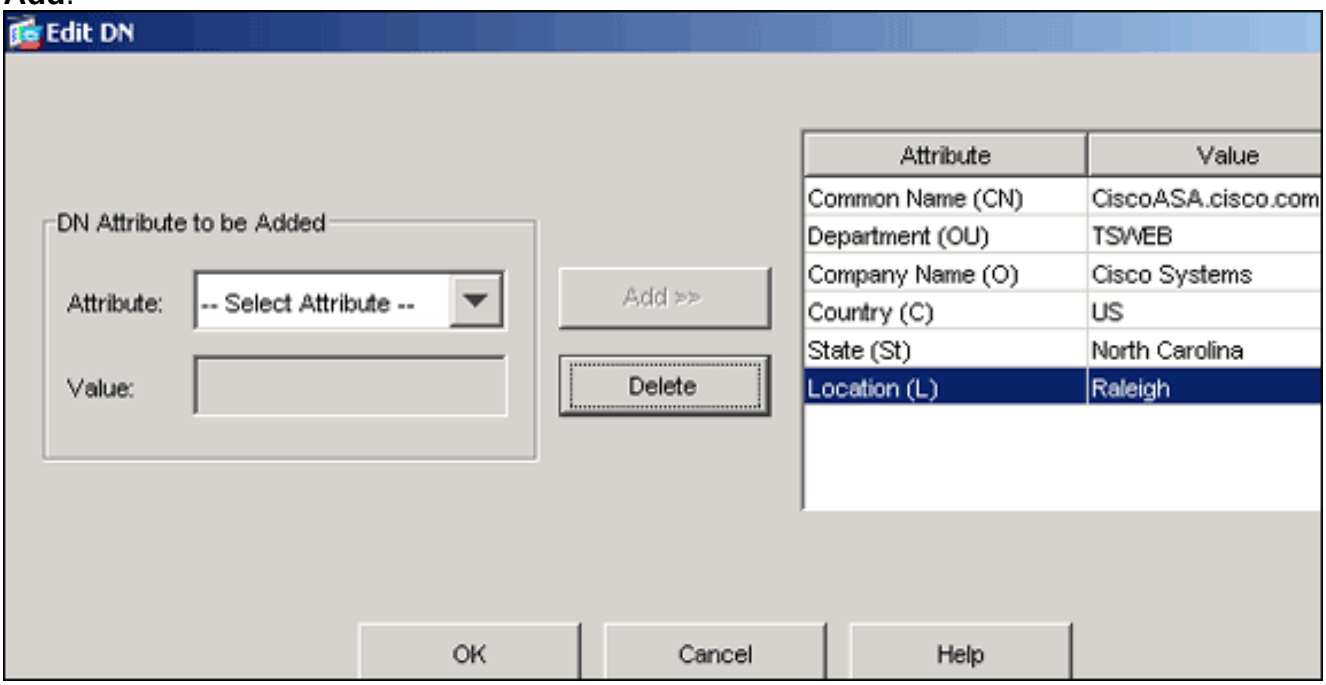
Trustpoints are required to declare the Certificate Authority (CA) that your ASA will use.

ASDM Procedure

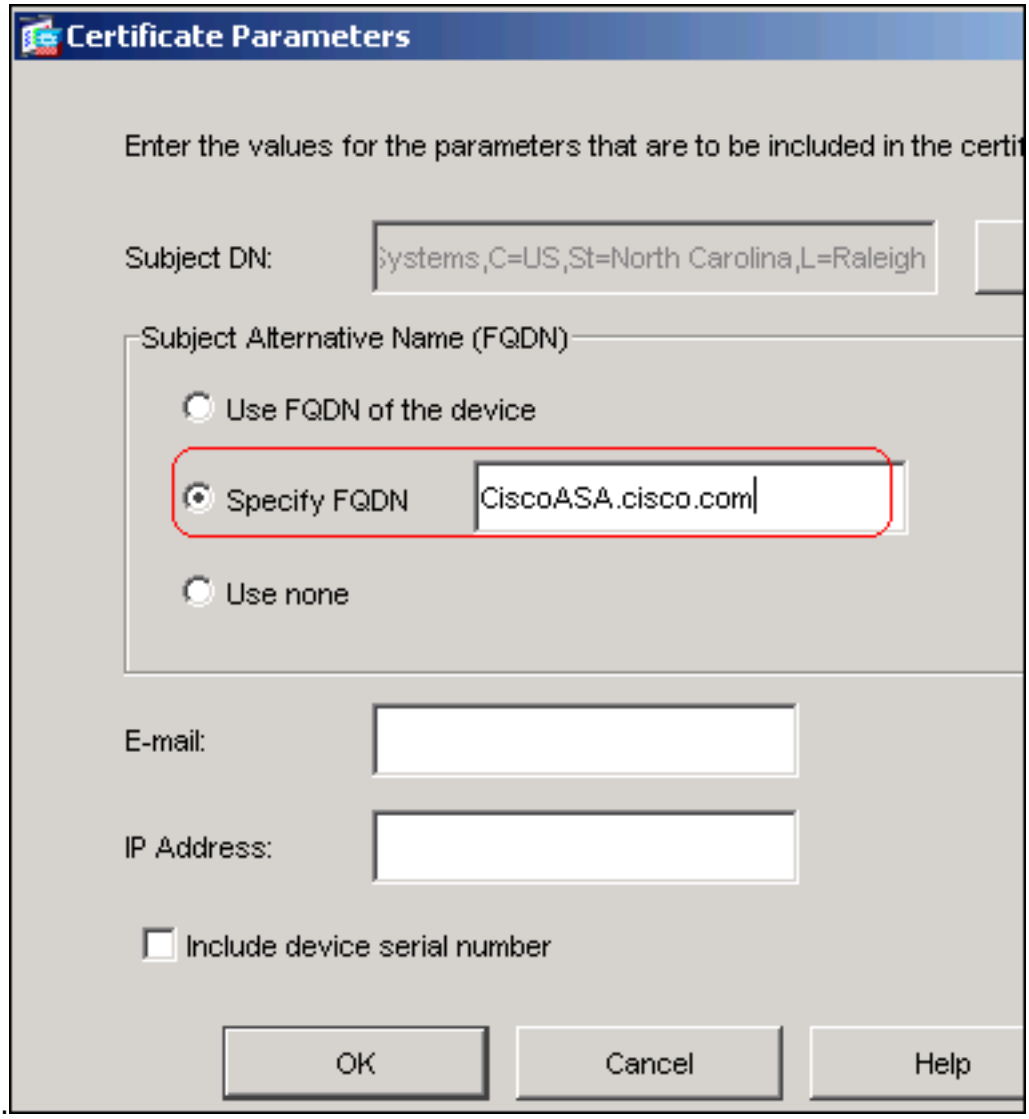
1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and then expand **Trustpoint**.
3. Choose **Configuration**, and then click **Add**.



4. Configure these values:**Trustpoint Name**: The trustpoint name should be relevant to the intended usage. (This example uses *CA1*.)**Key pair**: Select the key pair generated in Step 2 . (my.CA.key)
5. Ensure Manual Enrollment is selected.
6. Click **Certificate Parameters**.The Certificate Parameters dialog box appears.
7. Click **Edit**, and configure the attributes listed in this table:In order to configure these values, choose a value from the Attribute drop-down list, enter the value, and click **Add**.

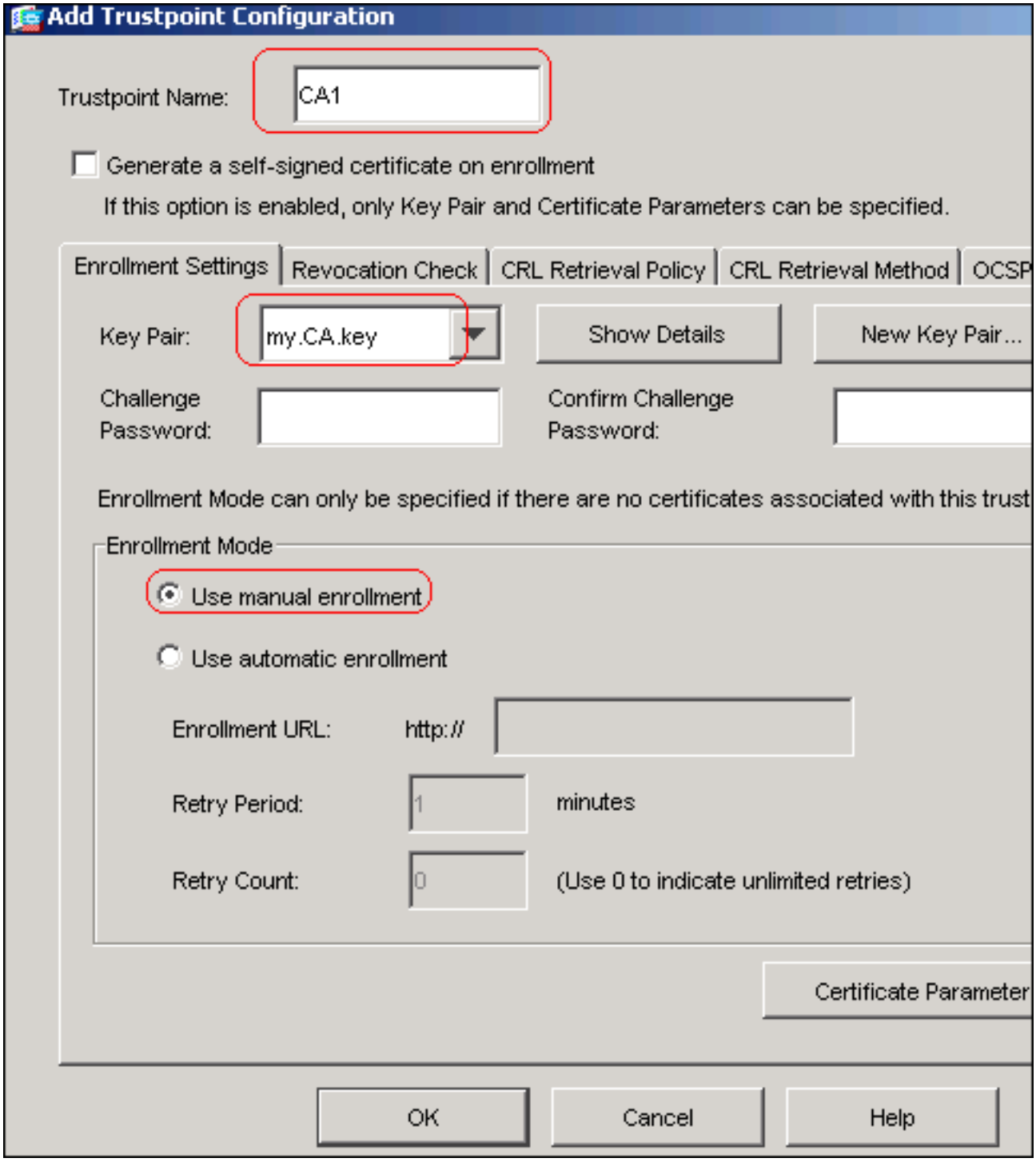


8. Once the appropriate values are added, click **OK**.
9. In the Certificate Parameters dialog box, enter the FQDN in the Specify FQDN field.This value should be same FQDN you used for the Common Name



(CN).

10. Click **OK**.
11. Verify the correct key pair is selected, and click the **Use manual enrollment** radio button.
12. Click **OK**, and then click **Apply**.



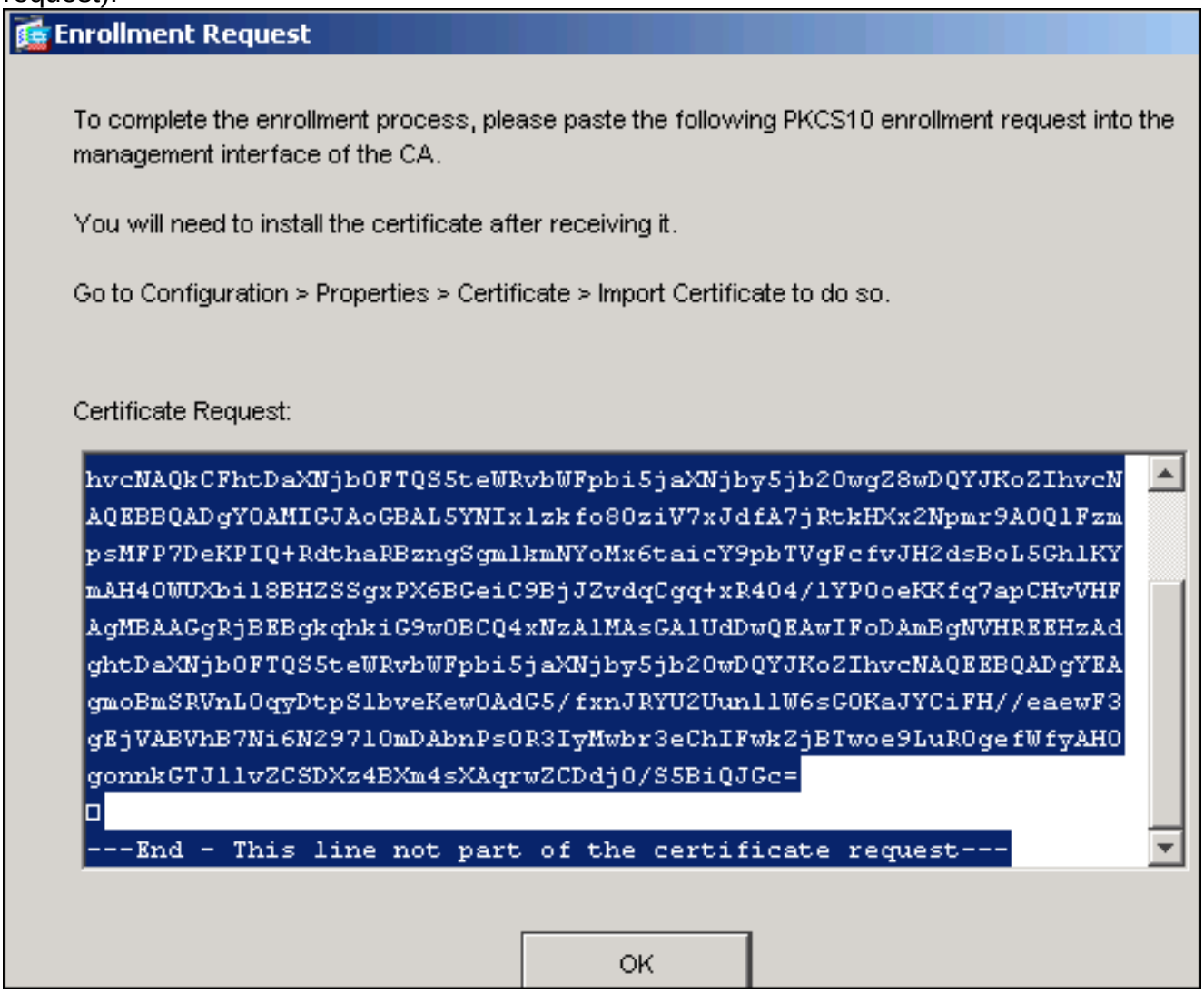
Command Line Example

CiscoASA
CiscoASA(config)#**crypto ca trustpoint CA1** *!--- Creates the trustpoint.* CiscoASA(config-ca-trustpoint)#**enrollment terminal** *!--- Specifies cut and paste enrollment with this trustpoint.* CiscoASA(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh** *!--- Defines x.500 distinguished name.* CiscoASA(config-ca-trustpoint)#**keypair my.CA.key** *!--- Specifies key pair generated in Step 2.* CiscoASA(config-ca-trustpoint)#**fqdn CiscoASA.cisco.com** *!--- Specifies subject alternative name (DNS:).* CiscoASA(config-ca-trustpoint)#**exit**

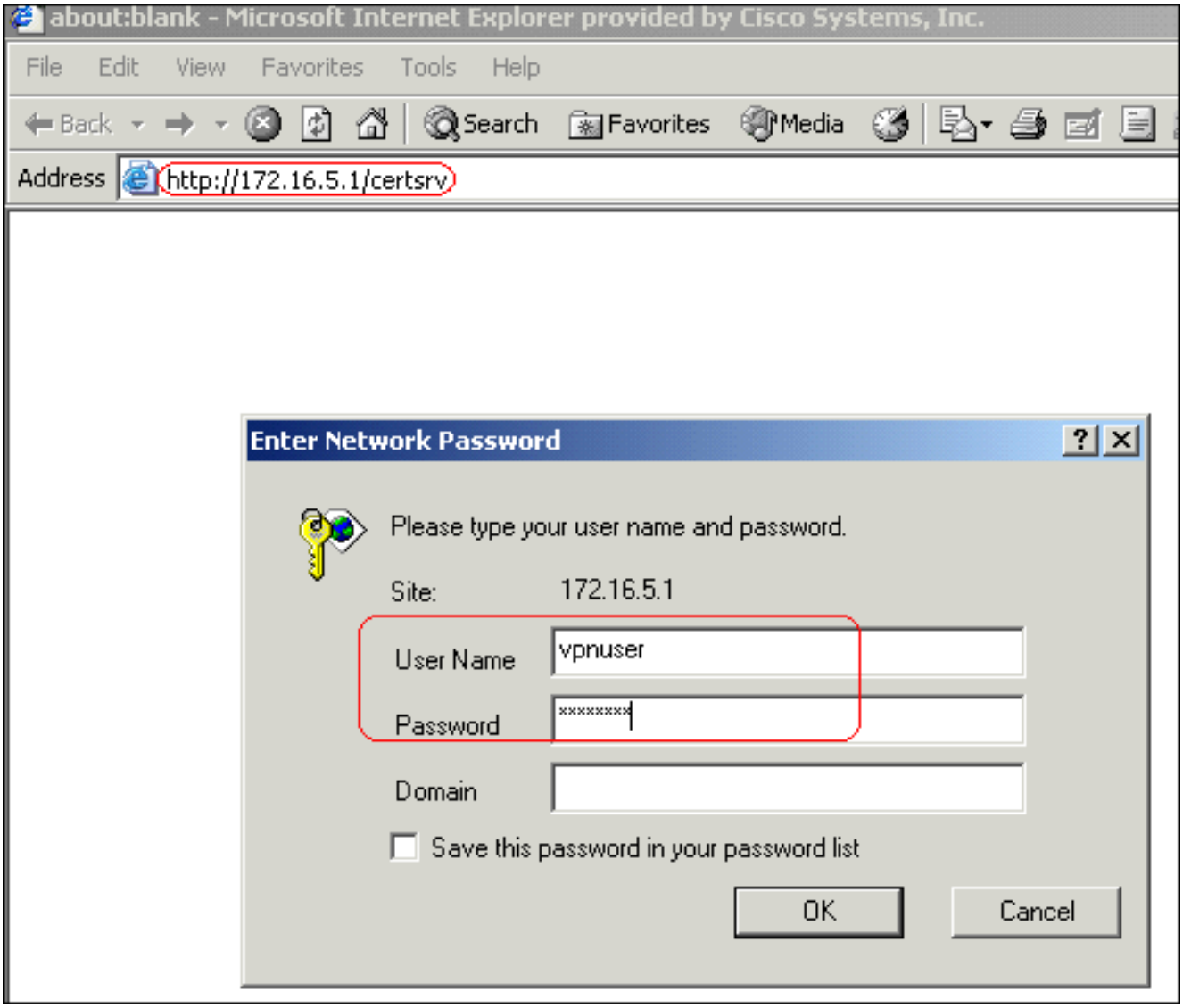
Step 4. Generate the Certificate Enrollment

ASDM Procedure

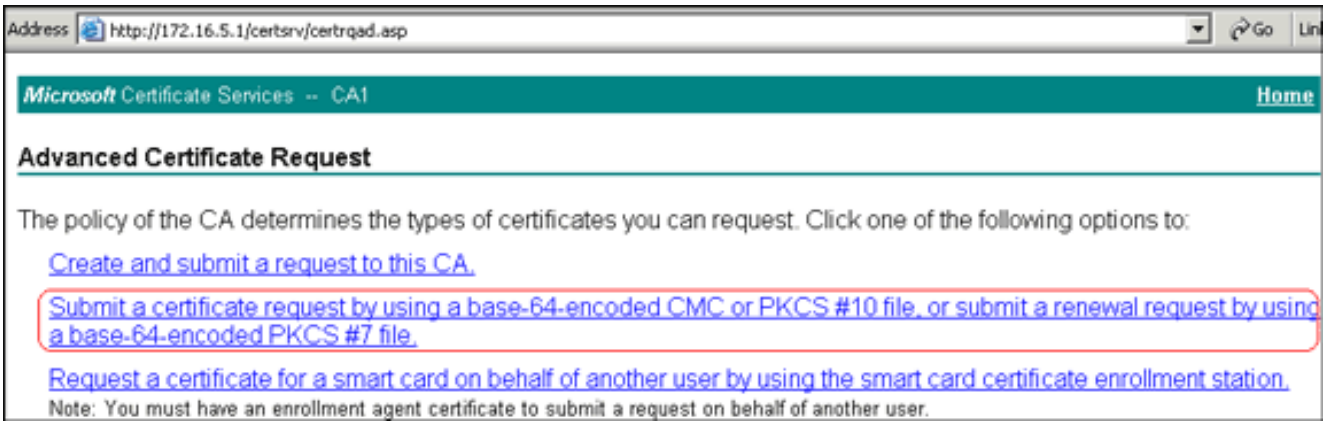
1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and choose **Enrollment**.
3. Verify the Trustpoint created in Step 3 is selected, and click **Enroll**.A dialog box appears that lists the certificate enrollment request (also referred to as a certificate signing request).



