Avaya Solution & Interoperability Test Lab

Configuring Avaya 9600 Series IP Telephone VPN feature for Certificate Authentication using Cisco 5510 Adaptive Security Appliance and Microsoft Certificate Authority with Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describes the configuration steps required to configure the Avaya 9600 IP Telephone VPN feature for Certificate Authentication using Cisco 5510 Adaptive Appliance and Microsoft Certificate Authority with Avaya Aura™ Communication Manager running on Avaya Aura™ Midsize Enterprise Single Server. The Application Notes identifies how to generate digital certificates using the Microsoft Certificate Authority and download these certificates to the Avaya 9600 Series IP Telephone and to administer the Cisco Adaptive Security Appliance to establish and terminate an IPSec VPN tunnel request from the Avaya 9600 Series VPN enabled IP Telephone.

The validation test of the sample configuration was conducted at the Avaya Solution and Interoperability Test Lab at the request of the Avaya Solutions and Marketing Team.

1. Introduction

The Microsoft Certificate Authority can issue multiple certificates in the form of a tree structure. A root certificate is the top most certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. A signature by a root certificate is somewhat analogous to notarizing an identity in the physical world. Certificates further down the tree also depend on the trustworthiness of the intermediates often known as subordinate certification authorities. Many software applications assume these root certificates are trustworthy on the user's behalf.

The 9600 Series IP Telephones support Media Encryption SRTP and use built in Avaya certificates for trust management. Trust management involves downloading certificates for additional trusted Certificate Authorities (CA) and the policy management of those CAs. Identity management is handled by Simple Certificate Enrollment Protocol (SCEP) with phone certificates and private keys. Simple Certificate Enrollment Process applies to the VPN operation or to standard enterprise network operation. The Simple Certificate Enrollment Protocol is the protocol used by the Microsoft CA to securely transport key information and digital certificates to network devices, such as the Avaya 9600 IP telephone and Cisco Adaptive Security Appliance. For the Microsoft CA to support SCEP, the Microsoft SCEP add-on for Certificate Services has been installed. Information on how to obtain and install the SCEP add-on is included in the **Section 3** of these Application Notes.

1.1. Interoperability Compliance Testing

The objective of this interoperability test is to verify that the Avaya 9600 IP telephone can provide VPN functionality with Certificate Authentication using Cisco Adaptive Security Appliance and Microsoft Certificate Authority with Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ SIP Enablement Services 5.2 running on Avaya Aura™ Midsize Enterprise Single Server. Testing was carried out on codec support and negotiation supported by Avaya 9600 IP telephones and as well as supplementary features such as Call Hold, Forward, Transfer and Conference between the Avaya IP and SIP endpoints.

1.2. Configuration

The configuration used in these Application Notes is shown in **Figure 1**. The Avaya Aura™ Midsize Enterprise software is installed and configured on Avaya Aura™ System Platform on a S8500C Media Server. The Avaya Aura™ Midsize Enterprise Single Server is a template running software applications. These software applications include Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services and Avaya Aura™ Application Enablement Services. The Avaya Aura™ Midsize Enterprise Media Server is connected to an Extreme Summit x250e 24P switch and is configured in a separate vlan. The IP telephones are physically connected to a single Cisco Catalyst 3750E-24P switch and are administered in a single subnet. The 9600 IP telephones register to Avaya Aura™ Communication Manager running on the Avaya Aura™ Midsize Enterprise Single Server and are administered as H.323 stations. Both the Extreme Summit x250e 24P switch and the Cisco Catalyst 3750E-24P switch are connected to an Extreme Summit x450e 48P router. Each of the two switches is configured with an uplink trunk port to connect to the router. The Microsoft Windows 2003 Server Certificate Authority is used to generate the digital certificates used by the 9600 Series IP Telephone and Cisco Adaptive Security Appliance. The Microsoft CA in the sample configuration is used in the enterprise network as a private certificate server for internal use. The Cisco Adaptive Security Appliance is configured for automatic certificate enrollment. The Cisco Adaptive Security Device Manager (ASDM) graphical user interface application is used to configure the Cisco ASA. The Juniper SSG 5 router provides broadband internet connection.

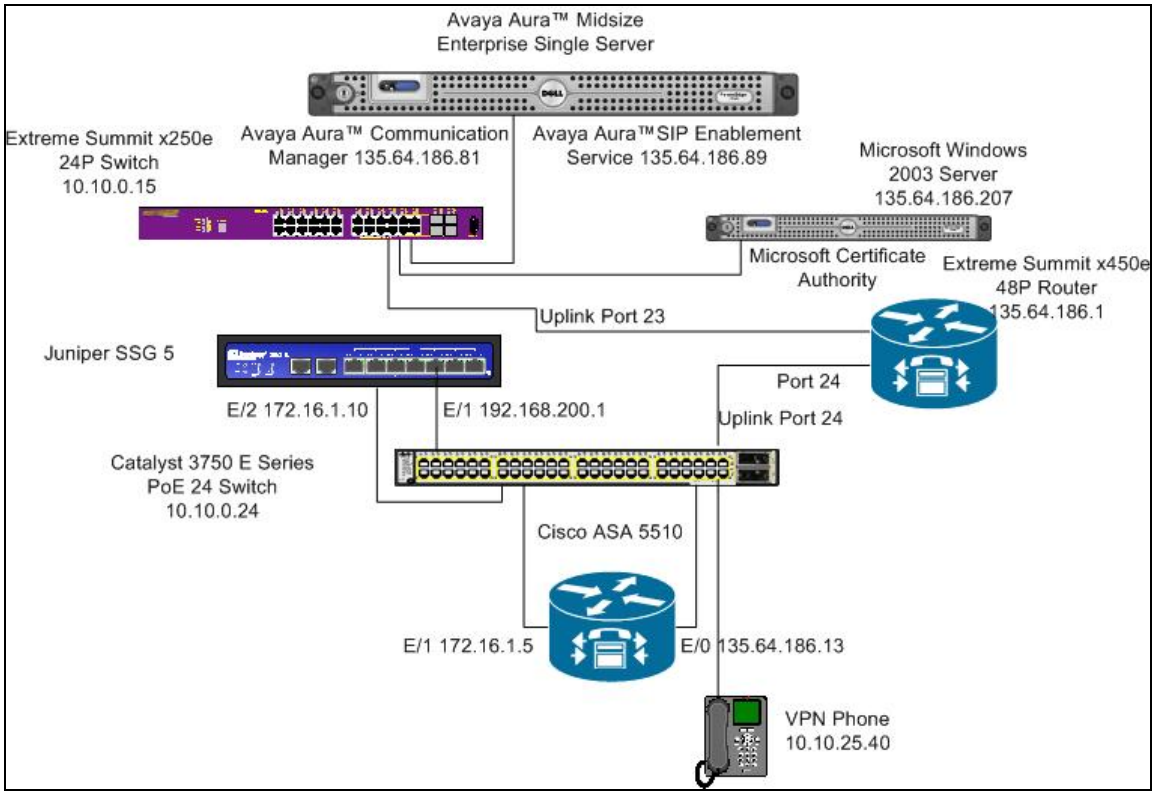


Figure 1: Avaya Aura™ Midsize Enterprise Single Server with Cisco Adaptive Security Appliance