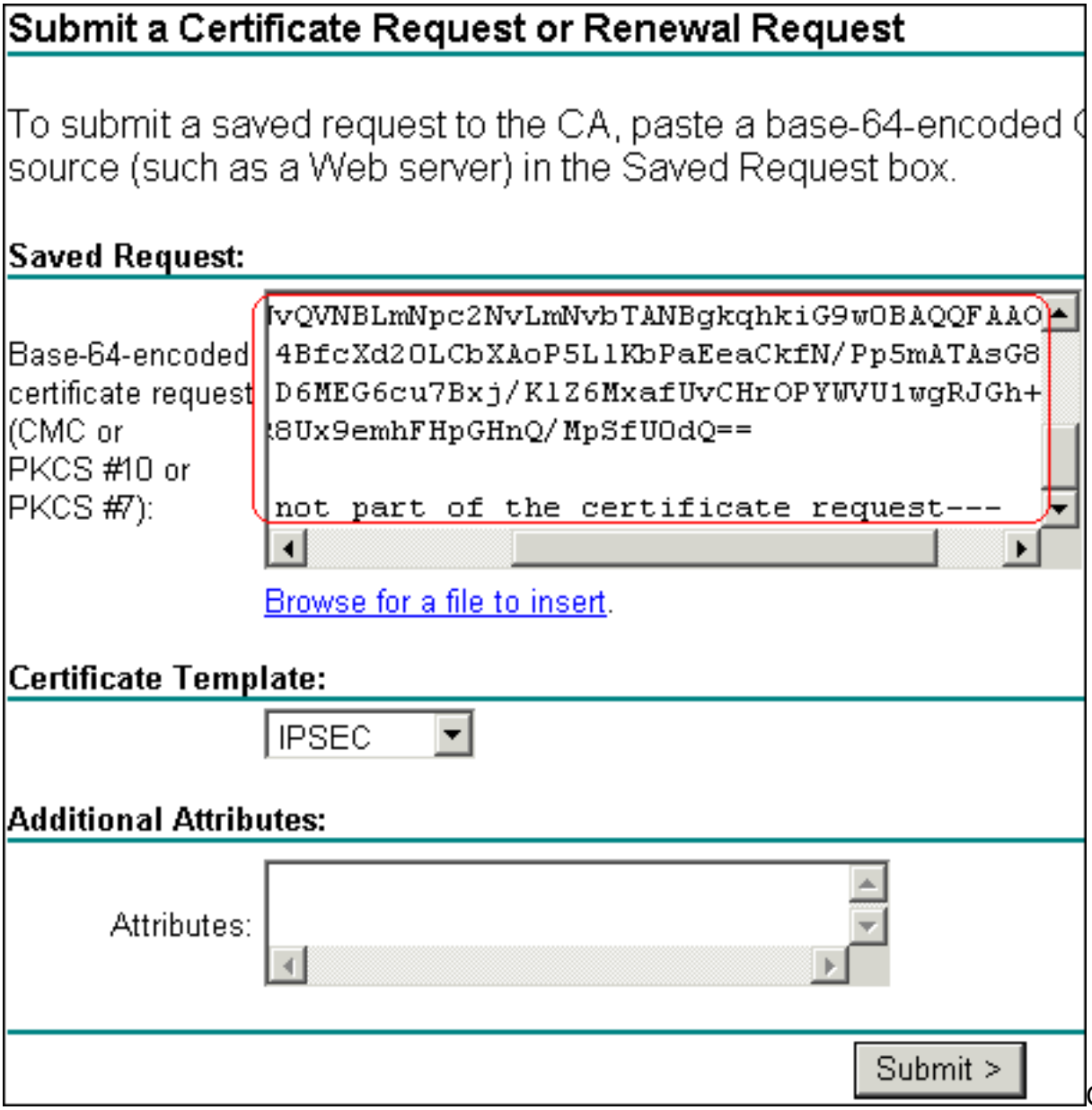
4. Copy the PKCS#10 enrollment request to a text file, and then submit the saved CSR to your 3rd party vendor (such as Microsoft CA) as shown in this procedure:Log in to the CA server 172.16.5.1 with the user credantials supplied to the vpn server.



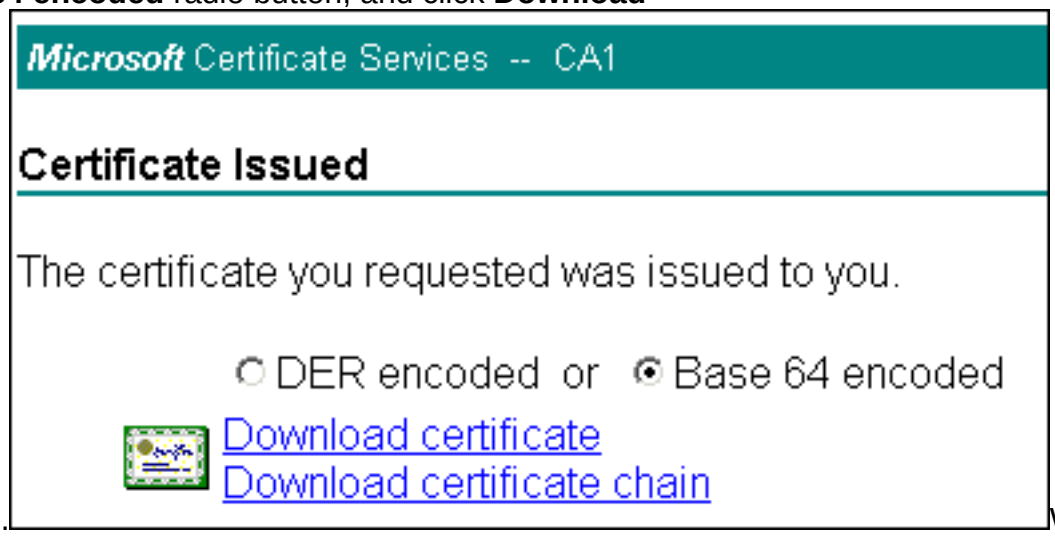
Note: Make sure you have a user account for the ASA (vpn server) with the CA server.Click **Request a certificate > advanced certificate request**, and then select **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file**.



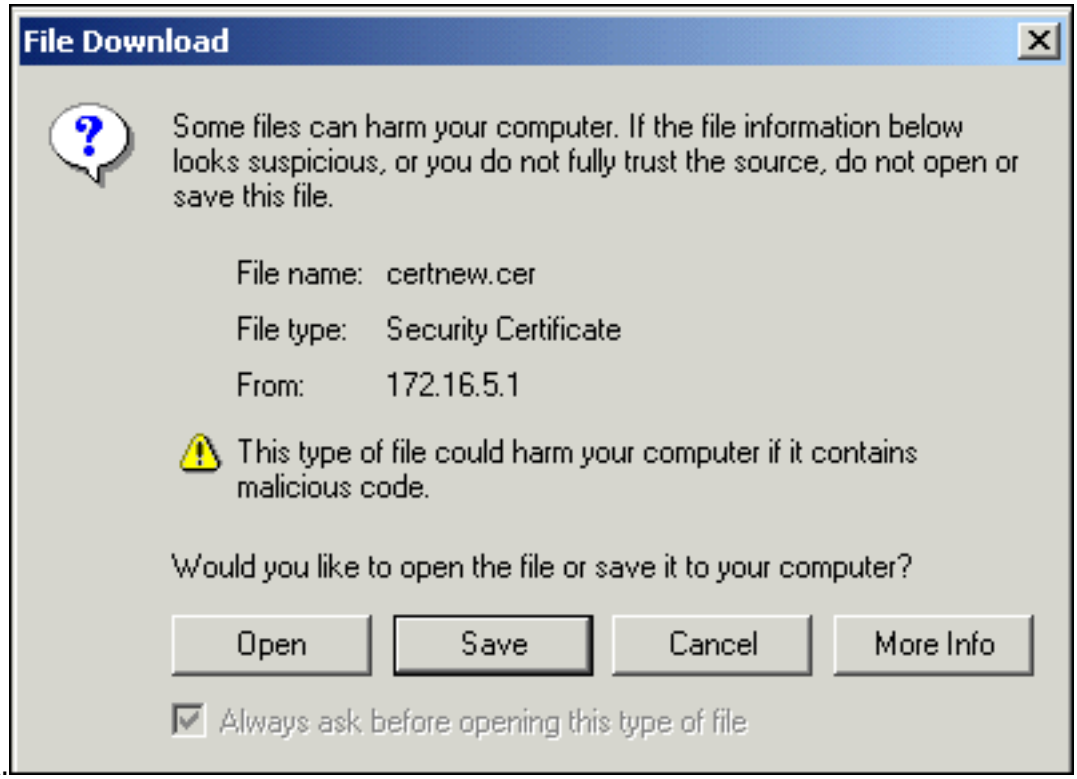
Copy and paste the encoded information into the **Saved Request** text field, and click **Submit**.



Click the **Base 64 encoded** radio button, and click **Download certificate**.



When the File Download dialob box appears, save it with the name **cert_client_id.cer**, which is the identity certificate to be installed on the



ASA.

Command Line Example

CiscoASA

```
CiscoASA(config)#crypto ca enroll CA1 !--- Initiates CSR.
This is the request to be submitted !--- via web or email to
the 3rd party vendor. % Start certificate enrollment .. % The
subject name in the certificate will be:
CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North
Carolina,L=Raleigh % The fully-qualified domain name in the
certificate will be: CiscoASA.cisco.com % Include the device
serial number in the subject name? [yes/no]: no !--- Do not
include the device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes !--- Displays
the PKCS#10 enrollment request to the terminal. !--- You will
need to copy this from the terminal to a text !--- file or
web text field to submit to the 3rd party CA. Certificate
Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgTDk5vc
nRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtc
zEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNvbTEhM
B8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBA
QUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yT
x5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt3oMXS
NPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKargwIDA
QAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISY
2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeOHZf3y
EJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPIbkc2y
kkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/Uo13y
```

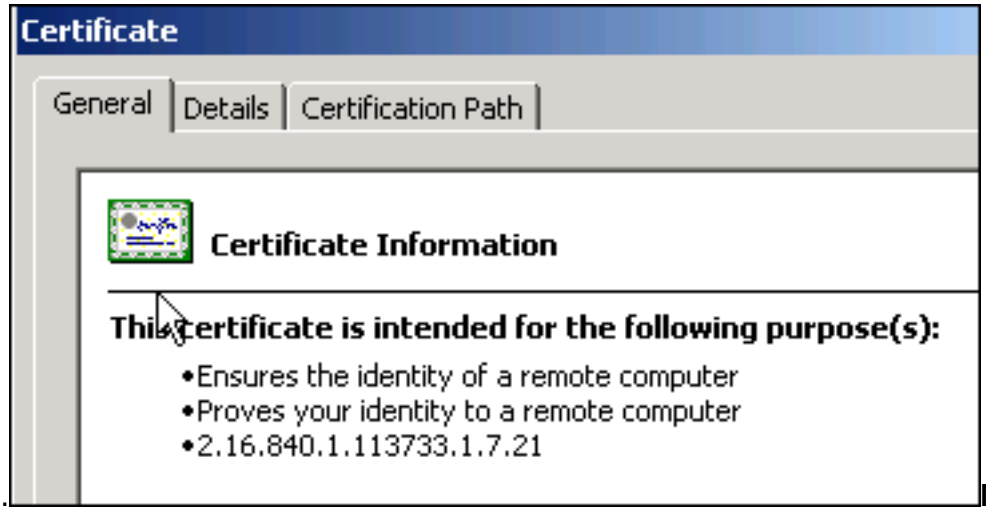
```
WCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not part of
the certificate request--- Redisplay enrollment request?
[yes/no]: no ciscoasa(config)#
```

Step 5. Authenticate the Trustpoint

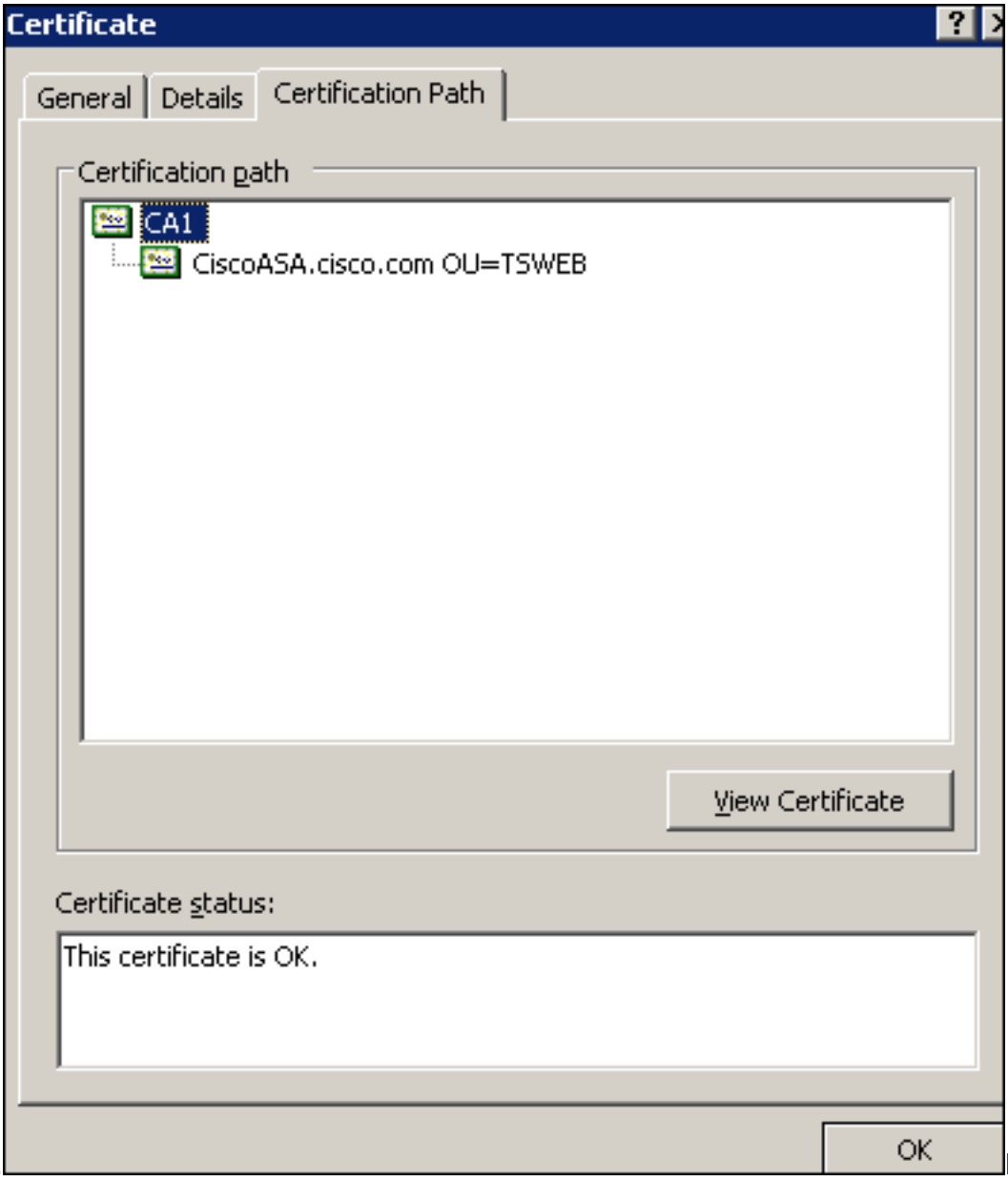
Once you receive the identity certificate from the 3rd party vendor, you can proceed with this step.

ASDM Procedure

1. Save the identity certificate to your local computer.
2. If you were provided a base64-encoded certificate that did not come as a file, you must copy the base64 message, and paste it into a text file.
3. Rename the file with a .cer extension.**Note:** Once the file is renamed with the .cer extension, the file icon should display as a certificate as shown. 

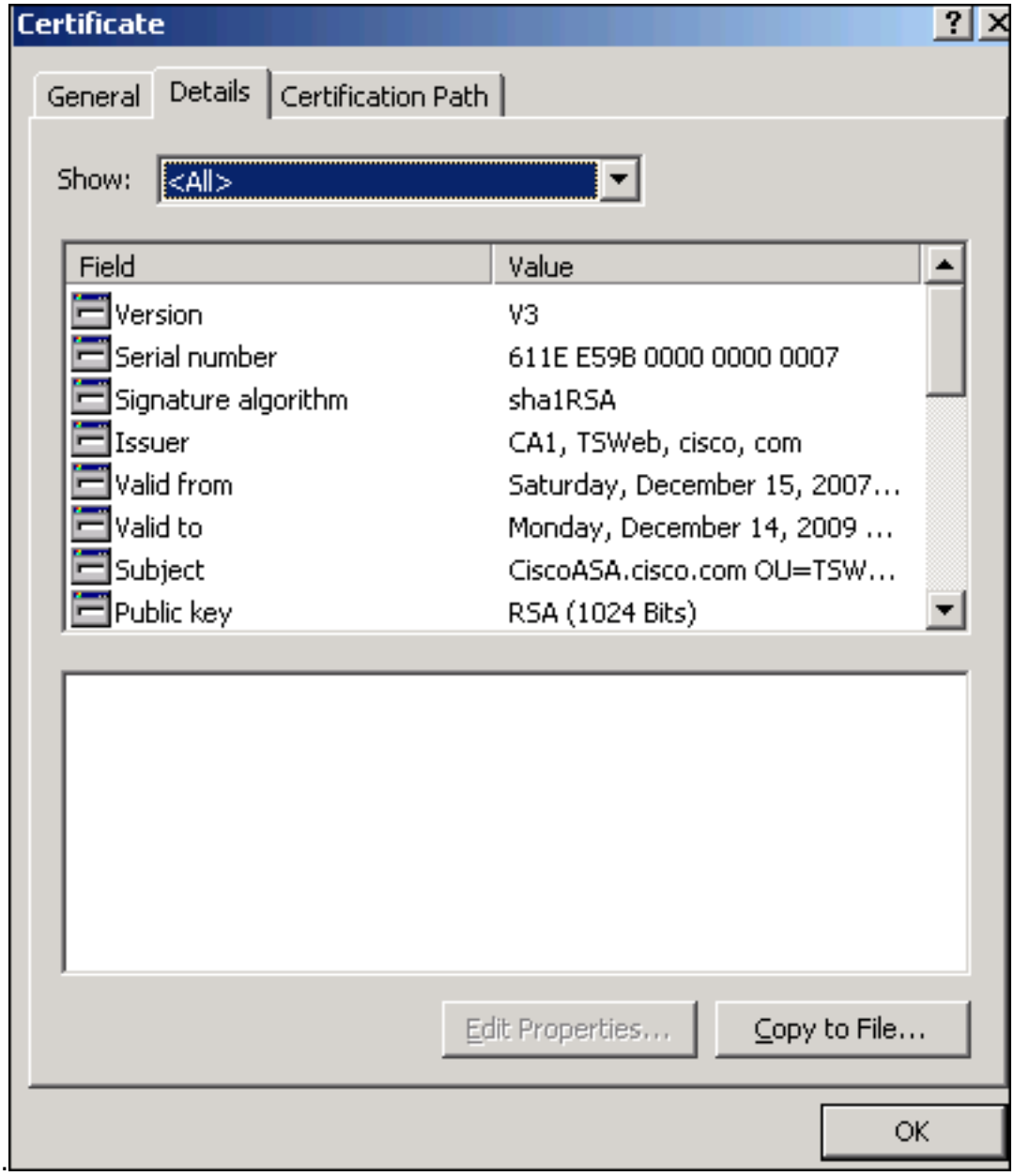
4. Double-click the certificate file. 

Note: If the "Windows does not have enough information to verify this certificate" message appears in the General tab, you must obtain the 3rd party vendor root CA or intermediate CA certificate before you continue with this procedure. Contact your 3rd party vendor or CA administrator in order to obtain the issuing root CA or intermediate CA certificate.
5. Click the **Certificate Path** tab
6. Click the CA certificate located above your issued identity certificate, and click **View**



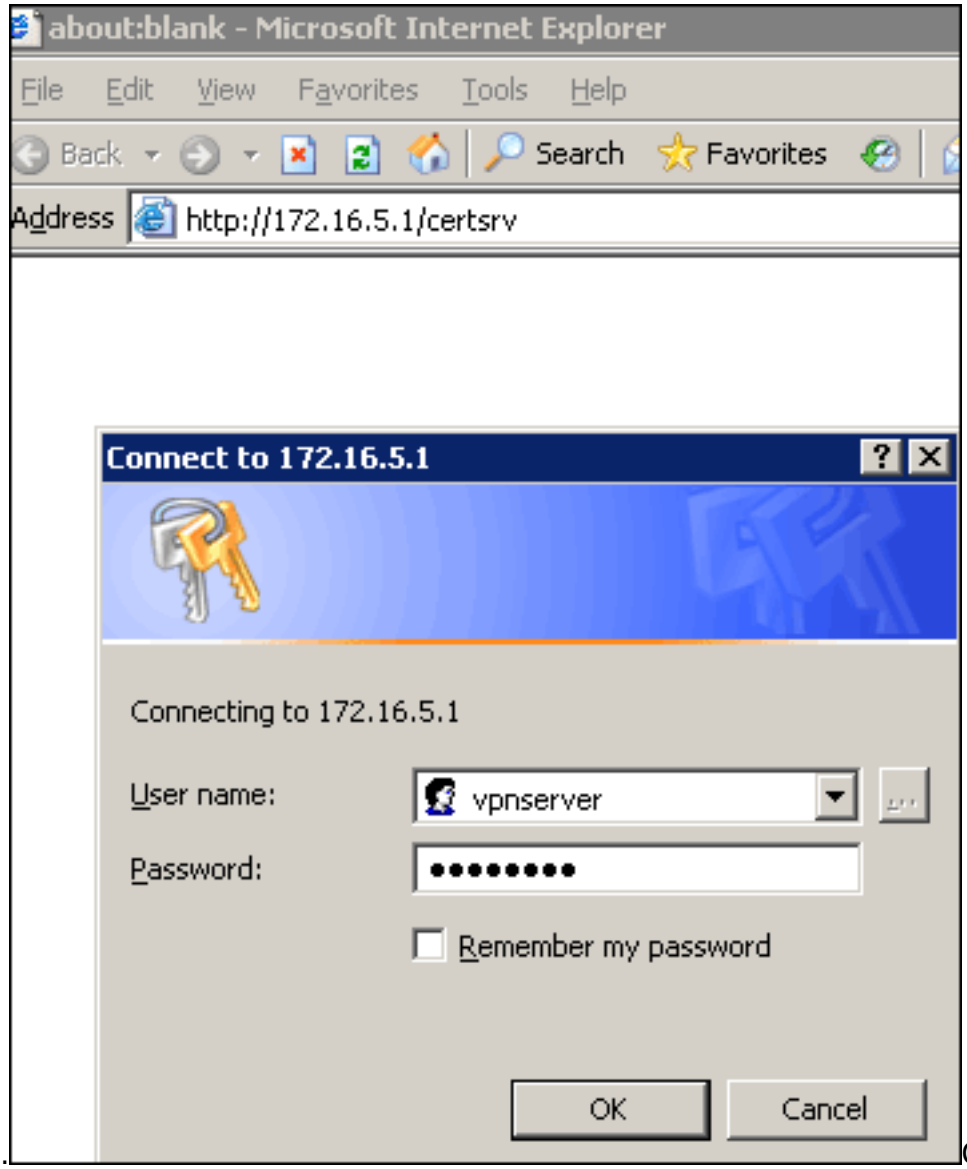
Certificate. Detailed information about the CA certificate appears.

7. Click **Details** in order to know more information about the identity

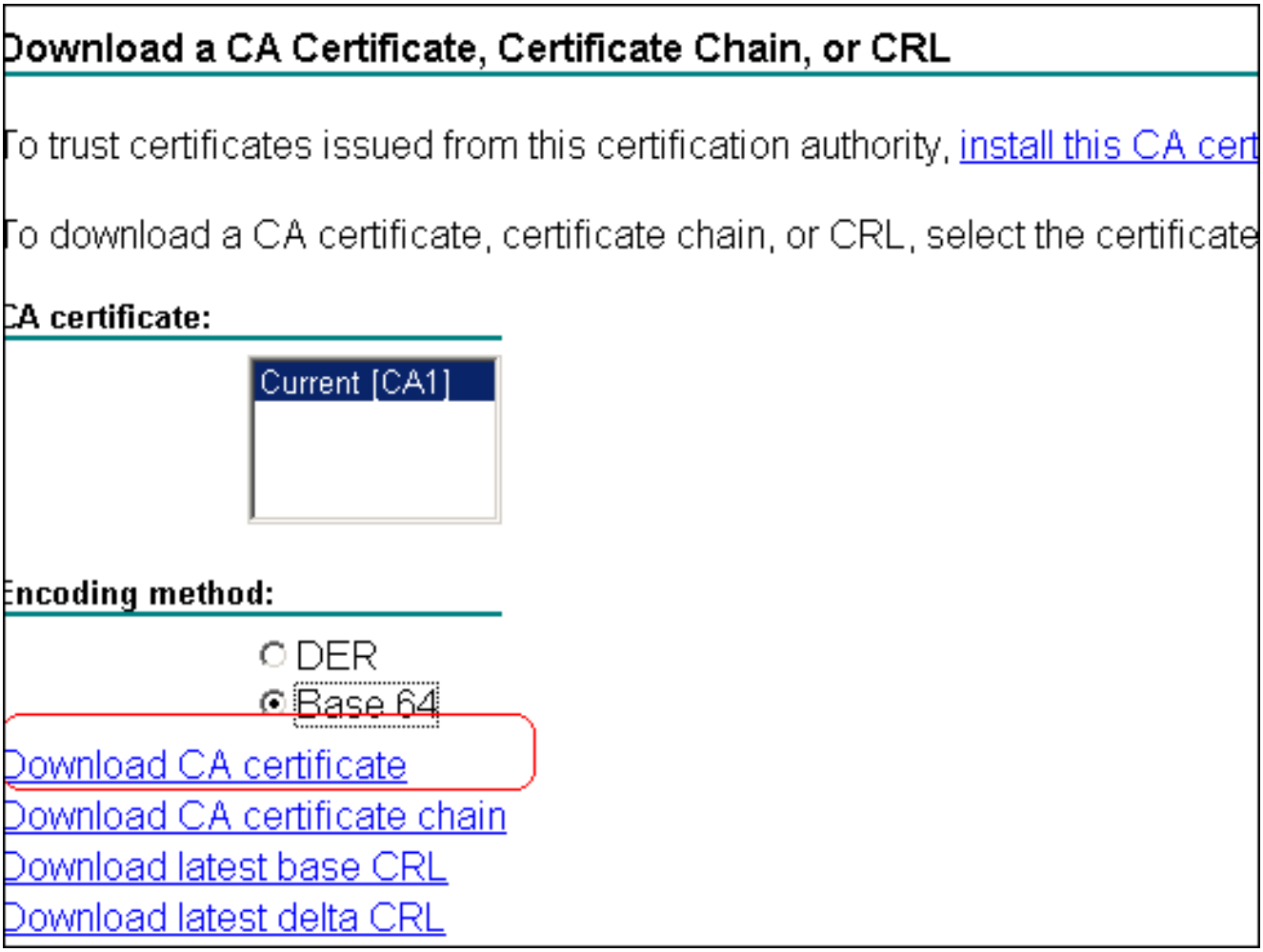


certificate.

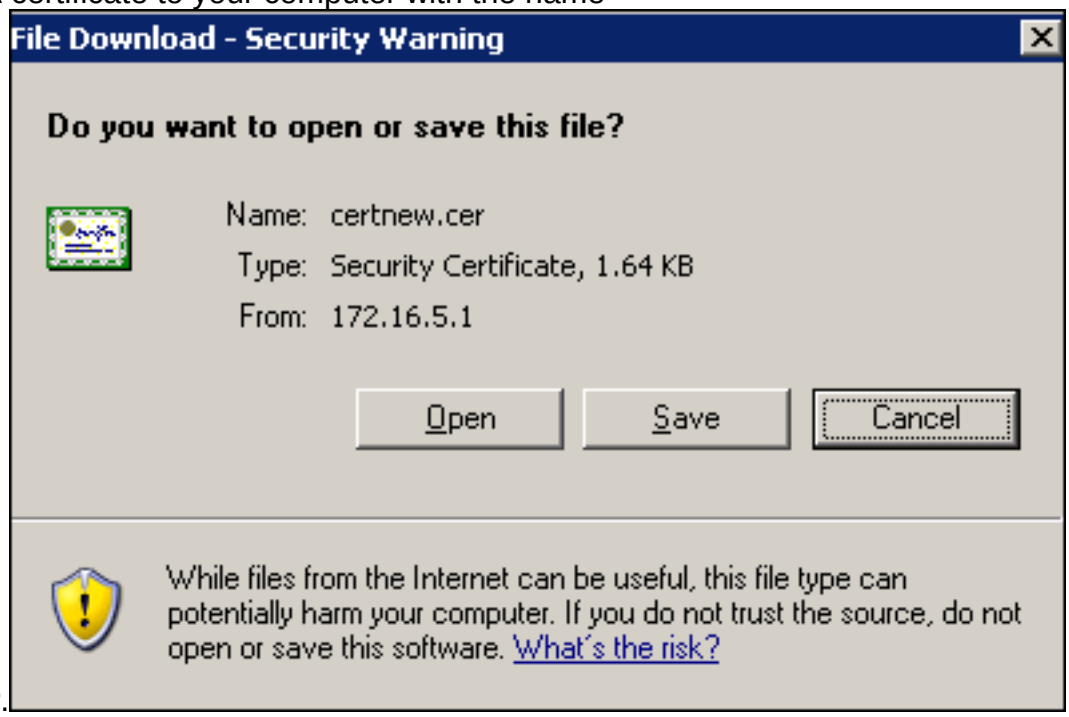
8. Before you install the identity certificate, the CA certificate must be downloaded from the CA server and installed in the ASA. Complete these steps in order to download the CA certificate from the CA server named *CA1*:Log in to the CA server 172.16.5.1 with user credantials supplied to the vpn



server.Click **Download a CA certificate, certificate chain or CRL** , and then select the **Base 64** radio button in order to specify the encoding method.Click the **Download CA certificate**.

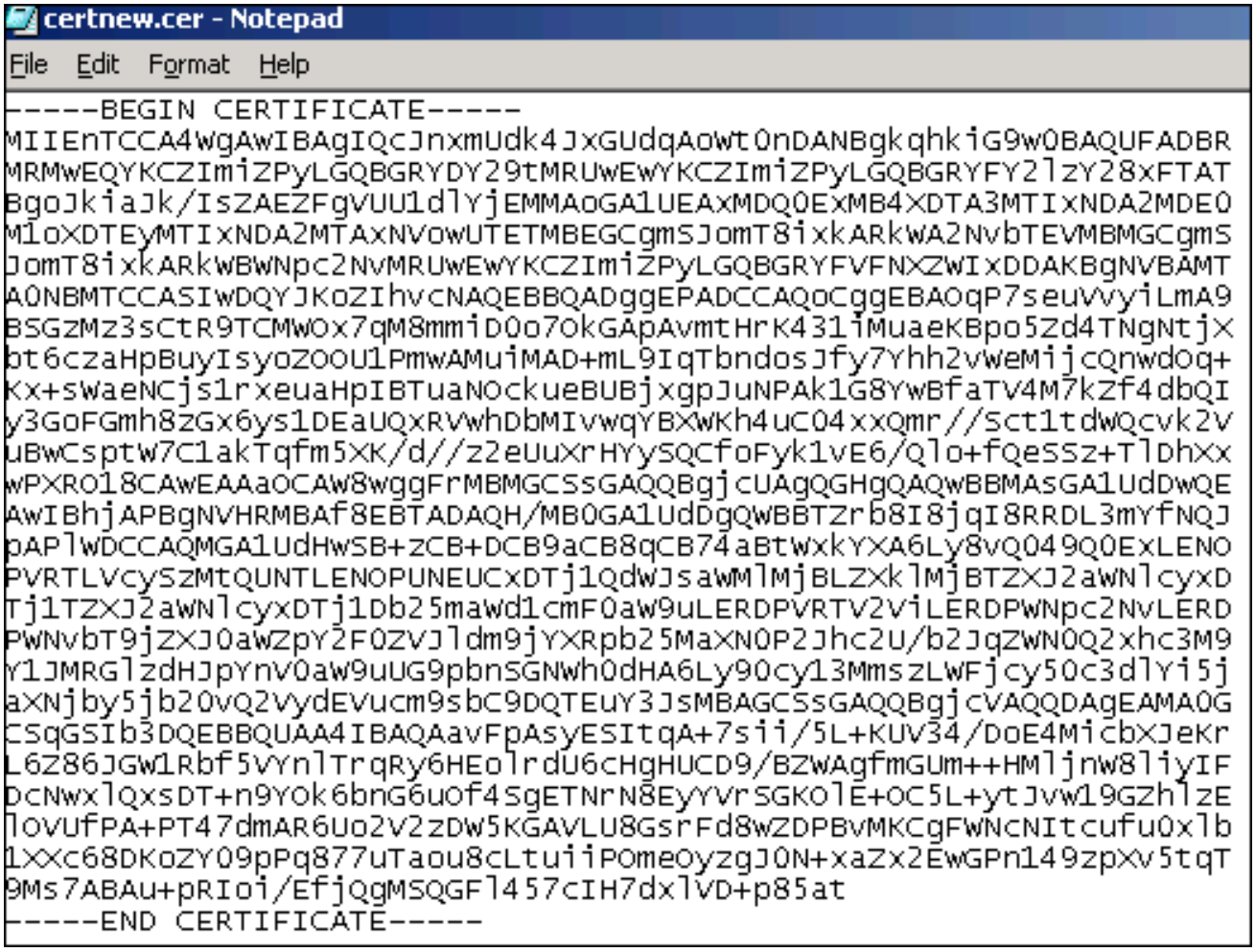


Save the CA certificate to your computer with the name

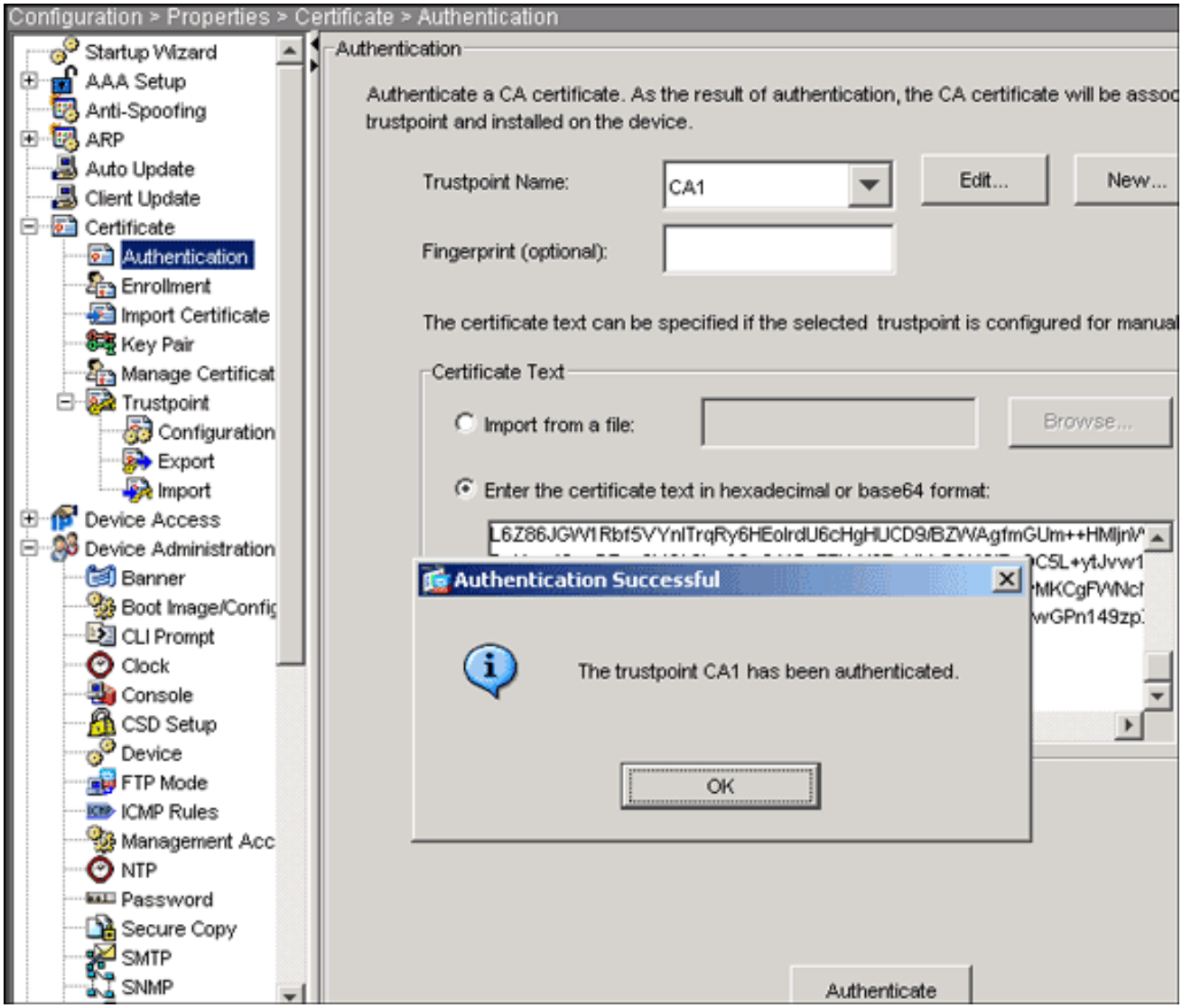


certnew.cer.