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

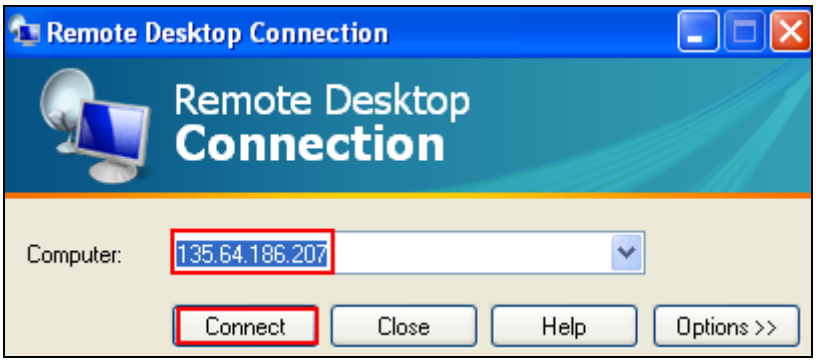
Avaya Aura™	Software
Avaya Aura™ Midsize Enterprise Single Server on a S8500C Media Server	Avaya Aura™ Midsize Enterprise R5.2 Release 5.2.1.2.5 Avaya Aura™ Communication Manager R5.2.1 Release 5.2.1 R15x.02.1.016.4 Update: Service Pack 0 Avaya Aura™ SIP Enablement Services R5.2 Release SES05.2.1.016.4 Update: Service Pack 0 Avaya Aura™ Application Enablement Services R5.2 Release 5.2.0.98 Update: Service Pack 0
Avaya one-X® 9600 Series IP Telephones (H.323)	Release 3.1
Cisco Catalyst 3750 PoE 24P Switch	SW Ver. 12.2(35)SE5
Extreme Summit x250 24P Switch	Release 12.0.3.16
Extreme Summit x450 48P Router	Release 12.0.3.16
Cisco 5510 Adaptive Security Appliance	Release 7.21
Cisco Adaptive Security Device Manager	Release 5.21
Juniper SSG	Release 6.2
Microsoft Windows 2003 Server	Microsoft Windows 2003 Server Version 2003 Update: Service Pack 2

3. Install Simple Certificate Enrollment Protocol

This section describes how to install the Simple Certificate Enrollment Protocol add-on to an existing Microsoft CA. It also describes how to download the digital certificate generated by the Simple Certificate Enrollment Protocol to the 9600 IP telephone. The Simple Certificate Enrollment Protocol is the protocol used by the Microsoft CA to securely transport key information and digital certificates to network devices, such as the Avaya 9600 IP telephone and Cisco Adaptive Security Appliance. The Simple Certificate Enrollment Protocol add-on is available from the Windows Server 2003 Resource Kit or by downloading directly from the Microsoft Download Center at the following URL:
http://www.microsoft.com/downloads/details.aspx?familyid=9f306763-d036-41d8-8860-1636411b2d01&displaylang=en

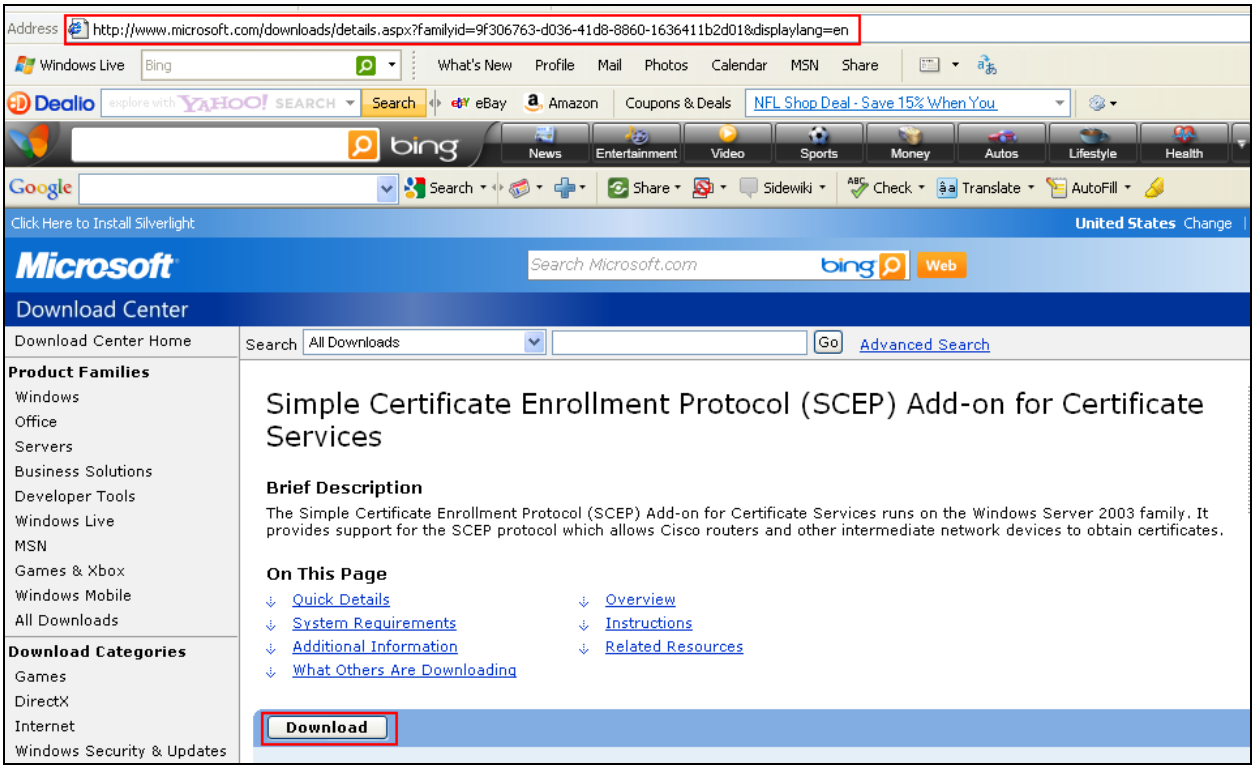
3.1. Access Windows 2003 Server

To access the Windows 2003 Server where the Simple Certificate Enrollment Protocol will be located, open a remote desktop connection and input the IP Address of the Windows 2003 Server. This was **135.64.186.207**. Press **Connect** to access the Widows 2003 Server.

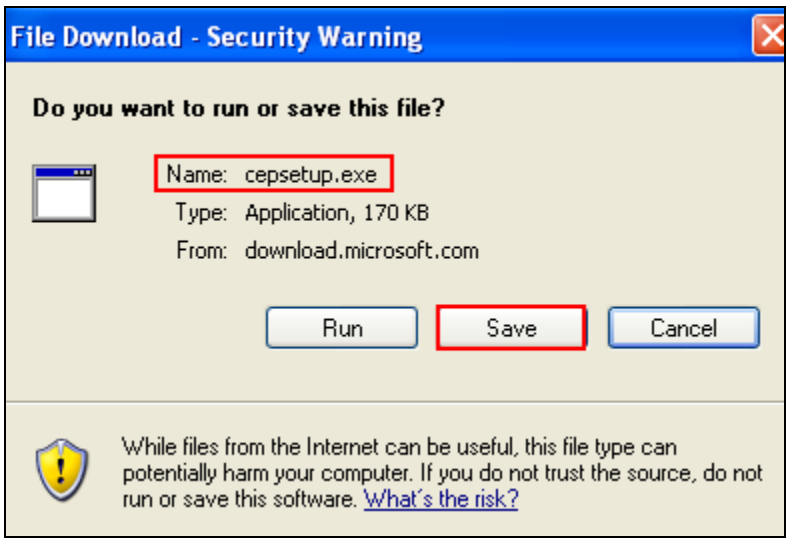


Login with the appropriate credentials.