9. Browse to the location where you saved the CA certificate.
10. Open the file with a text editor, such as Notepad. (Right-click the file, and choose **Send To > Notepad**.)
11. The base64-encoded message should appear similar to the certificate in this image:



12. Within ASDM, click **Configuration**, and then click **Properties**.
13. Expand **Certificate**, and choose **Authentication**.
14. Click the **Enter the certificate text in hexadecimal or base64 format** radio button.
15. Paste the base64-formatted CA Certificate from your text editor into the text area.
16. Click
    Authenticate.



17. Click **OK**.

Command Line Example

CiscoASA
CiscoASA(config)#**crypto ca authenticate CA1** *!--- Initiates the prompt to paste in the base64 CA root !--- or intermediate certificate.* Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself **-----BEGIN CERTIFICATE-----** **MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR** **MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT** **BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNDA2MDE0** **M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmS** **JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAKBgNVBAMT** **A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuVvyiLmA9** **BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX** **bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMijcQnwdOq+** **Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI** **y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1tdWQcv**

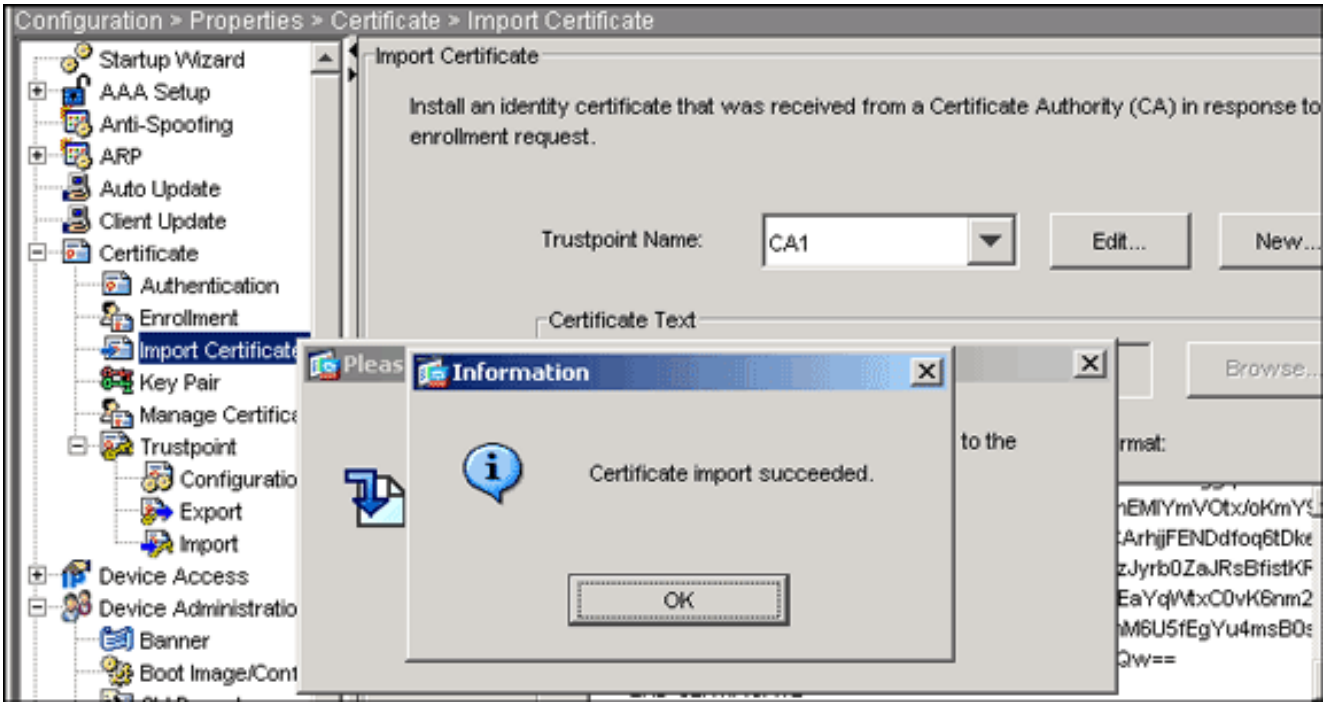
```
k2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlD
hXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdD
wQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYf
NQJ
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049Q0ExL
ENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlc
yxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvL
ERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc
3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50c3dlY
i5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQDAgEAM
A0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJ
eKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMljnW8li
yIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw19GZh
lzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNItcufu0
xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5
tqT 9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+p85at -----END
CERTIFICATE----- quit !--- Manually pasted certificate into
CLI. INFO: Certificate has the following attributes:
Fingerprint: 98d66001 f65d98a2 b455fbce d672c24a Do you
accept this certificate? [yes/no]: yes Trustpoint CA
certificate accepted. % Certificate successfully imported
CiscoASA(config)#
```

Step 6. Install the Certificate

ASDM Procedure

Use the identity certificate provided by the 3rd party vendor to perform these steps:

1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and then choose **Import Certificate**.
3. Click the **Enter the certificate text in hexadecimal or base64 format** radio button, and paste the base64 identity certificate into the text field.



4. Click **Import**, and then click **OK**.

Command Line Example

CiscoASA

```
CiscoASA(config)#crypto ca import CA1 certificate !---
Initiates prompt to paste the base64 identity certificate !---
provided by the 3rd party vendor. % The fully-qualified
domain name in the certificate will be: CiscoASA.cisco.com
Enter the base 64 encoded certificate. End with the word
"quit" on a line by itself !--- Paste the base 64 certificate
provided by the 3rd party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBRMRMwE
QYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTATBgoJk
iaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUzOVoXD
TA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhc
m9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zM
SQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJKoZIh
vcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14CqB9j3
HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCOsS8iq
xqO
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lzY29BU0Eu
Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAfBgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJs
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb
```

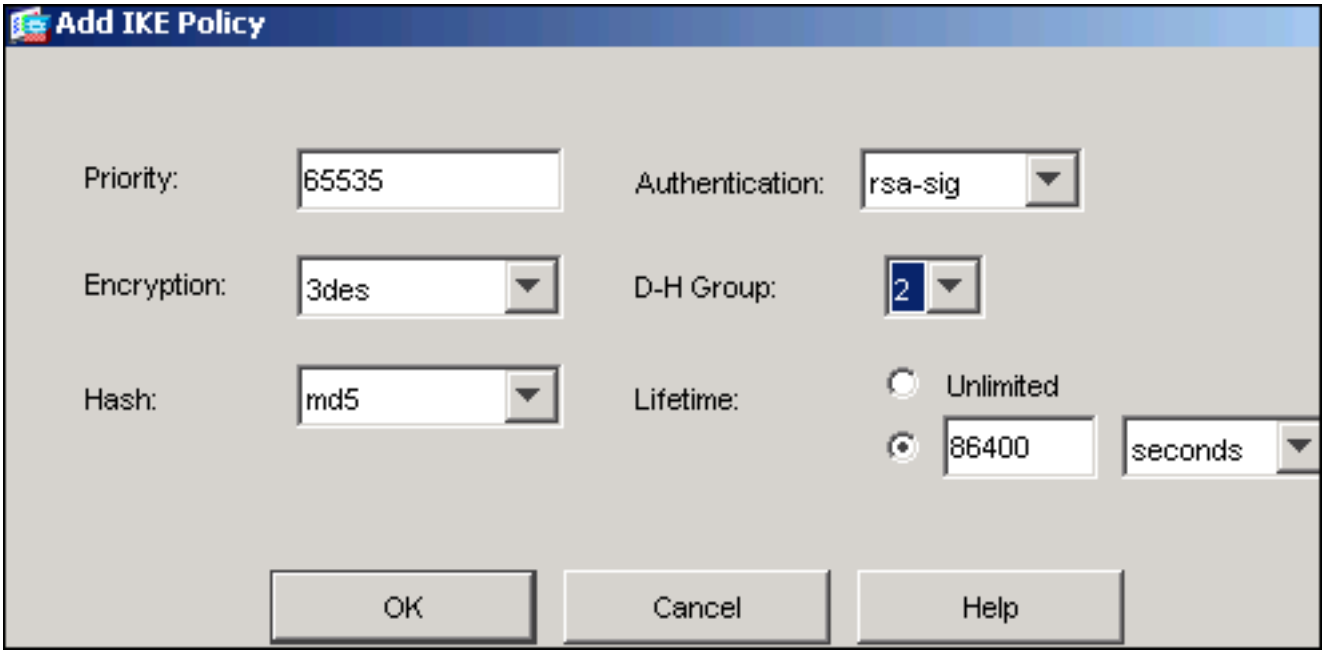
```
25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0d
HA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9DQTEuY
3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL
0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2Vyd
mlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1jb20/Y
0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob
3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5jaXNjb
y5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21fQ0ExL
mNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1UdEwEB/
wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEBAIqCa
A9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB7wXQa
Gph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8+3Ghg
8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b901516IzQP5l51Y
B0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87ychngK
B+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtSt1nwL
psc lL5nuPsd8MaexBc= -----END CERTIFICATE----- quit INFO:
Certificate successfully imported CiscoASA(config)#
```

Step 7. Configure Remote Access VPN (IPSec) to Use the Newly Installed Certificate

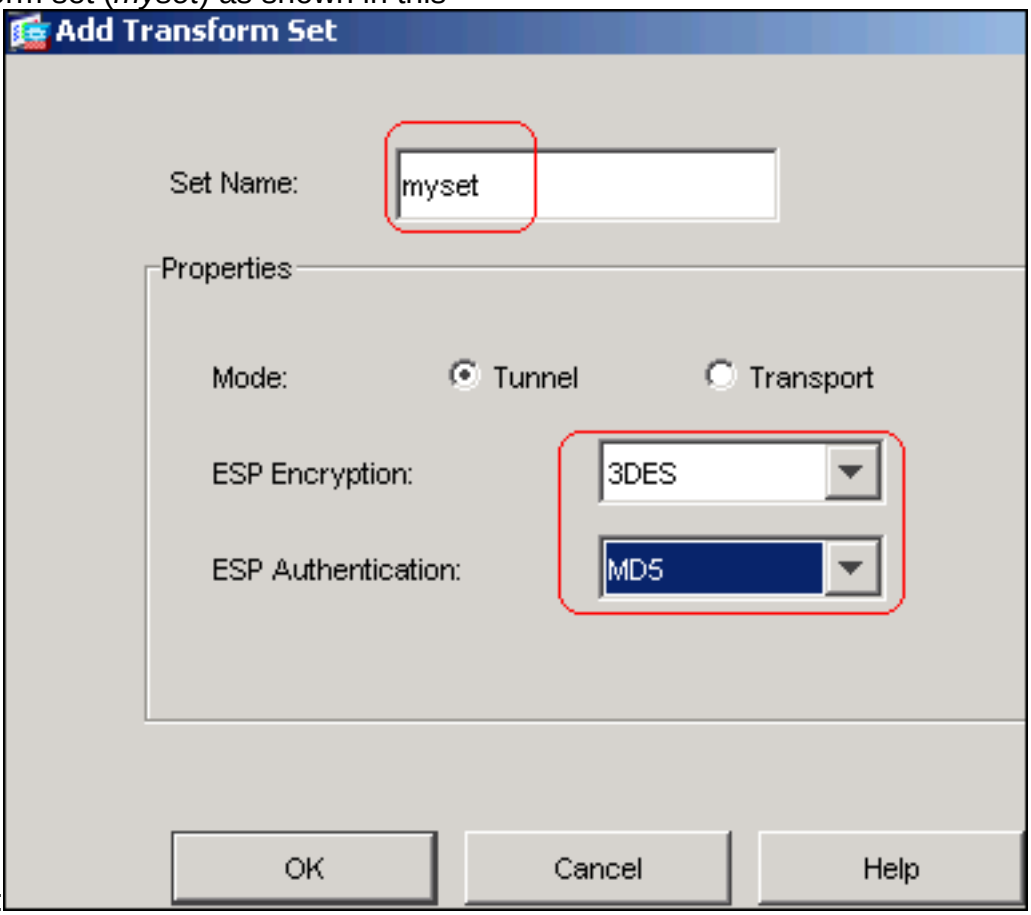
ASDM Procedure

Complete these steps in order to configure the remote access VPN:

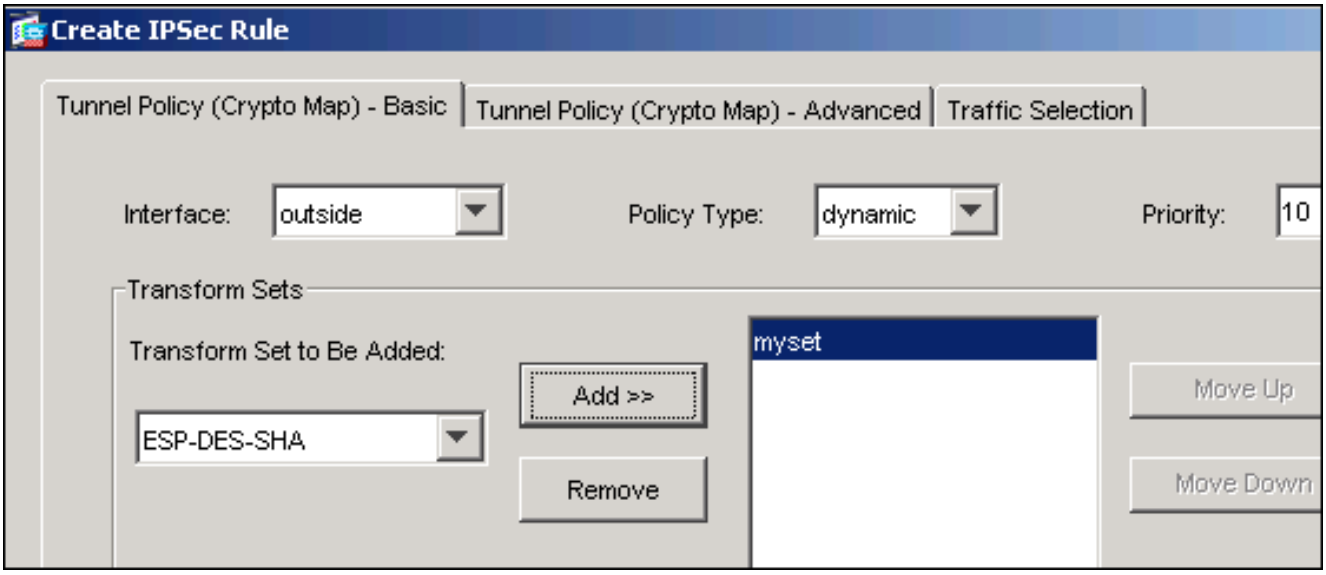
1. Choose **Configuration > VPN > IKE > Policies > Add** in order to create a ISAKMP policy 65535 as shown in this
   image.