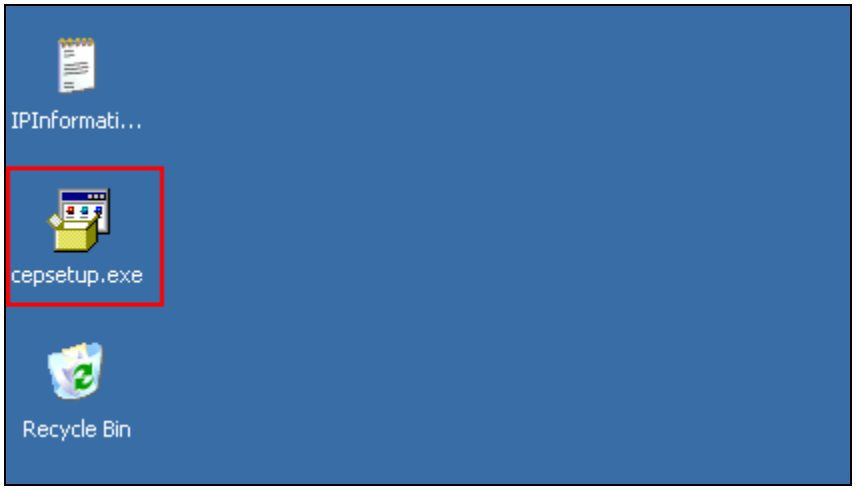
Access the URL **http://www.microsoft.com/downloads/details.aspx?familyid=9f306763-d036-41d8-8860-1636411b2d01&displaylang=en** and download the Simple Certificate Enrollment Protocol add-on for Certificates Services by pressing the **Download** button.



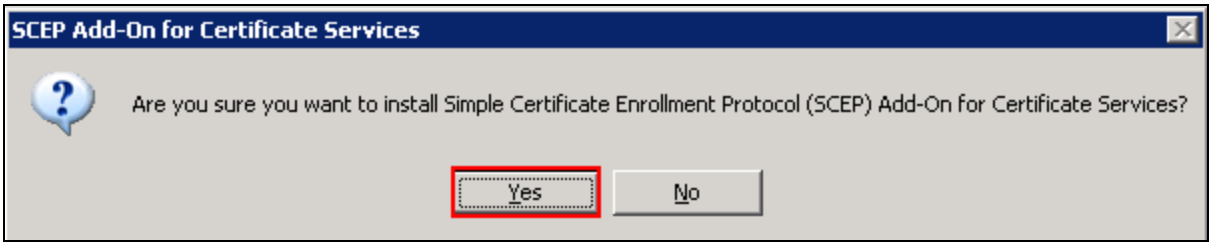
Save the **cepsetup.exe** file to a location on the Windows 2003 Server.



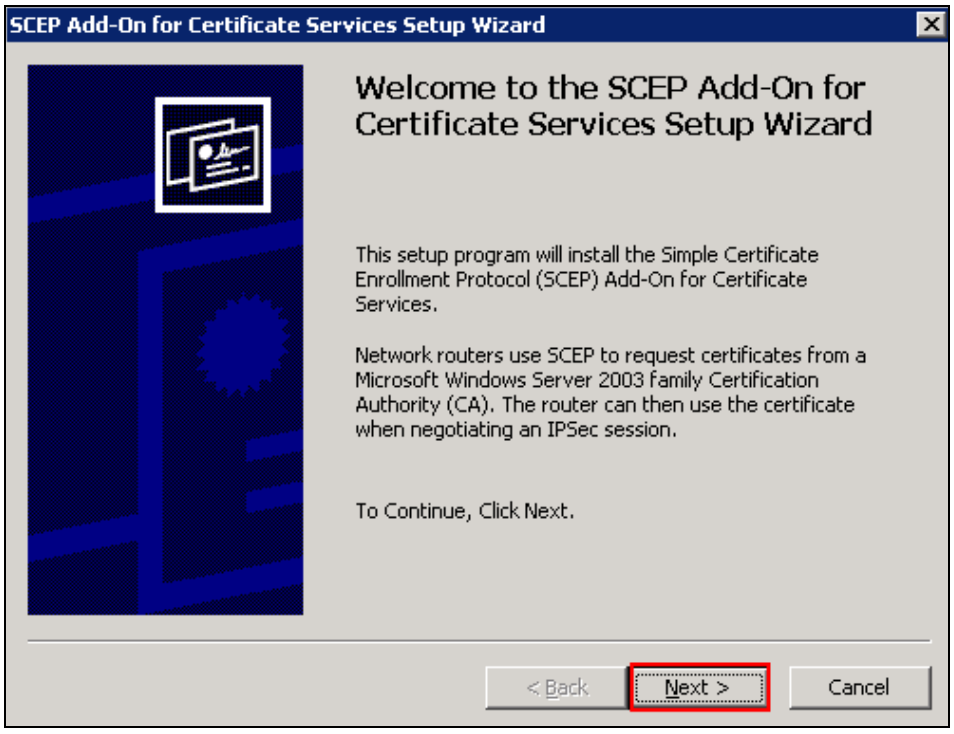
Run the **cepsetup.exe** file



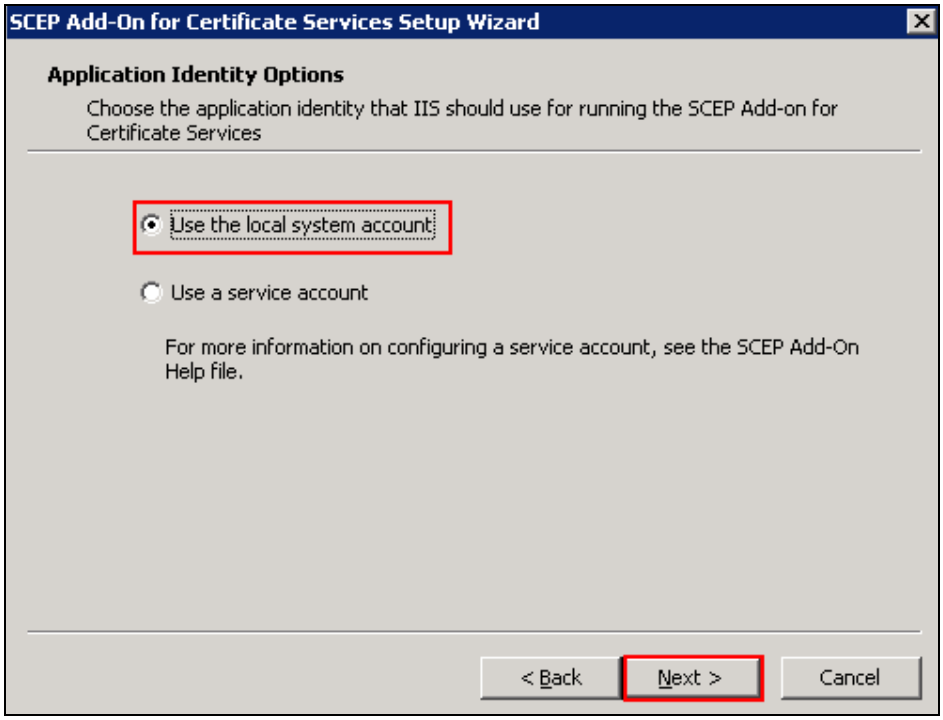
The user is prompted with the following prompt. Press the **YES** button to continue the installation.