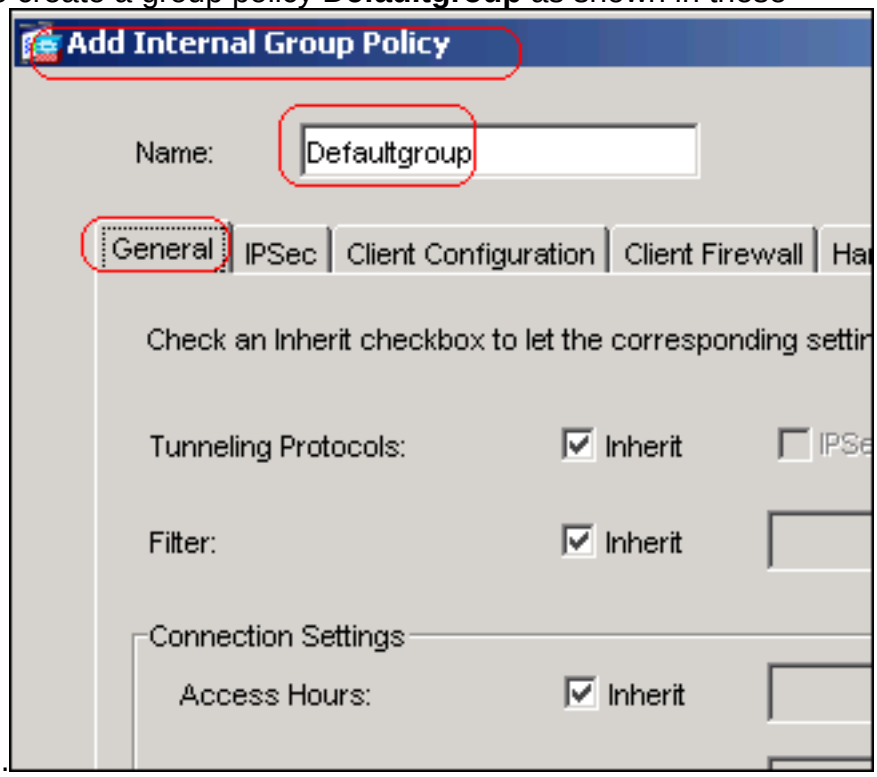
2. Click **OK**, and then click **Apply**.
3. Choose **Configuration > VPN > IPSec > Transform Sets >Add** in order to create a transform set (*myset*) as shown in this image:

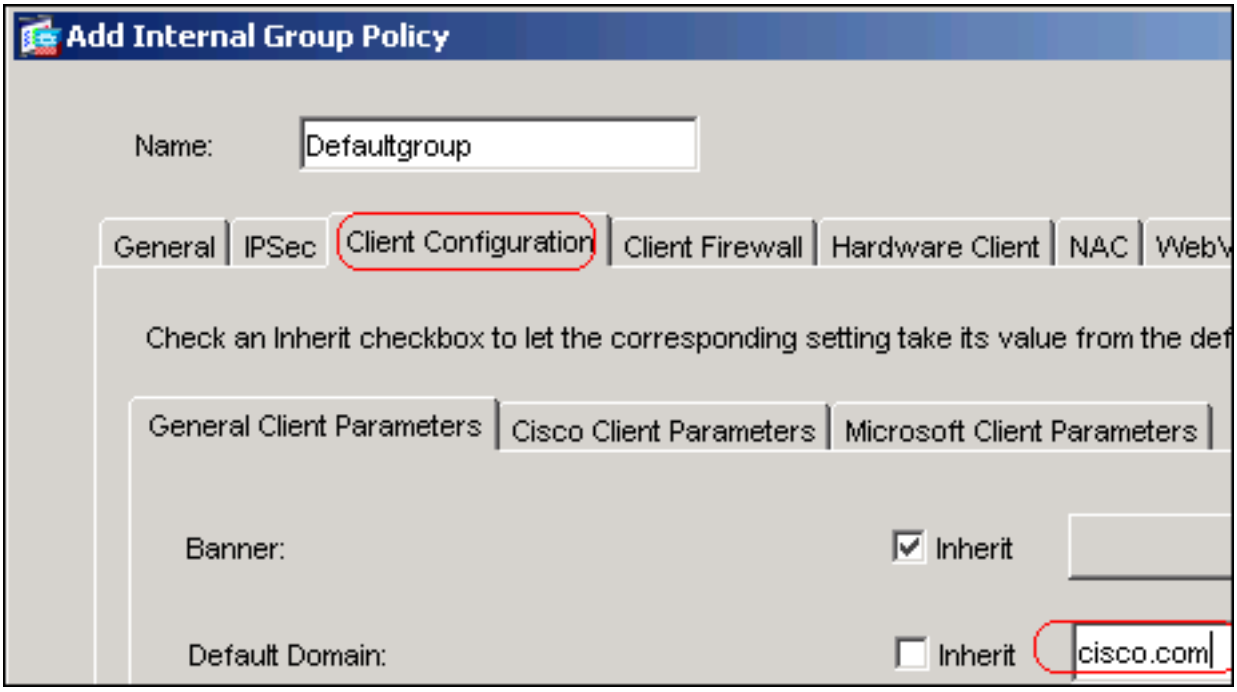


4. Click **OK**, and then **Apply**
5. Choose **Configuration > VPN > IPSec > IPSec Rules >Add** in order to create a crypto map with dynamic policy of priority 10 as shown in this image:

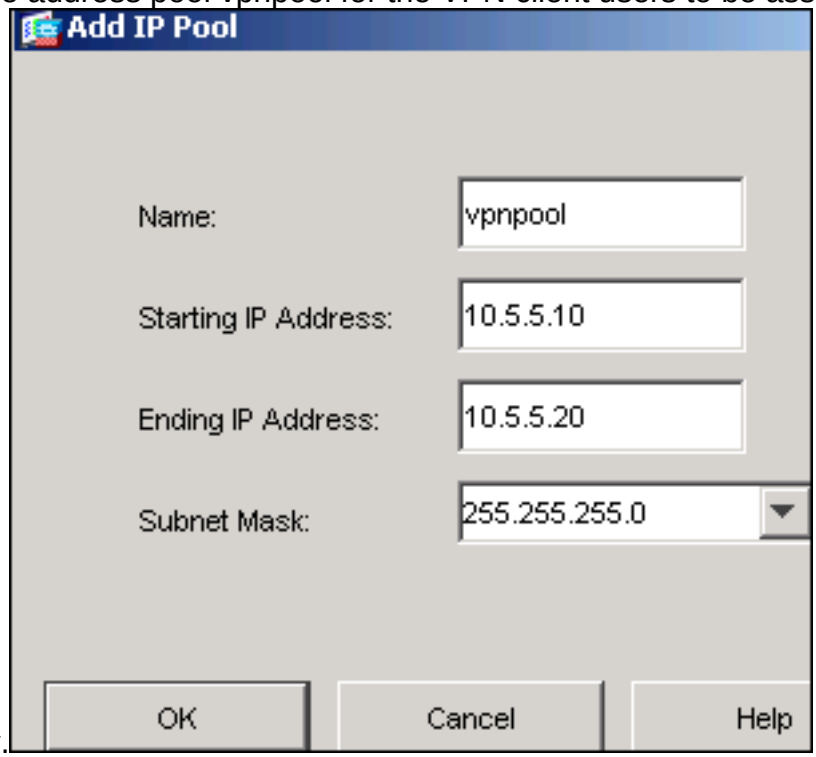


6. Click **OK**, and then **Apply**
7. Choose **Configuration > VPN > General > Group Policy > Add Internal Group Policy** in order to create a group policy **Defaultgroup** as shown in these images.

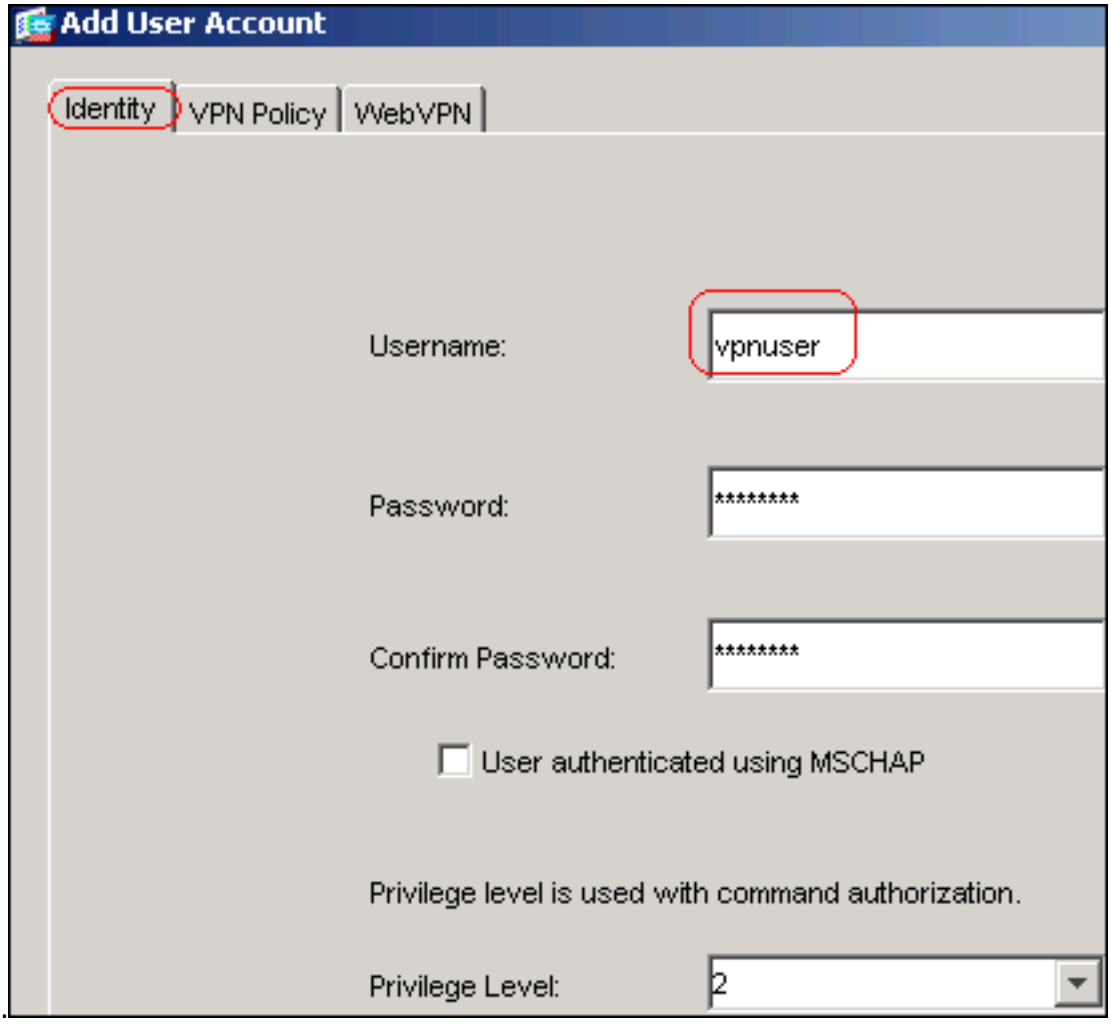




8. Click **OK**, and then **Apply**
9. Choose **Configuration > VPN > IP Address Management > IP Pools > Add** in order to configure the address pool vpnpool for the VPN client users to be assigned dynamically.

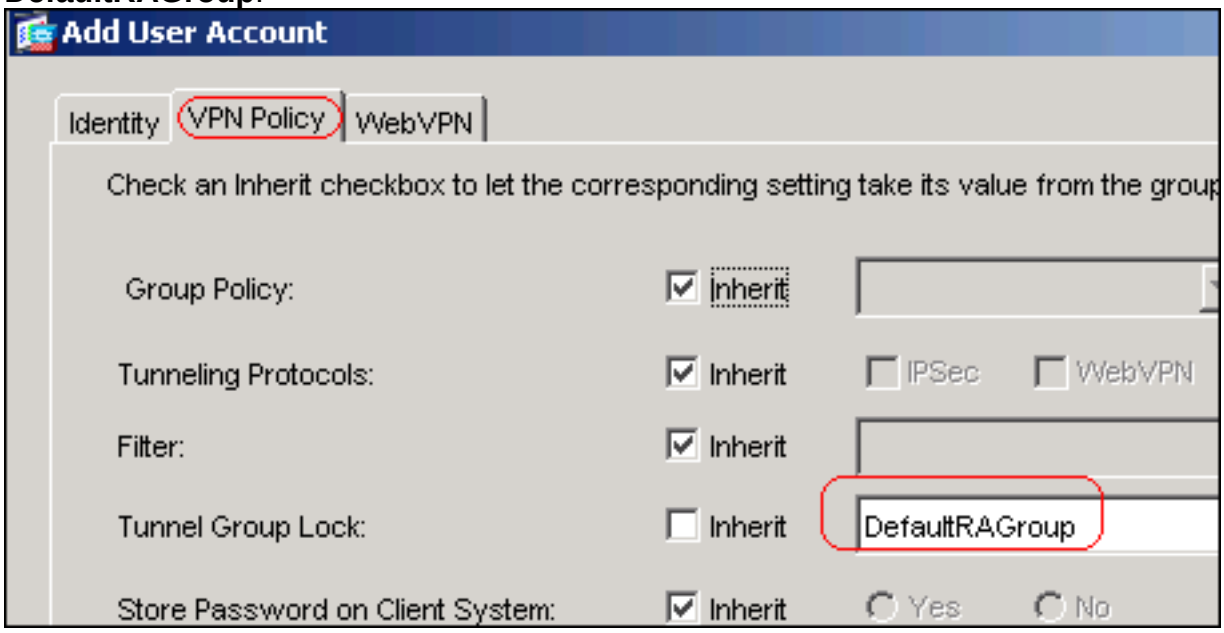


10. Click **OK**, and then **Apply**
11. Choose **Configuration > VPN > General > Users > Add** in order to create a user account **vpnuser** for VPN client

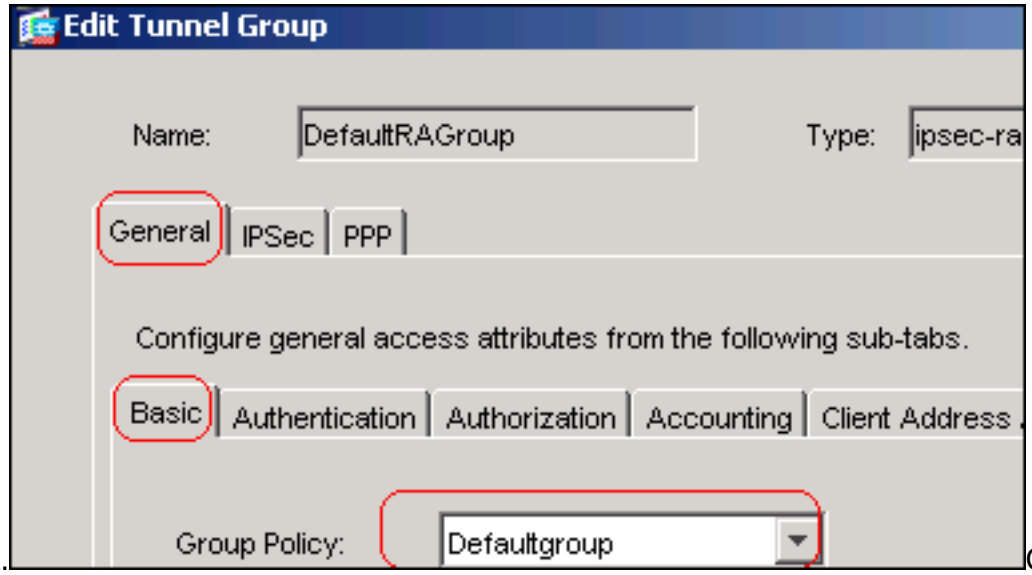


access.

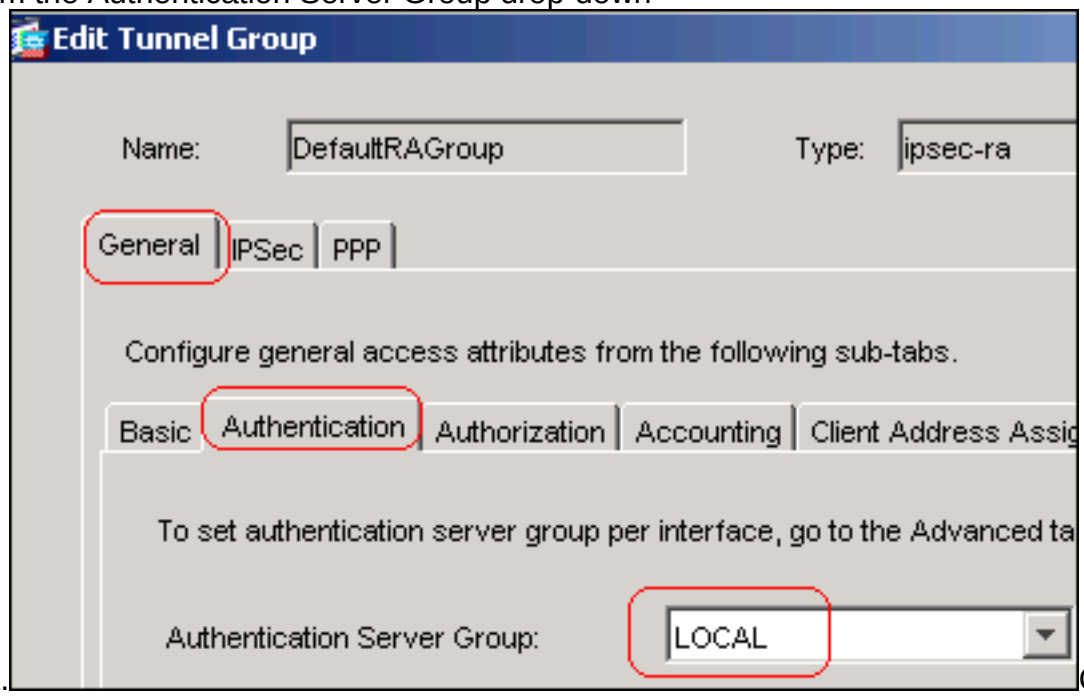
12. Add this user to **DefaultRAGroup**.



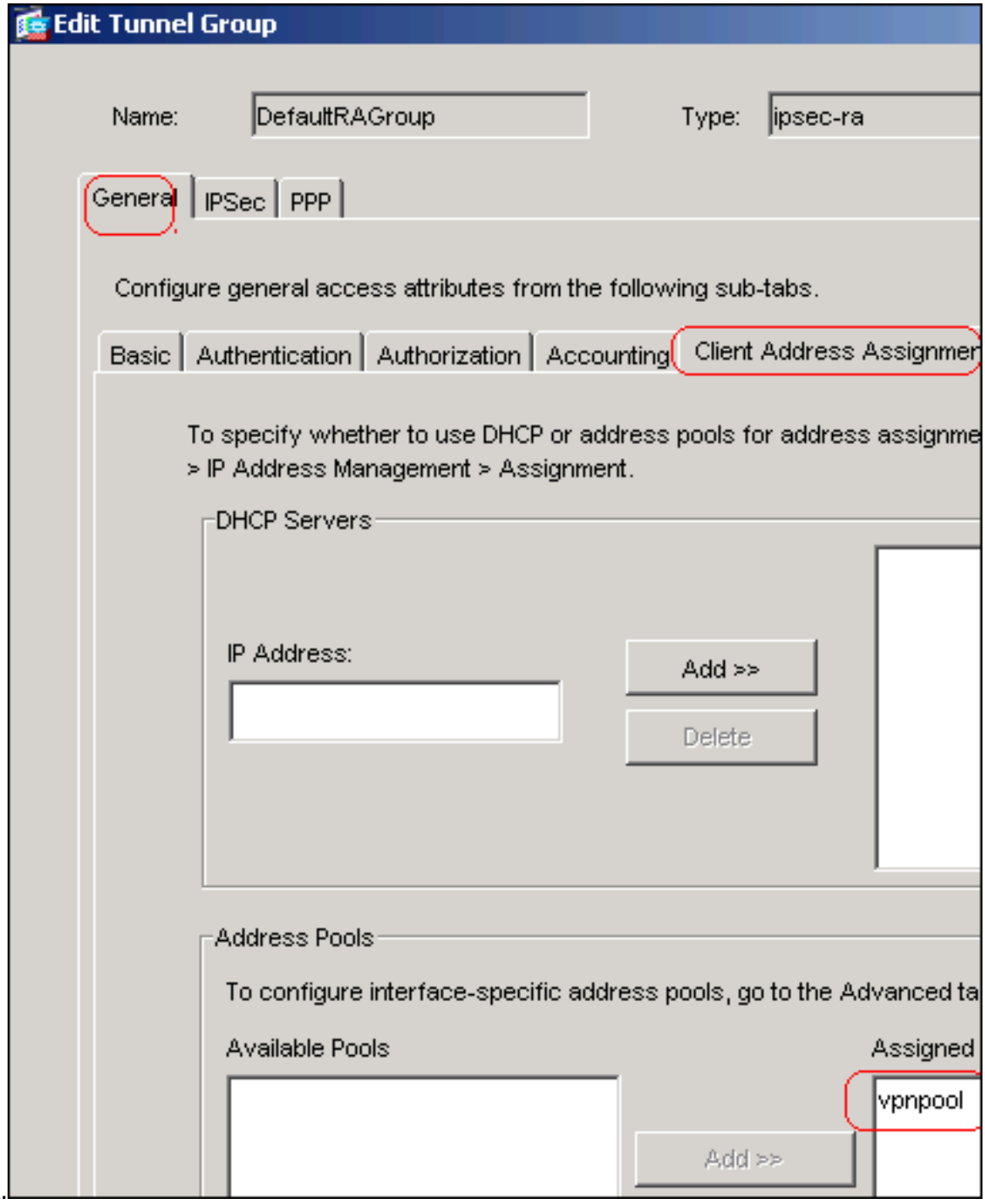
13. Click **OK**, and then **Apply**
14. Edit the DefaultRAGroup as described in this procedure:Choose **Configuration > VPN > General > Tunnel Group > Edit**.Choose **Defaultgroup** from the Group Policy drop-down



list.Choose **LOCAL** from the Authentication Server Group drop-down



list.Choose **vpnpool** from the Client Address Assignment drop-down



list.

15. Click **OK**, and then **Apply**.

Command Line Example

CiscoASA
CiscoASA(config)#**crypto isakmp enable outside** CiscoASA(config)#**crypto isakmp policy 65535** CiscoASA(config-isakmp-policy)#**authentication rsa-sig** CiscoASA(config-isakmp-policy)#**encryption 3des** CiscoASA(config-isakmp-policy)#**hash md5** CiscoASA(config-isakmp-policy)#**group 2** CiscoASA(config-isakmp-policy)#**lifetime 86400** CiscoASA(config-isakmp-policy)#**exit** CiscoASA(config)#**crypto isakmp identity auto** *!-- Phase 1 Configurations* CiscoASA(config)#**crypto ipsec transform-set myset esp-3des esp-md5-hmac** CiscoASA(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set myset** CiscoASA(config)#**crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map** CiscoASA(config)#**crypto map outside_map interface outside** *!-- Phase 2 Configurations* CiscoASA(config)#**group-policy**

```
defaultgroup internal CiscoASA(config)#group-policy
defaultgroup attributes CiscoASA(config-group-
policy)#default-domain value cisco.com CiscoASA(config-group-
policy)#exit !--- Create a group policy "Defaultgroup" with
domain name !--- cisco.com CiscoASA(config)#username vpnuser
password password123 CiscoASA(config)#username vpnuser
attributes CiscoASA(config-username)#group-lock value
DefaultRAGroup CiscoASA(config-username)#exit !--- Create an
user account "vpnuser" and added to "DefaultRAGroup"
CiscoASA(config)#tunnel-group DefaultRAGroup general-
attributes !--- The Security Appliance provides the default
tunnel groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool !---
Associate the vpnpool to the tunnel group using the address
pool. CiscoASA(config-tunnel-general)#default-group-policy
Defaultgroup !--- Associate the group policy "Defaultgroup"
to the tunnel group. CiscoASA(config-tunnel-general)#exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit !--- Associate the
trustpoint CA1 for IPSec peer authentication
```

ASA Configuration Summary

CiscoASA

```
CiscoASA#show running-config : Saved : ASA Version 7.2(2) !
hostname CiscoASA domain-name cisco.com enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 192.168.1.5
255.255.255.0 ! interface Ethernet0/1 shutdown nameif inside
security-level 100 ip address 10.2.2.1 255.255.255.0 !
interface Ethernet0/2 nameif DMZ security-level 90 ip address
10.77.241.142 255.255.255.192 ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-level
no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa722-k8.bin ftp mode passive dns server-group
DefaultDNS domain-name cisco.com access-list 100 extended
permit ip 10.2.2.0 255.255.255.0 10.5.5.0 255.255.255.0 pager
lines 24 mtu outside 1500 mtu inside 1500 mtu DMZ 1500 ip
local pool vpnpool 10.5.5.10-10.5.5.20 mask 255.255.255.0 no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp timeout
14400 nat (inside) 0 access-list 100 route outside 10.1.1.0
255.255.255.0 192.168.1.1 1 route outside 172.16.5.0
255.255.255.0 192.168.1.1 1 route DMZ 0.0.0.0 0.0.0.0
10.77.241.129 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
group-policy Defaultgroup internal group-policy Defaultgroup
attributes default-domain value cisco.com username vpnuser
password TXttW.eFqbHusJQM encrypted username vpnuser
attributes group-lock value DefaultRAGroup http server enable
http 0.0.0.0 0.0.0.0 outside http 0.0.0.0 0.0.0.0 DMZ no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac crypto
dynamic-map outside_dyn_map 10 set transform-set myset crypto
map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside crypto ca trustpoint
```

```
CA1 enrollment terminal subject-name cn=CiscoASA.cisco.com
OU=TSWEB, O=Cisco Systems, C=US,St=North Carolina,L=Raleigh
keypair my.CA.key crl configure crypto ca certificate chain
CA1 certificate 3f14b70b00000000001f 308205eb 308204d3
a0030201 02020a3f 14b70b00 00000000 1f300d06 092a8648
86f70d01 01050500 30513113 3011060a 09922689 93f22c64
01191603 636f6d31 15301306 0a099226 8993f22c 64011916
05636973 636f3115 3013060a 09922689 93f22c64 01191605
54535765 62310c30 0a060355 04031303 43413130 1e170d30
37313232 37313430 3033365a 170d3038 31323236 31343030
33365a30 67311330 11060a09 92268993 f22c6401 19160363
6f6d3115 3013060a 09922689 93f22c64 01191605 63697363
6f311530 13060a09 92268993 f22c6401 19160554 53576562
310e300c 06035504 03130555 73657273 31123010 06035504
03130976 706e7365 72766572 30819f30 0d06092a 864886f7
0d010101 05000381 8d003081 89028181 00b8e20a a8332356
b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a
570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01
a14cc01d 98b1320e 9fe84905 5ab94b18 ef308eb1 2f22ab1a
8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2 d903f722
bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64
4d020301 0001a382 03313082 032d300b 0603551d 0f040403
02052030 34060355 1d11042d 302ba029 060a2b06 01040182
37140203 a01b0c19 76706e73 65727665 72405453 5765622e
63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb
490cde1a fe2d63e3 1e1fb28c 974c4216 301f0603 551d2304
18301680 14d9adbf 08f23a88 f114432f 79987cd4 09a403e5
58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081
ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453
2d57324b 332d4143 532c434e 3d434450 2c434e3d 5075626c
69632532 304b6579 25323053 65727669 6365732c 434e3d53
65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e
2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f
6d3f6365 72746966 69636174 65526576 6f636174 696f6e4c
6973743f 62617365 3f6f626a 65637443 6c617373 3d63524c
44697374 72696275 74696f6e 506f696e 74863568 7474703a
2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363
6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131 2e63726c
3082011d 06082b06 01050507 01010482 010f3082 010b3081
a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e
3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230
4b657925 32305365 72766963 65732c43 4e3d5365 72766963
65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54
53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143
65727469 66696361 74653f62 6173653f 6f626a65 6374436c
6173733d 63657274 69666963 6174696f 6e417574 686f7269
7479305d 06082b06 01050507 30028651 68747470 3a2f2f74
732d7732 6b332d61 63732e74 73776562 2e636973 636f2e63
6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143
532e5453 5765622e 63697363 6f2e636f 6d5f4341 312e6372
74301506 092b0601 04018237 14020408 1e060045 00460053
300c0603 551d1301 01ff0402 30003015 0603551d 25040e30
0c060a2b 06010401 82370a03 04304406 092a8648 86f70d01
090f0437 3035300e 06082a86 4886f70d 03020202 0080300e
06082a86 4886f70d 03040202 00803007 06052b0e 03020730
0a06082a 864886f7 0d030730 0d06092a 864886f7 0d010105
05000382 010100bf 99b9daf2 e24f1bd6 ce8271eb 908fadb3
772df610 0e78b198 f945f379 5d23a120 7c38ae5d 8f91b3ff
3da5d139 46d8fb6e 20d9a704 b6aa4113 24605ea9 4882d441
09f128ab 4c51a427 fa101189 b6533eef adc28e73 fcfed3f1
f4e64981 0976b8a1 2355c358 a22af8bb e5194b42 69a7c2f6
c5a116f6 d9d77fb3 a7f3d201 e3cff8f7 48f8d54e 243d2530
31a733af 0e1351d3 9c64a0f7 4975fc66 a017627c cfd0ea22
2992f463 9412b388 84bf8b33 bd9f589a e7087262 a4472e69
```

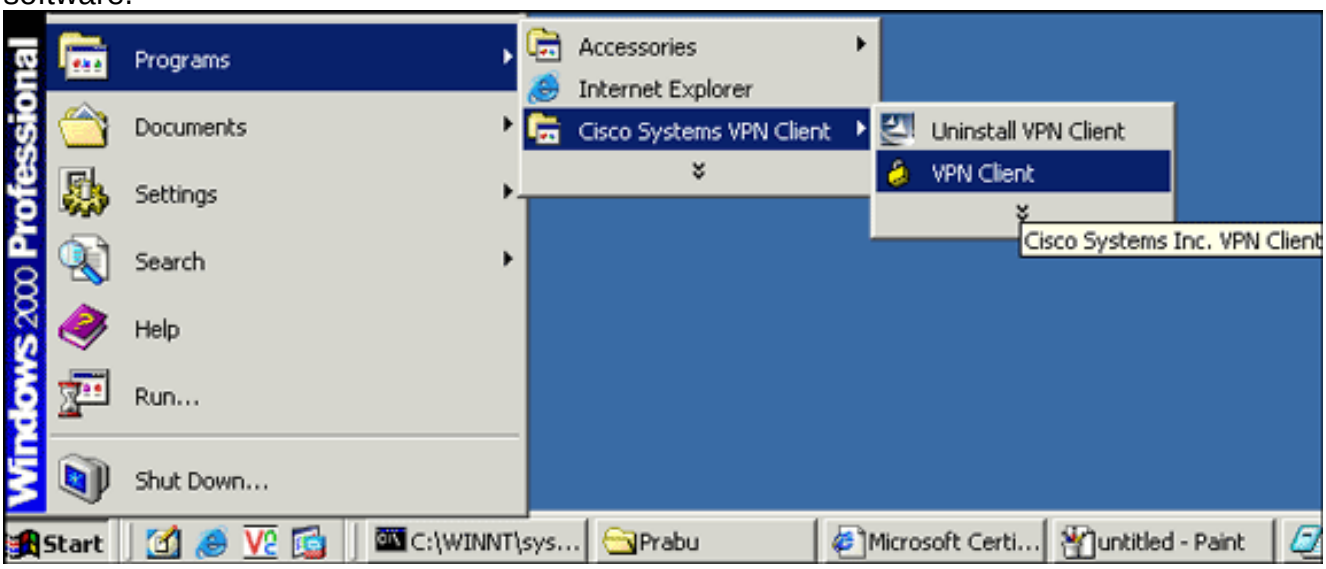
```
775ab608 e5714857 4f887163 705220e3 aca870be b107ab8d
73faf76d b3550553 1a2b873f 156f9dff 5386c839 1380fda8
945a7f6c c2e9d5c8 83e2e761 394dd4da 63eaefc6 a44df5 quit
certificate ca 7099f1994764e09c4651da80a16b749c 3082049d
30820385 a0030201 02021070 99f19947 64e09c46 51da80a1
6b749c30 0d06092a 864886f7 0d010105 05003051 31133011
060a0992 268993f2 2c640119 1603636f 6d311530 13060a09
92268993 f22c6401 19160563 6973636f 31153013 060a0992
268993f2 2c640119 16055453 57656231 0c300a06 03550403
13034341 31301e17 0d303731 32313430 36303134 335a170d
31323132 31343036 31303135 5a305131 13301106 0a099226
8993f22c 64011916 03636f6d 31153013 060a0992 268993f2
2c640119 16056369 73636f31 15301306 0a099226 8993f22c
64011916 05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00ea8fee c7ae56fc a22e603d 0521b333
3dec0ad4 7d4c2316 3b1eea33 c9a6883d 28ece906 02902f9a
d1eb2b8d f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
a1e906ec 88b32a19 38e5353e 6c0032e8 8c003fa6 2fd22a4d
b9dda2c2 5fcbb621 876bd678 c8a37109 f074eabe 2b1fac59
a78d0a3b 35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4
9b8d3c09 351bc630 05f69357 833b9197 f875b408 cb71a814
69a1f331 b1eb2b35 0c469443 1455c210 db308bf0 a9805758
a878b82d 38c71426 afffd272 dd6d7564 1cbe4d95 b81c02b2
9b56ec2d 5a913a9f 9b95cafd dfffcf67 94b97ac7 63249009
fa05ca4d 6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b
5f020301 0001a382 016f3082 016b3013 06092b06 01040182
37140204 061e0400 43004130 0b060355 1d0f0404 03020186
300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e
04160414 d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb 3081f830 81f5a081 f2a081ef
8681b56c 6461703a 2f2f2f43 4e3d4341 312c434e 3d54532d
57324b33 2d414353 2c434e3d 4344502c 434e3d50 75626c69
63253230 4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c
44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d
3f636572 74696669 63617465 5265766f 63617469 6f6e4c69
73743f62 6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50 6f696e74 86356874 74703a2f
2f74732d 77326b33 2d616373 2e747377 65622e63 6973636f
2e636f6d 2f436572 74456e72 6f6c6c2f 4341312e 63726c30
1006092b 06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101 001abc5a 40b32112 22da80fb
bb228bfe 4bf8a515 df8fc3a0 4e0c89c6 d725e2ab 2fa67ce8
9196d516 dfe55627 953aea47 2e871289 6b754e9c 1e01d408
3f7f0595 8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b ab8e7f84 a011336b 37c13261
5ad218a3 a513e382 e4bfb2b4 9bf0d7d1 99865cc4 94e5547c
f03e3d3e 3b766011 e94a3657 6cc35b92 860152d4 f06b2b15
df306433 c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d aa2ef1c2 edba288f 3a678ecb
3809d0df b1699c76 13018f9f 5e3dce95 efe6da93 f4cb3b00
102efa94 48a22fc4 7e342031 2406165e 39edc207 eddc6554
3fa9f396 ad quit crypto isakmp enable outside crypto isakmp
policy 65535 authentication rsa-sig encryption 3des hash md5
group 2 lifetime 86400 crypto isakmp identity auto tunnel-
group DefaultRAGroup general-attributes address-pool vpnpool
default-group-policy Defaultgroup tunnel-group DefaultRAGroup
ipsec-attributes trust-point CA1 telnet timeout 5 ssh timeout
5 console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512 policy-
map global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras
```

```
inspect netbios inspect rsh inspect rtsp inspect skinny
inspect esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp ! service-policy global_policy
global prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0 : end
CiscoASA#
```

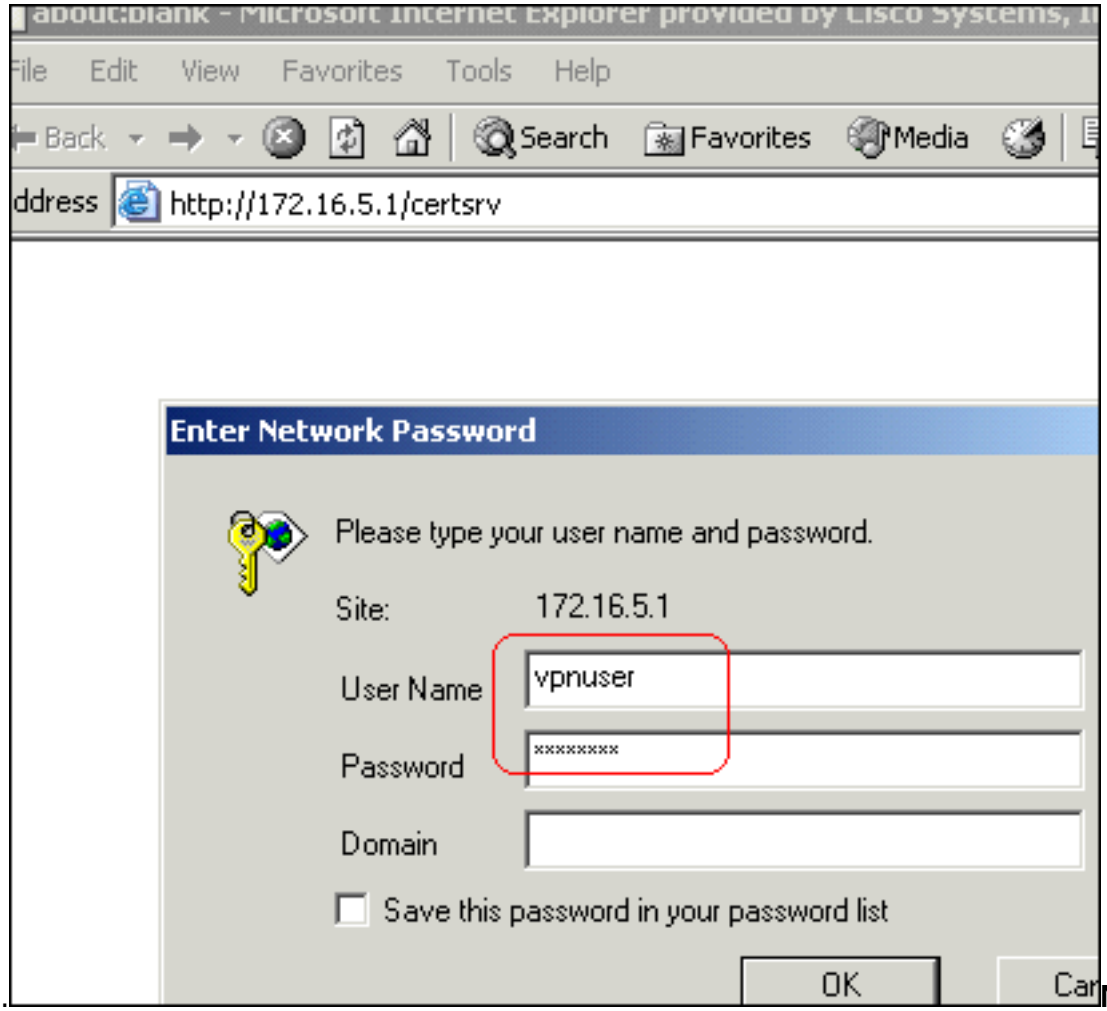
VPN Client Configuration

Complete these steps in order to configure the VPN client:

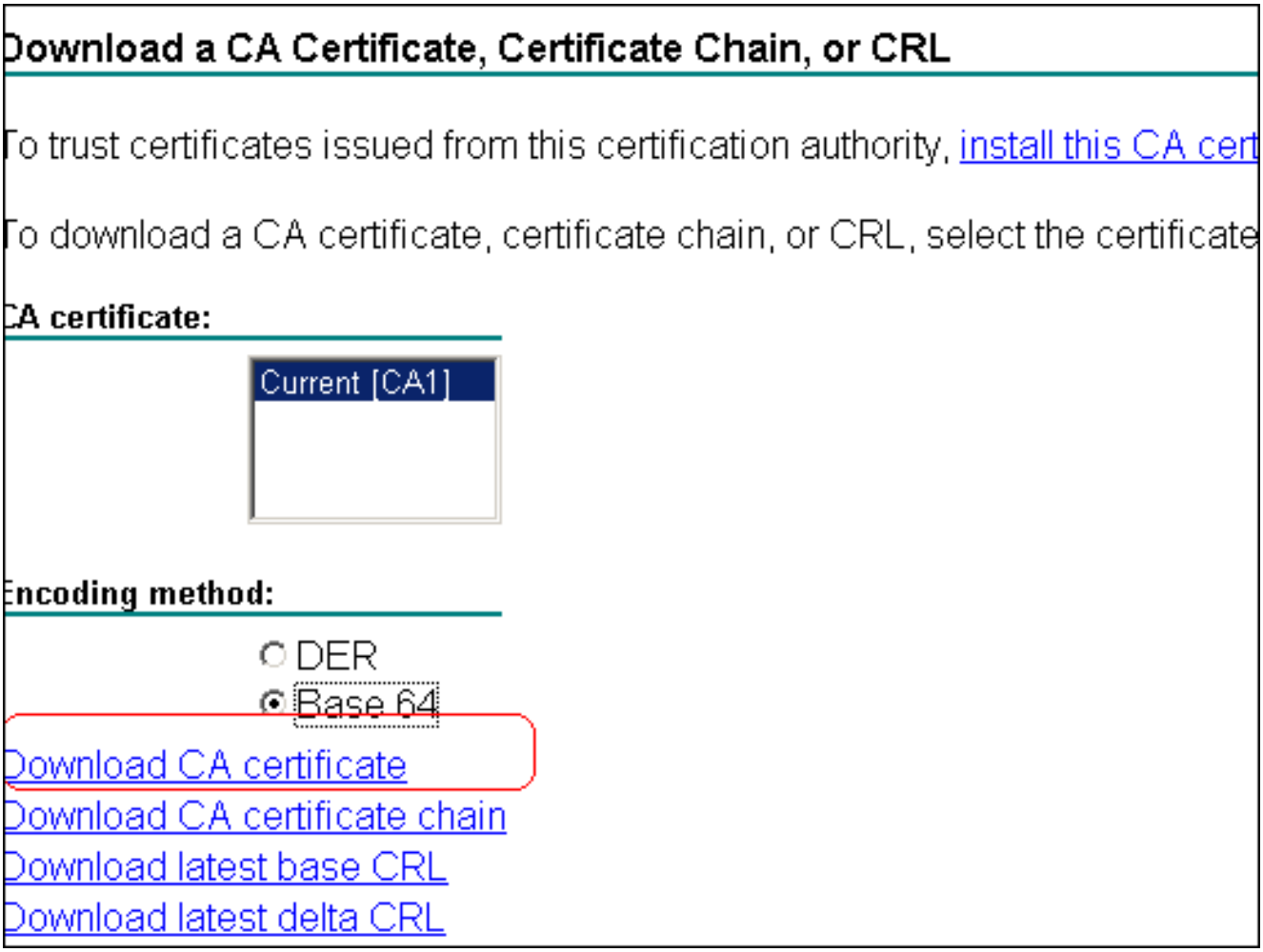
1. Select **Start > Programs > Cisco Systems VPN Client > VPN Client** in order to launch the VPN client
   software.



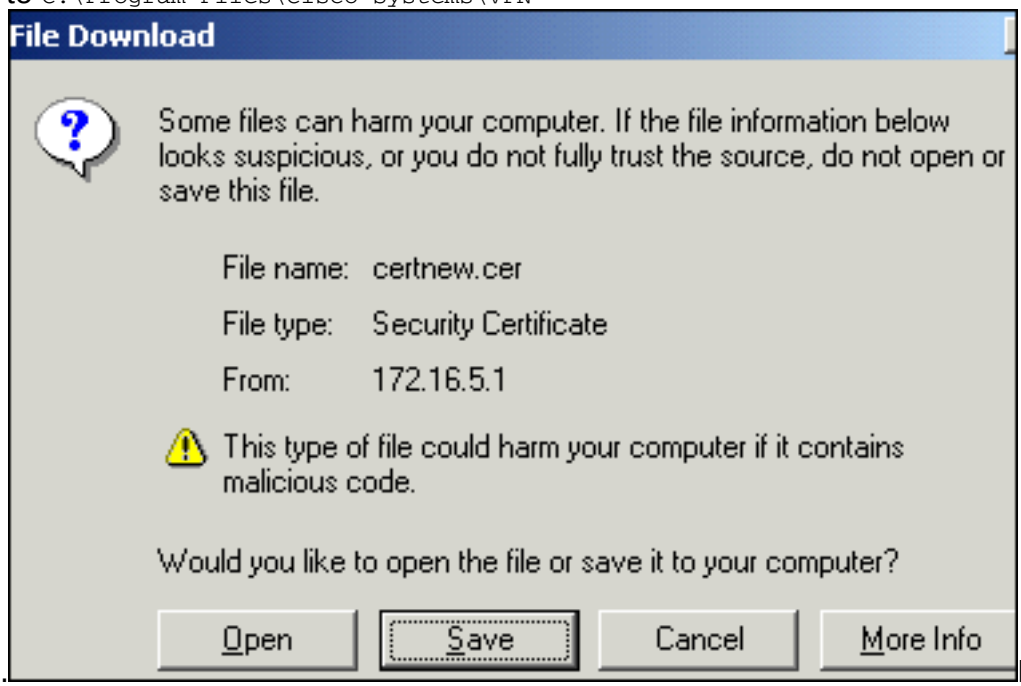
2. Complete these steps in order to download the CA certificate from the CA server named **CA1** and install it into Cisco VPN Client:Log in to the CA server 172.16.5.1 with the user credantials supplied to the



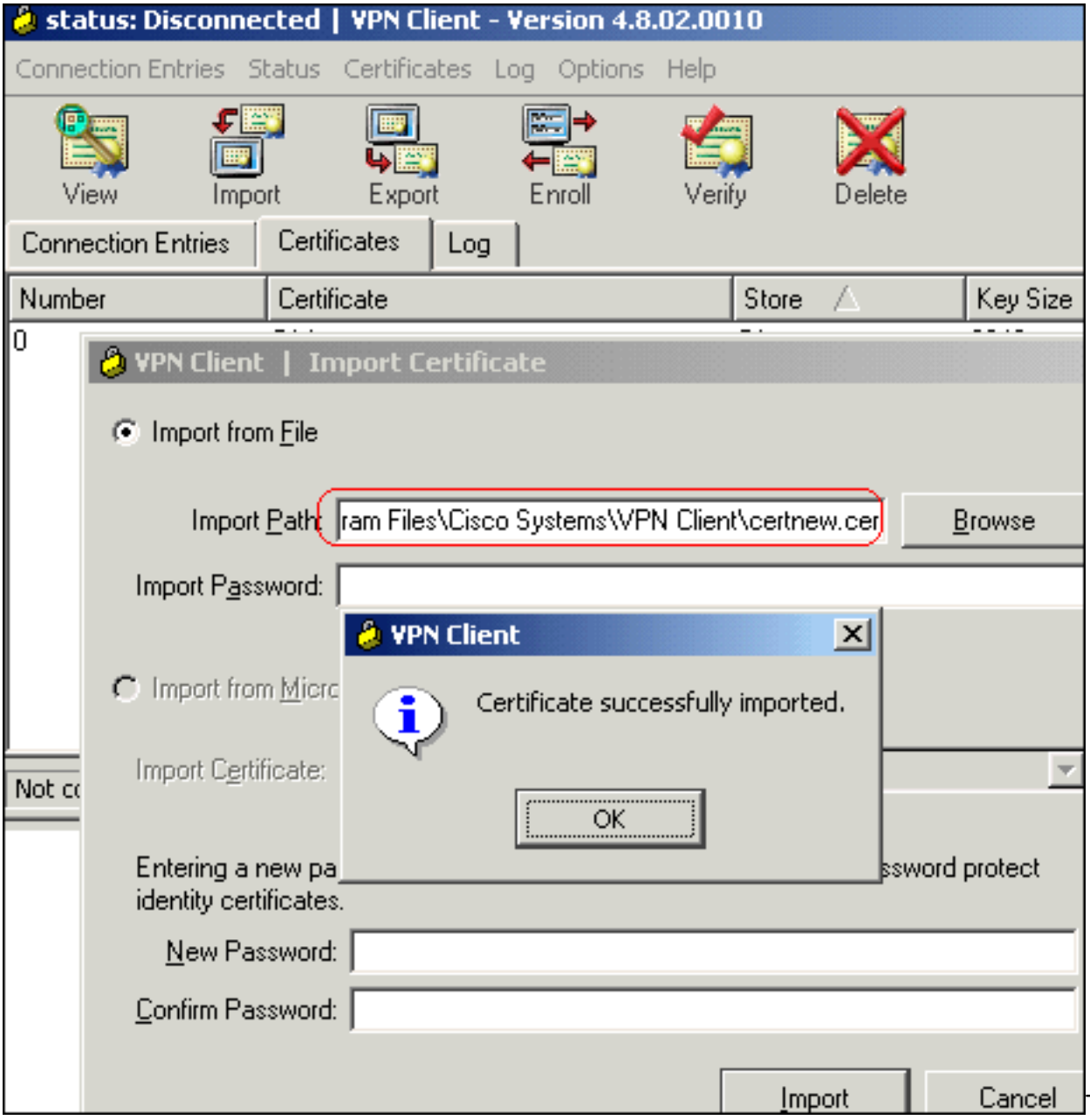
vpnuser.**Note:** Make sure you have a user account for the VPN client user with the CA server.Click **Download a CA certificate, certificate chain or CRL** , and then select the **Base 64** radio button in order to specify the encoding method.Click the **Download CA certificate**.



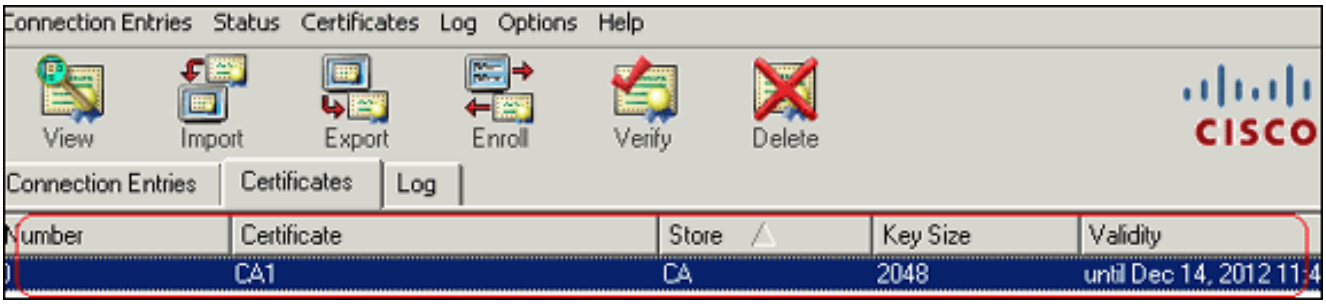
Save the CA certificate to your computer with the name **certnew.cer**. By default, the file saves to `C:\Program Files\Cisco Systems\VPN Client`.



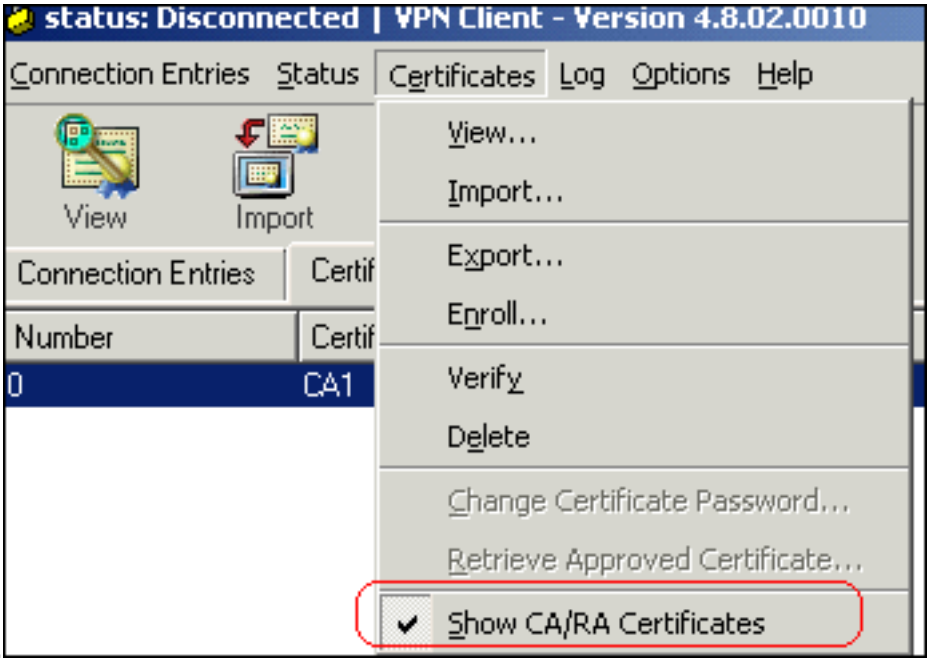
In the VPN client, click the **Certificates** tab, and then choose **Import**.Click the **Import from File** radio button, and then click **Browse** in order to import the CA certificate from the stored location `C:\Program Files\Cisco Systems\VPN Client`.Click **Import**.A dialog box appears that states the certificate was successfully
imported.



The CA Certificates CA1 appears in the Certificates tab.

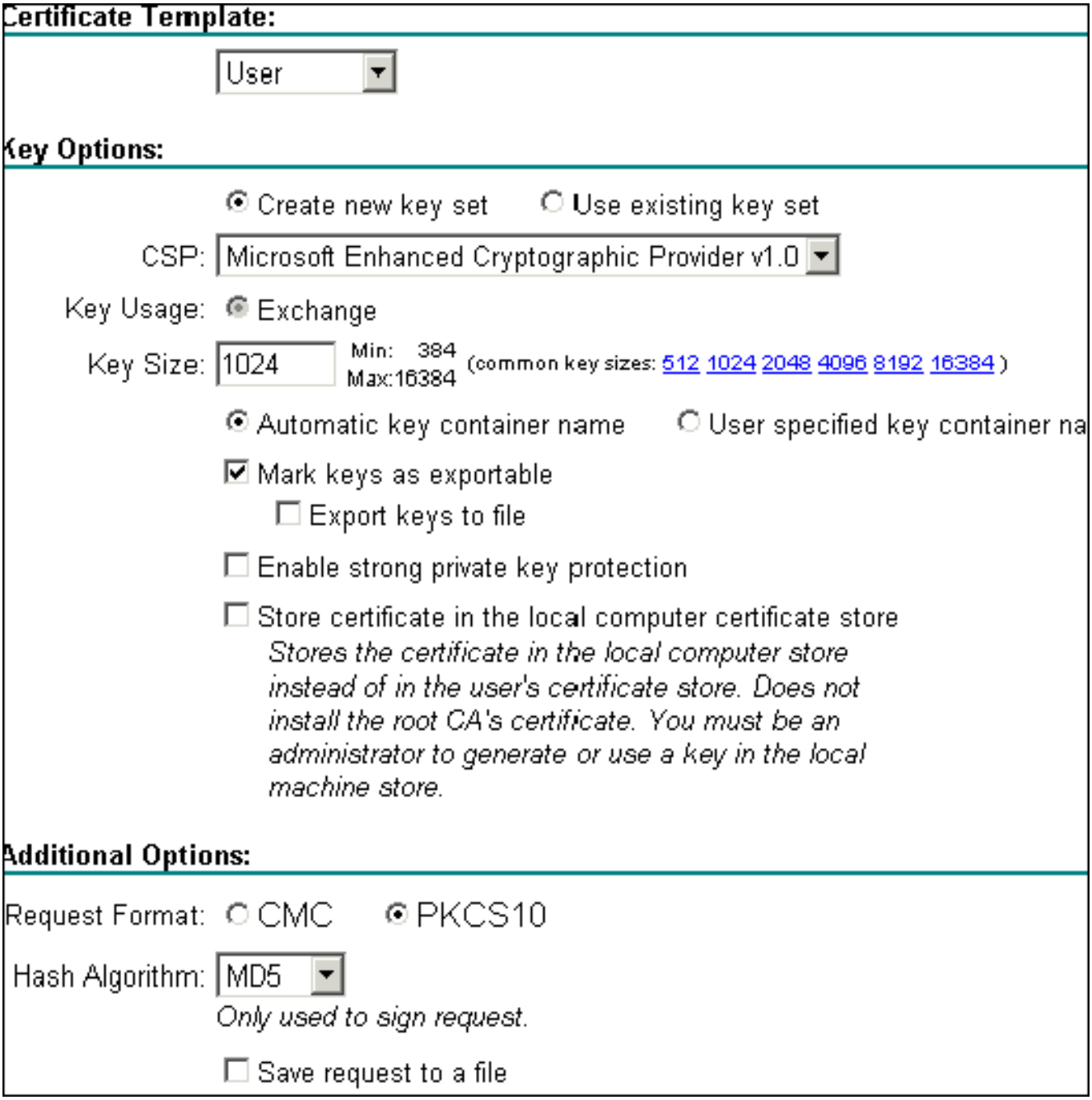


Note: Make sure the **Show CA/RA Certificates** option is selected; otherwise, the CA certificates will not appear in the certificate

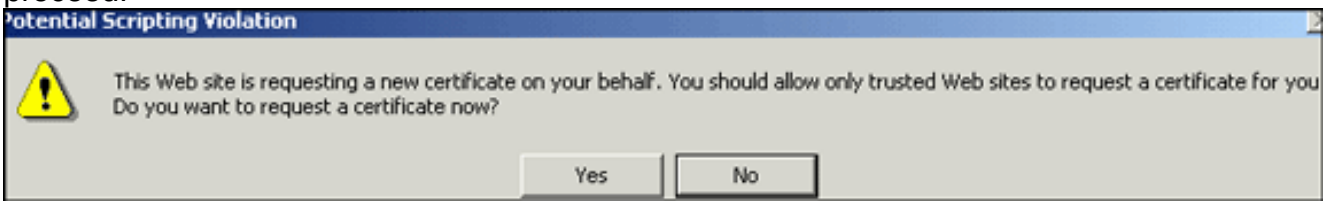


window.