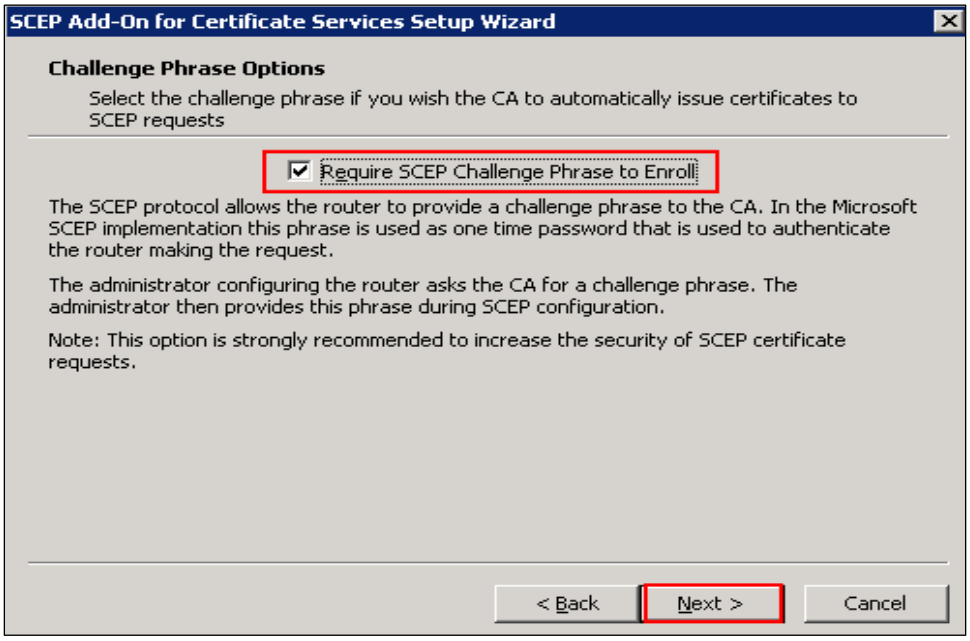
The **Welcome to the SCEP Add-On for Certificates Services Setup Wizard** page is shown in the screenshot below. Press the **Next** button



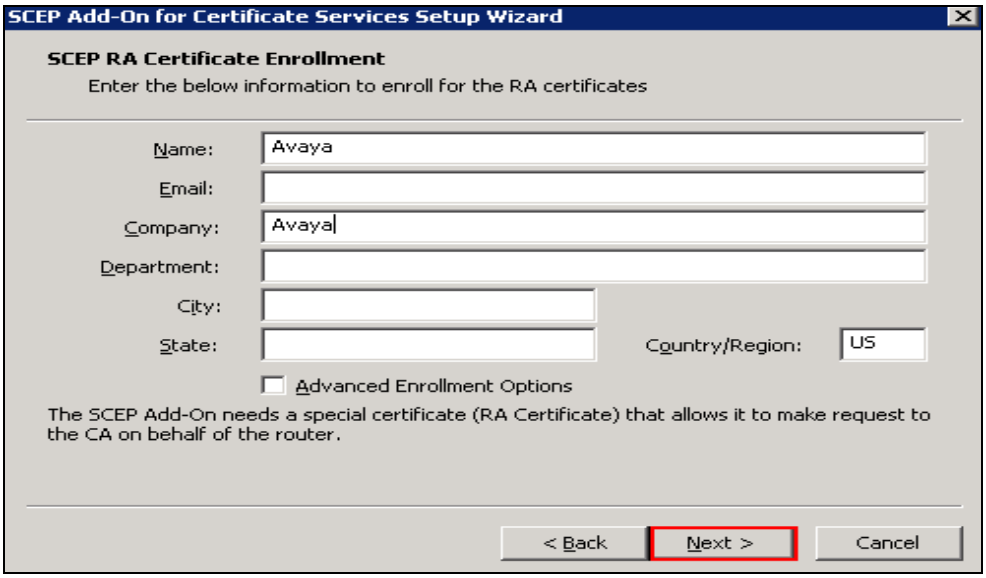
Select **Use the local system account** and press the **Next** button



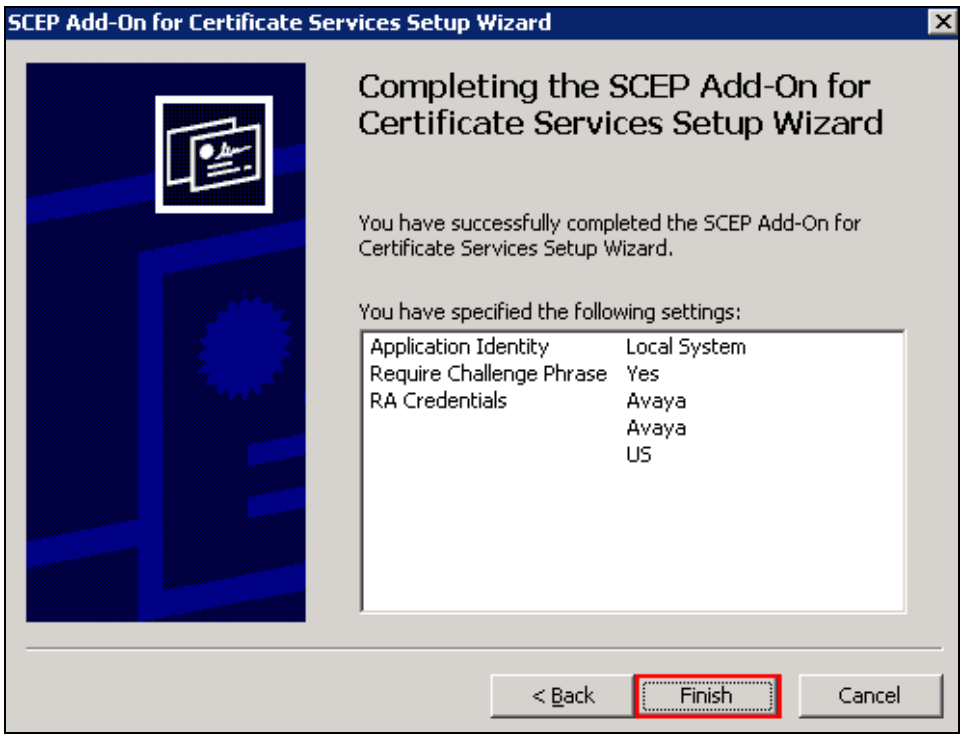
Enable **Require SCEP Challenge Phrase to Enroll** and press the **Next** button. As recommended by Microsoft, the Challenge Phrase option is enabled in the sample configuration.



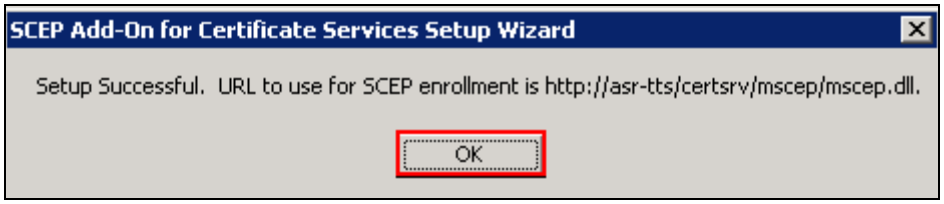
Enter the required information below and press the **Next** button.



Press the **Finish** button.

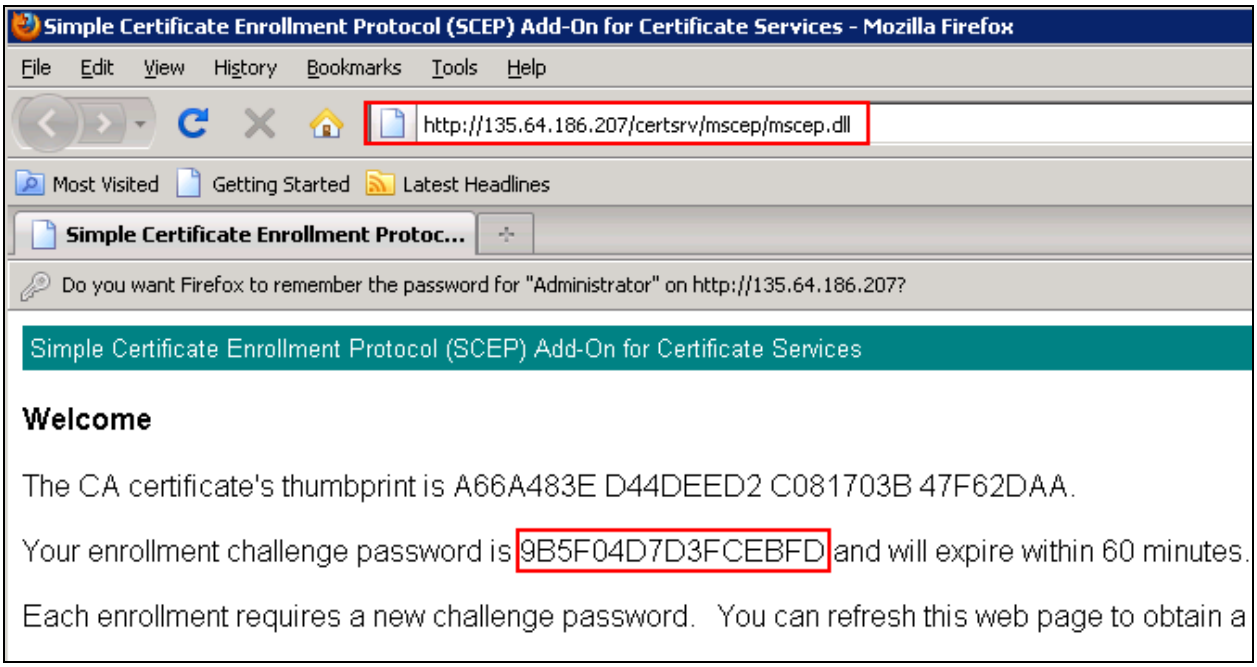


The following prompt is seen. Press the **OK** button.



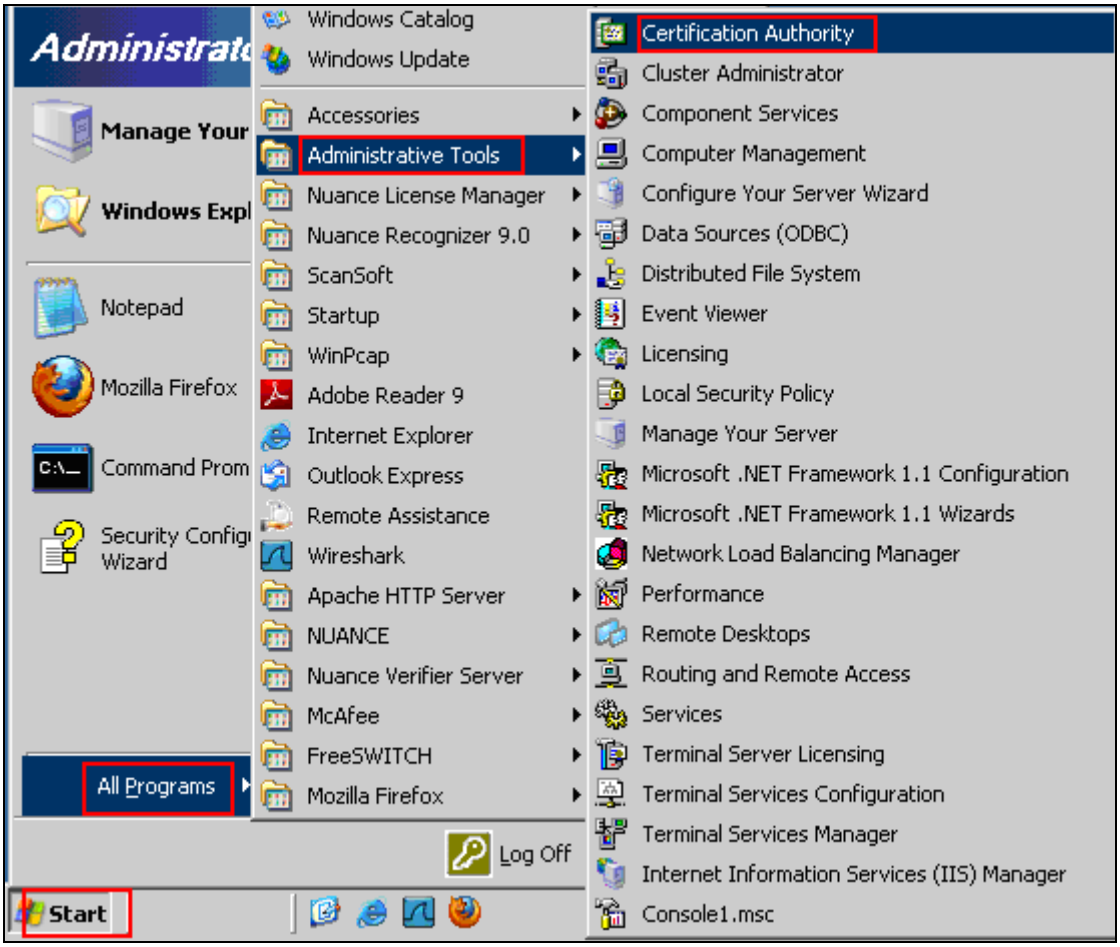
3.2. Generate Simple Certificate Enrollment Prototocol Password

From a web browser, go to the URL **http://135.64.186.207/certsrv/mscep/mscep.dll**, where 135.64.186.207 is the ip address of the Windows 2003 Server where the Simple Certificate Enrollment Protocol is stored. The following page is displayed as shown below. The enrollment challenge password is generated **9B5F04D7D3FCEBFD** in the example below. The password will expire after 60 minutes from the time it was generated and is only able to be used once. The Challenge Phrase is a one time password generated by the Microsoft CA at the request of an administrator. Once the Challenge Phrase is used, it becomes invalid and a new challenge phrase request must be sent to the Microsoft CA to generate a password. This ensures certificates will not be downloaded from the Microsoft CA by unwanted devices. Because the Challenge Phrase is only valid for one time use, a new request must be made for each Avaya 9600 Series IP telephone to import the digital certificate to the phone.