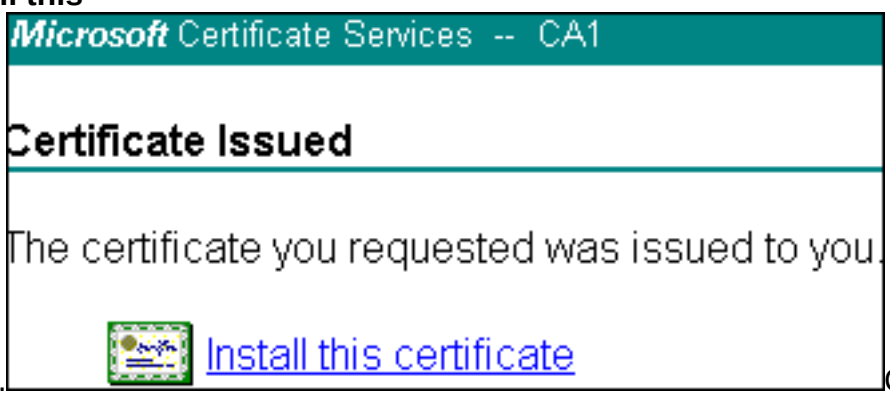
3. Complete these steps in order to download the identity certificate and install it into the VPN client:In the CA server CA1, choose **Request a Certificate > advanced certificate request > Create and submit a request to this CA** in order to enroll for the identity certificate.Click **Submit**.



Click **Yes** to proceed.

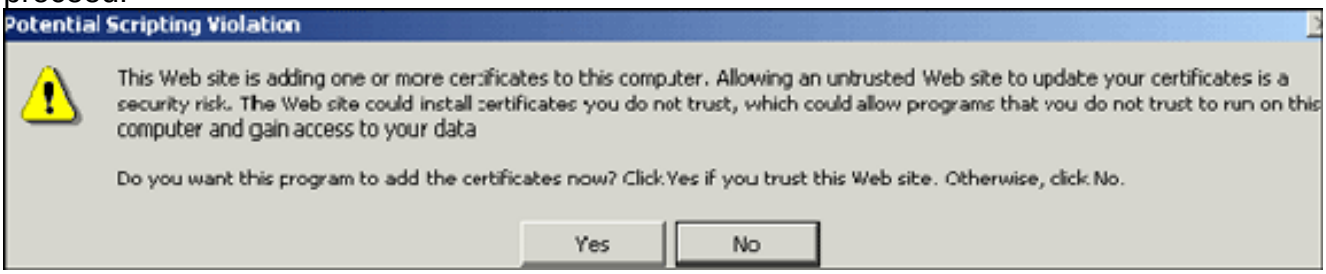


Click **Install this certificate**.

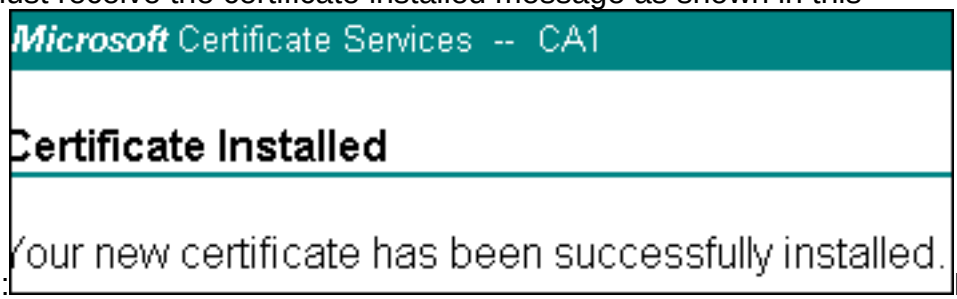


Click **Yes** to

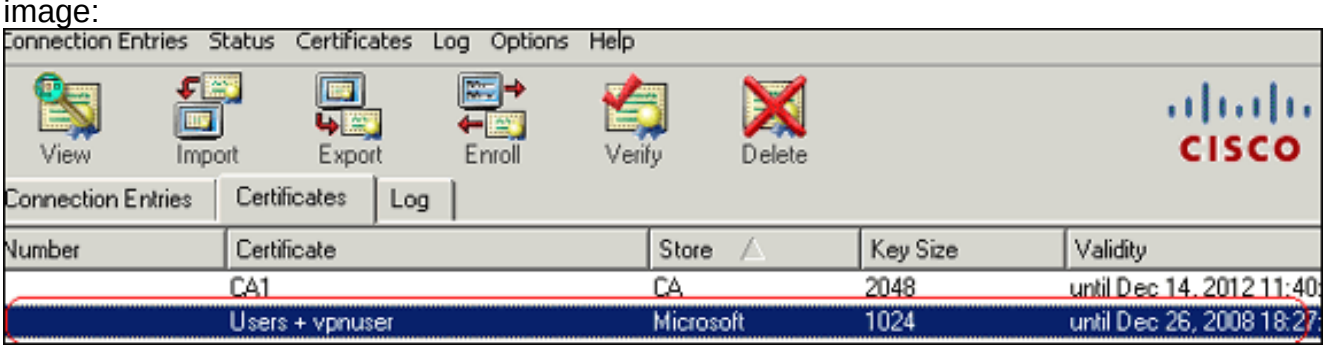
proceed.



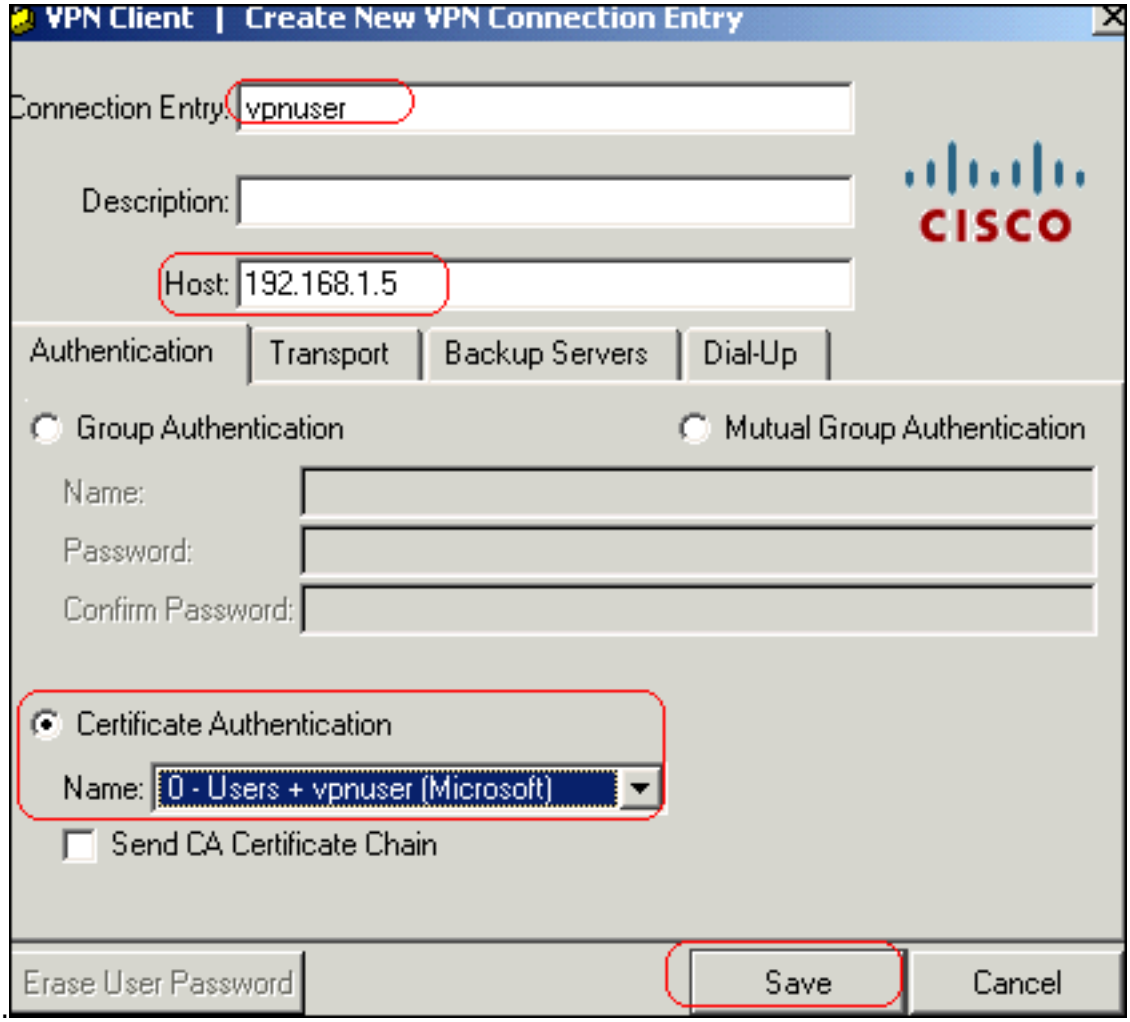
You must receive the certificate installed message as shown in this image:



Exit and then relaunch the VPN client in order to allow the installed identity certificate to appear in the Certificates tab of the VPN client as shown in this image:

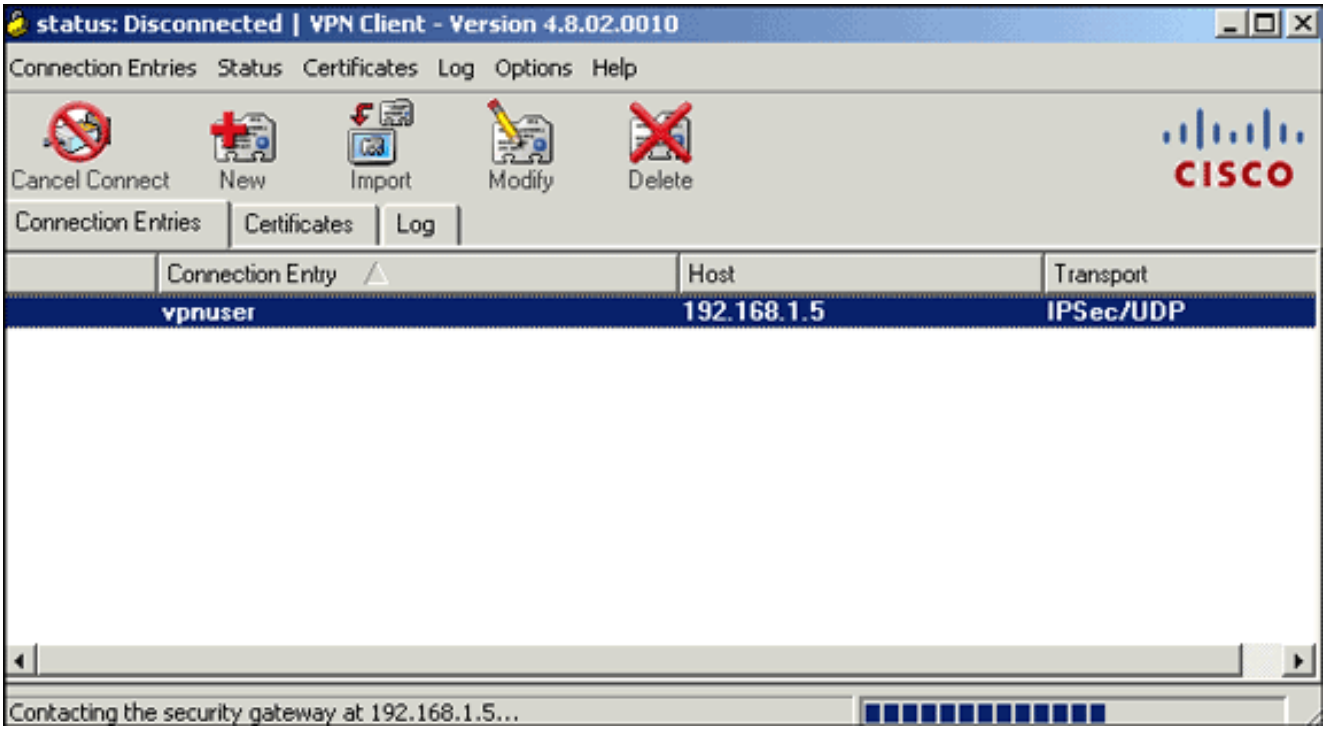


4. Complete these steps in order to create a connection entry (*vpnuser*):Click the Connection Entries tab, and then click **New**.Enter the remote peer IP address (routable) in the Host field.Select the **Certificate Authentication** radio button, and choose the identity certificate from the drop-down list.Click

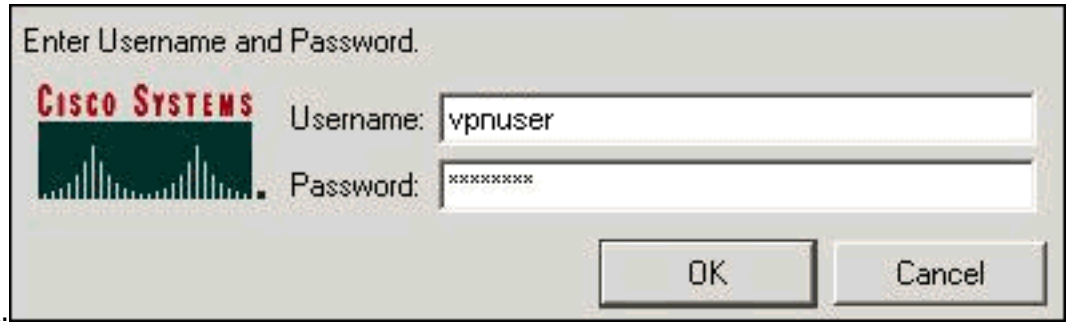


Save.

5. Click **Connect**.



6. When prompted, enter the user name and password information for xauth, and click **OK** in order to connect to the remote

network. 

7. The VPN Client connects with the ASA as shown in this image: 

Verify

On the ASA you can use several show commands at the command line in order to verify the status of a certificate.

Use this section to confirm that your configuration works properly.

- **show crypto ca trustpoint**—Displays configured trustpoints.`CiscoASA#`**`show crypto ca trustpoints`** `Trustpoint CA1: Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com Serial Number: 7099f1994764e09c4651da80a16b749c Certificate configured.`
- **show crypto ca certificate**—Displays all the certificates installed on the system.`CiscoASA#`**`show crypto ca certificates`** `Certificate Status: Available Certificate Serial Number: 3f14b70b00000000001f Certificate Usage: Encryption Public Key Type: RSA (1024 bits) Issuer Name: cn=CA1 dc=TSWeb dc=cisco dc=com Subject Name: cn=vpnserver cn=Users dc=TSWeb dc=cisco dc=com PrincipalName: vpnserver@TSWeb.cisco.com CRL Distribution Points: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services, CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl Validity Date: start date: 14:00:36 UTC Dec 27 2007 end date: 14:00:36 UTC Dec 26 2008 Associated Trustpoints: CA1 CA Certificate Status: Available Certificate Serial Number: 7099f1994764e09c4651da80a16b749c Certificate Usage: Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=CA1 dc=TSWeb dc=cisco dc=com Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com CRL Distribution Points: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services, CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl Validity Date: start date: 06:01:43 UTC Dec 14 2007 end date: 06:10:15 UTC Dec 14 2012 Associated Trustpoints: CA1`
- **show crypto ca crls**—Displays cached certificate revocation lists (CRL).
- **show crypto key mypubkey rsa**—Displays all generated crypto key pairs.`CiscoASA#`**`show crypto key mypubkey rsa`** `Key pair was generated at: 01:43:45 UTC Dec 11 2007 Key name: <Default-RSA-Key> Usage: General Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509 99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541 f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b 4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68 2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001 Key pair was generated at: 06:36:00 UTC Dec 15 2007 Key name: my.CA.key Usage: General Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905 5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2 d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001 Key pair was generated at: 07:35:18 UTC Dec 21 2007 CiscoASA#`
- **show crypto isakmp sa**—Displays the IKE 1 tunnel information.`CiscoASA#`**`show crypto isakmp sa`** `Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.1.1.5 Type : user Role : responder Rekey : no State : MM_ACTIVE`

- **show crypto ipsec sa**—Dislays the IPSec tunnel information.
```
CiscoASA#show crypto ipsec sa
interface: outside Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5 local ident
(addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port):
(10.5.5.10/255.255.255.255/0/0) current_peer: 10.1.1.5, username: vpnuser dynamic allocated peer ip:
10.5.5.10 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 144, #pkts decrypt: 144,
#pkts verify: 144 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp
failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created:
0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv
errors: 0 local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5 path mtu 1500, ipsec
overhead 58, media mtu 1500 current outbound spi: FF3EEE7D inbound esp sas: spi: 0xEFDF8BA9
(4024404905) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id:
4096, crypto-map: dynmap sa timing: remaining key lifetime (sec): 28314 IV size: 8 bytes replay
detection support: Y outbound esp sas: spi: 0xFF3EEE7D (4282314365) transform: esp-3des esp-md5-hmac
none in use settings ={RA, Tunnel, } slot: 0, conn_id: 4096, crypto-map: dynmap sa timing: remaining
key lifetime (sec): 28314 IV size: 8 bytes replay detection support: Y
```

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

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

Here are some possible errors that you might encounter:

- **ERROR: Failed to parse or verify imported certificate**This error can occur when you install the identity certificate and do not have the correct intermediate or root CA certificate authenticated with the associated trustpoint. You must remove and reauthenticate with the correct intermediate or root CA certificate. Contact your 3rd party vendor in order to verify that you received the correct CA certificate.
- **Certificate does not contain general purpose public key**This error can occur when you attempt to install your identity certificate to the wrong Trustpoint. You attempt to install an invalid identity certificate, or the key pair associated with the Trustpoint does not match the public key contained in the identity certificate. Use the **show crypto ca certificates trustpointname** command in order to verify you installed your identity certificate to the correct trustpoint. Look for the line stating **Associated Trustpoints**. If the wrong trustpoint is listed, use the procedures described in this document in order to remove and reinstall the appropriate trustpoint. Also, verify the key pair has not changed since the CSR was generated.
- **ERROR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:**You might receive this error in the VPN client if a problem occurs with the certificates during authentication. In order to resolve this issue, use the **crypto isakmp identity auto** command in the ASA/PIX configuration.

Related Information

- **Cisco Adaptive Security Appliance Support page**
- **Cisco VPN Client Support Page**
- **Cisco PIX 500 Series Security Appliances**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**

- Requests for Comments (RFCs)
- Technical Support & Documentation - Cisco Systems