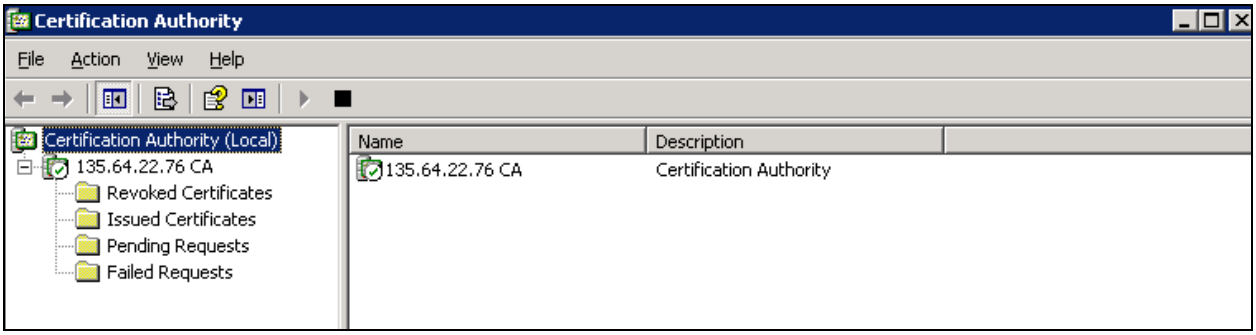


3.3. Export Certificate to .CER file

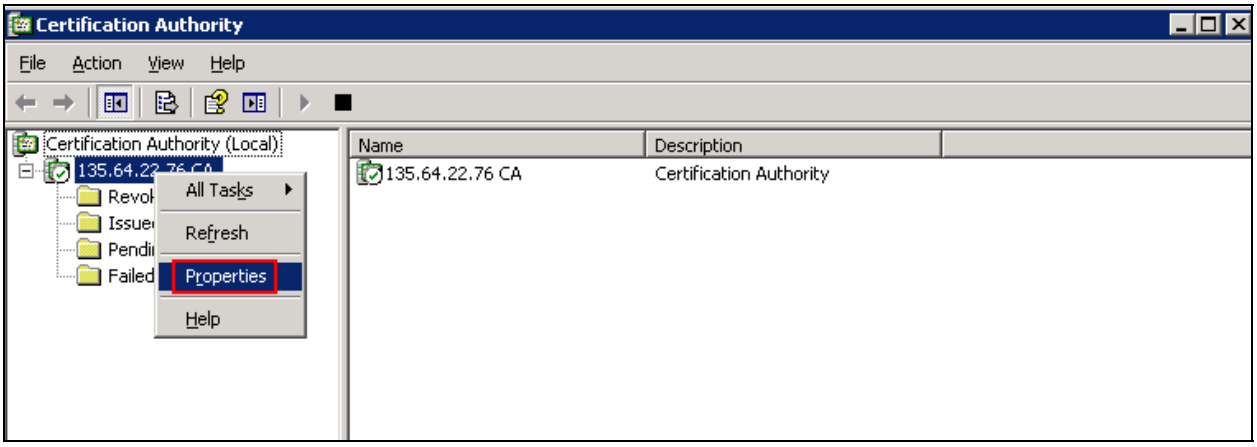
To open the Microsoft Certificate Authority click **Start→All Programs→Admin tools→Certification Authority.** For the Avaya 9600 IP telephone to download the digital certificate, the certificate must first be exported from the Microsoft CA to a file with a .cer extension. Microsoft Windows associates files containing a .cer extension with a file type of Security Certificate. The .cer file is then copied to the upload directory of the HTTP server.



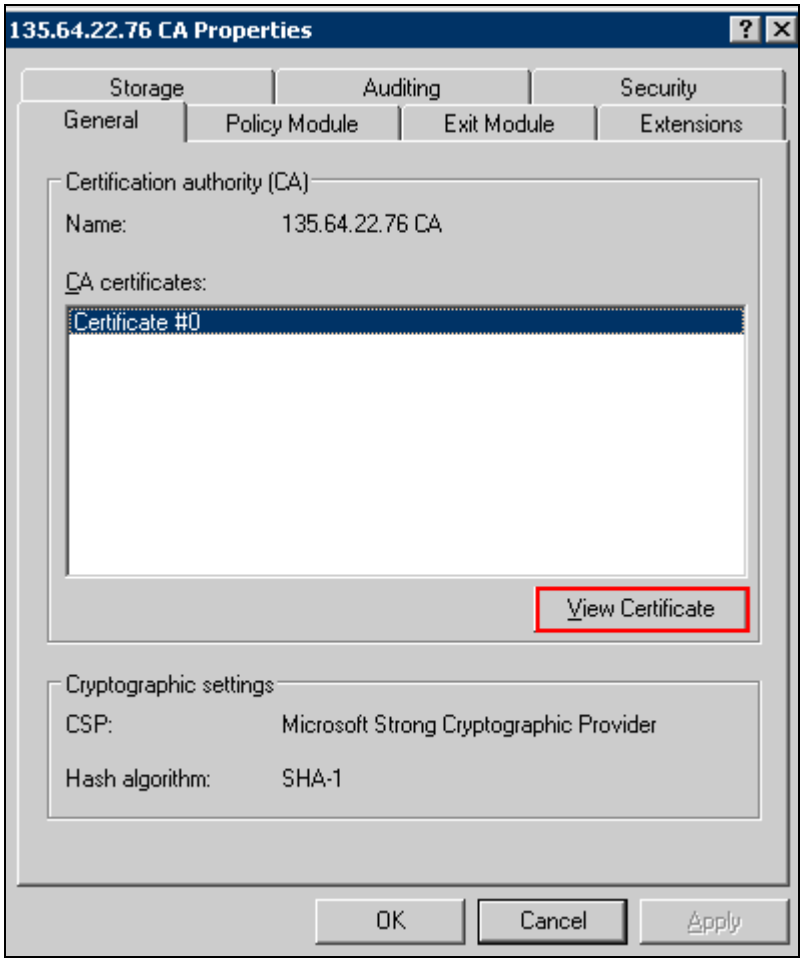
The following screenshot is displayed.



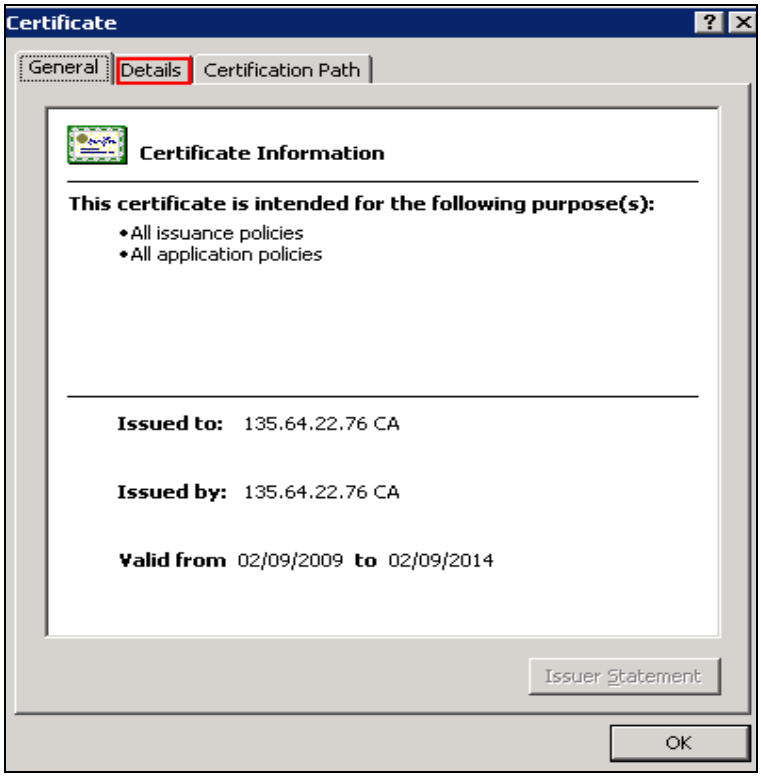
From the Microsoft CA management window right click on the CA name and select **Properties**.



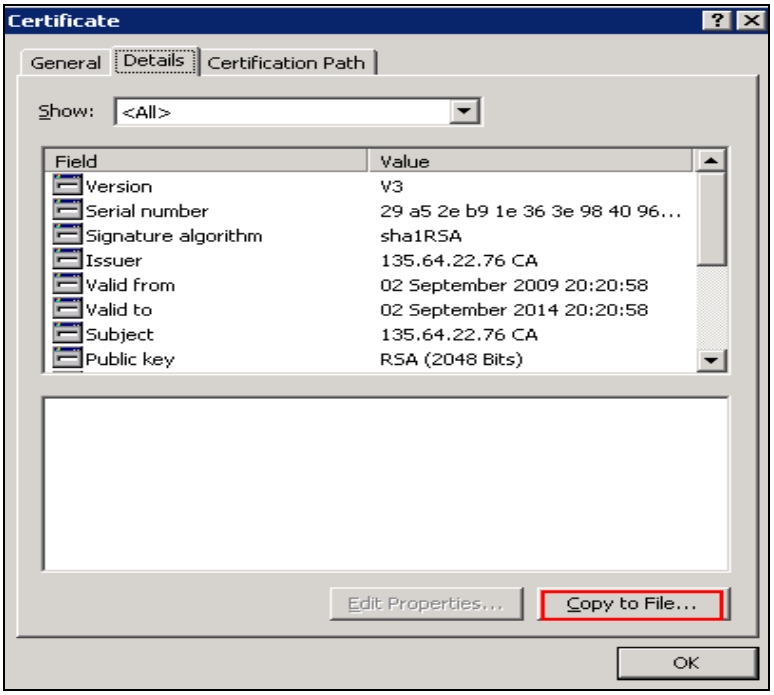
The following screenshot is shown below. Click on the **View Certificate** button.



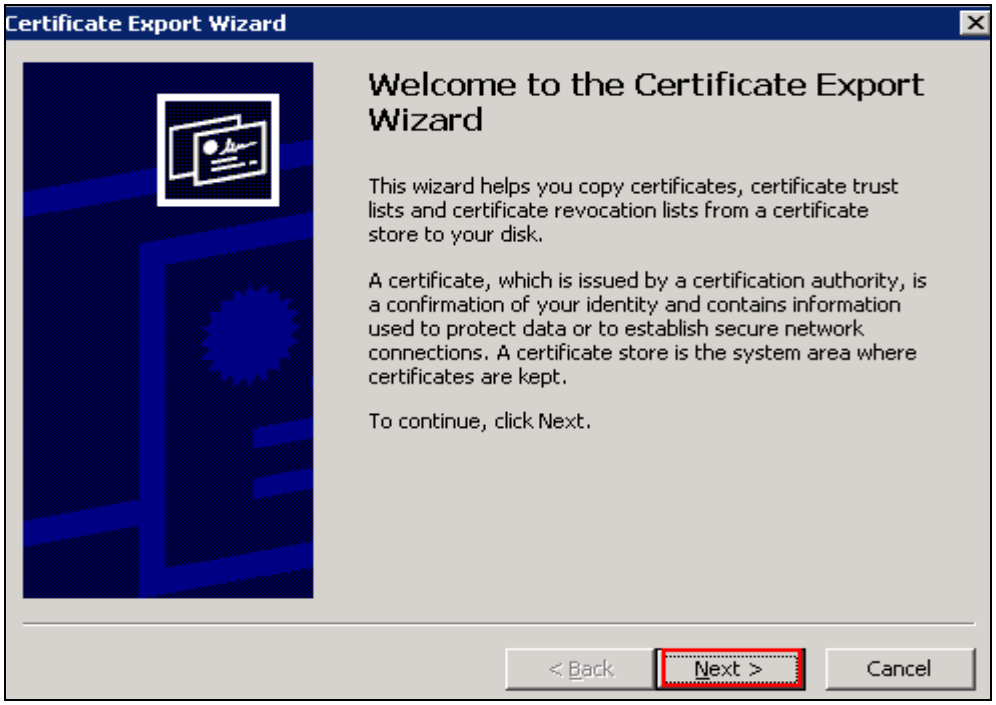
Click on the **Details** tab of the **Certificate** window.



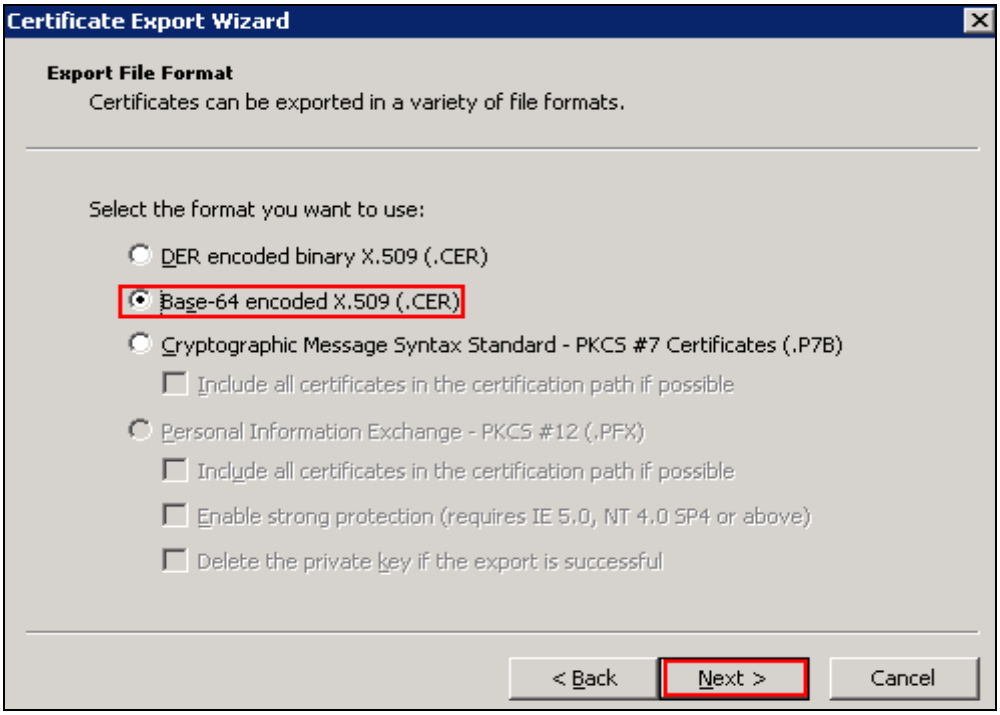
Select **Copy to File**.



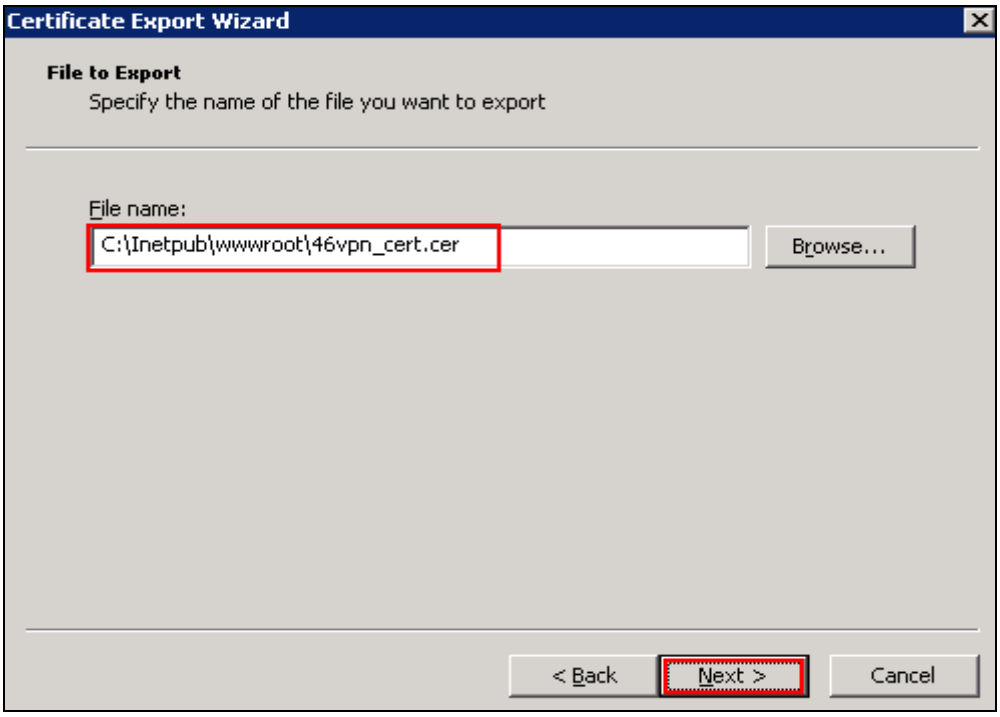
The **Welcome to the Certificate Export Wizard** page is displayed. Click on the **Next** button.



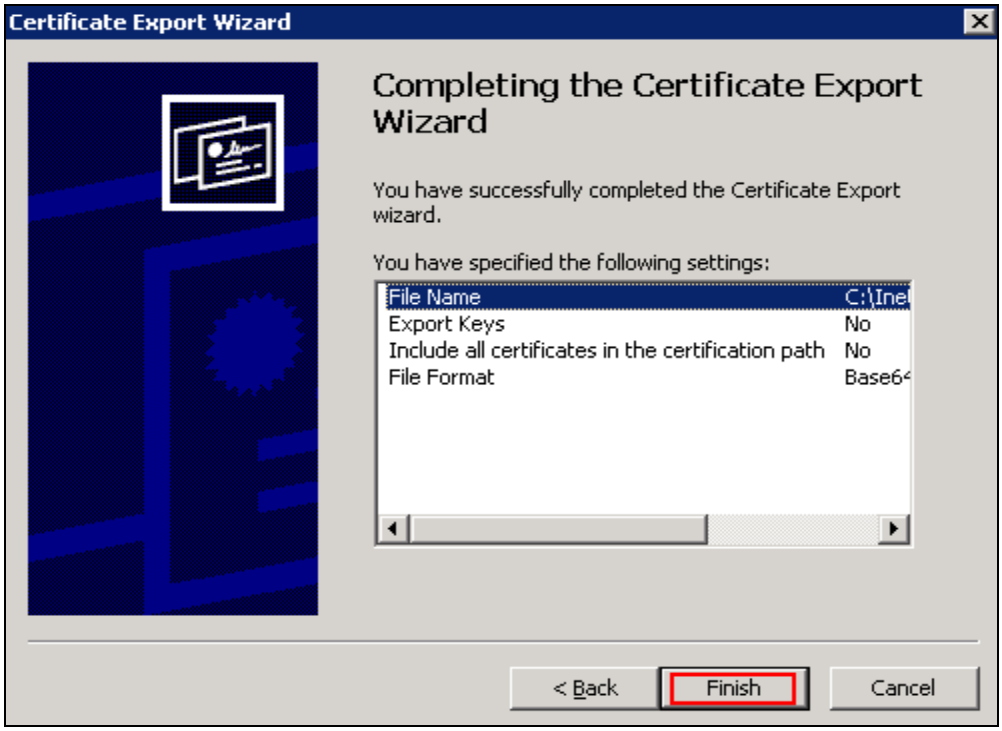
Select the **Base-64 encoded X.509 (.CER)** option and select the **Next** button.



Specify a location to store the certificate file. The file was stored in **C:\Inetpub\wwwroot** location. Select the **Next** button.



The **Completing the Certificate Export Wizard** screen is shown. Select the **Finish** button.



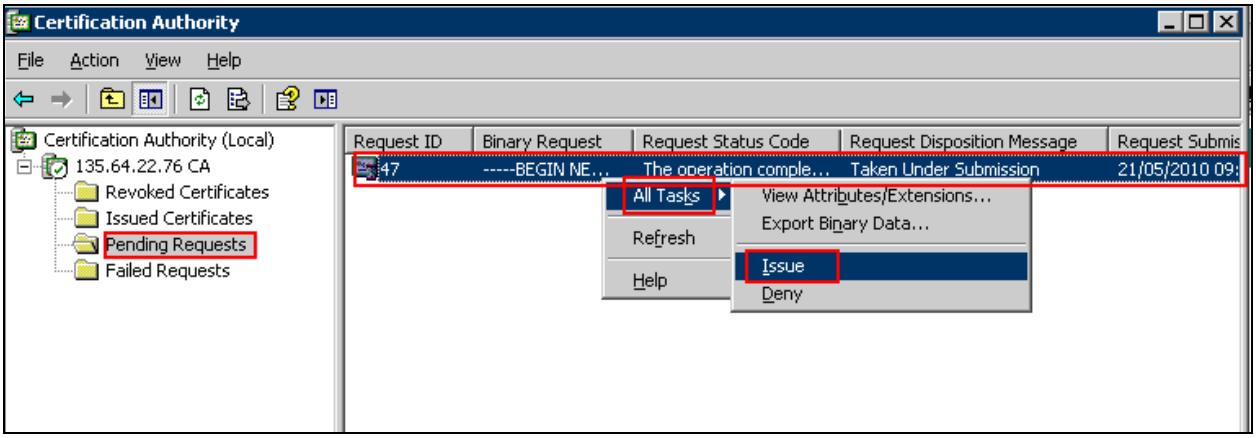
The **export was successful** dialog box was shown to confirm the successful export of the certificates.

3.4. Upload Certificates to 9600 IP Telephone

To upload the exported certificates to the 9600 IP telephone the 46xxsettings file is used. A number of settings need to be adjusted within the settings file to accomplish this. The **SCEPPASSWORD** and **SET TRUSTCERTS** variables need to be set. The SCEPPASSWORD is set to the password generated in **Section 3.2**. SET TRUSTCERTS is set to the file name **46vpn_cert.cer**, the file name of the exported certificates in **Section 3.3**. With these settings put into the 46xxsettings file the 9600 IP telephone is rebooted to upload the new 46xxsettings file to the 9600 IP telephone. When the 9600 IP telephone receives the 46xxsettings file, the IP telephone will enroll with the Microsoft CA. The 9600 IP telephone begins the uploading of the certificates to the IP telephone. The SCEP timeout is displayed on the 9600 IP telephone as the certificates are uploaded.

```
SCEP  10 secs
```

The 9600 IP telephone has begun requesting the certificates from the Microsoft CA and will continue requesting the certificate for 60 minutes until the certificate is issued. On the Microsoft CA the certifcates are currently in a Pending state and need to be issued to the 9600 IP telephone by the user for the uploading of the certificates to take place. From the **Pending Request** folder in the Microsoft CA subfolder right click on the pending certificate. Highlight the **All Tasks** heading and select **Issue**. This completes the uploading of the certificates



The following screen is displayed on the 9600 IP telephone.

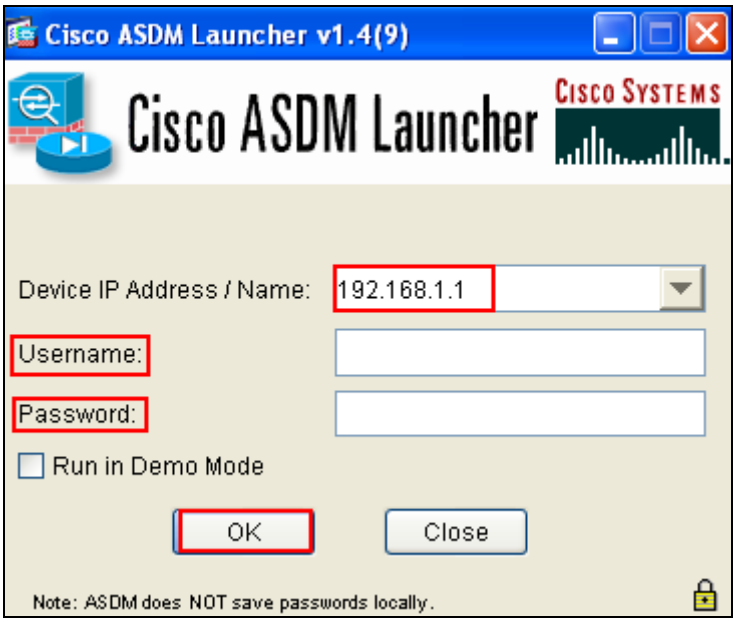
SCEP Successful

4. Configure Cisco 5510 Adaptive Security Appliance

The Cisco 5510 Adaptive Security Appliance was configured using Adaptive Security Device Manager software. The following steps describe how generate a keypair, create and authenticate a Trustpoint and enroll the TrustPoint with the Microsoft Certifcate Authority. It also describes the steps needed to create the IPSec VPN tunnel and VPN user accounts using the Adaptive Security Device Manager VPN Wizard of the Adaptive Security Device Manager application.

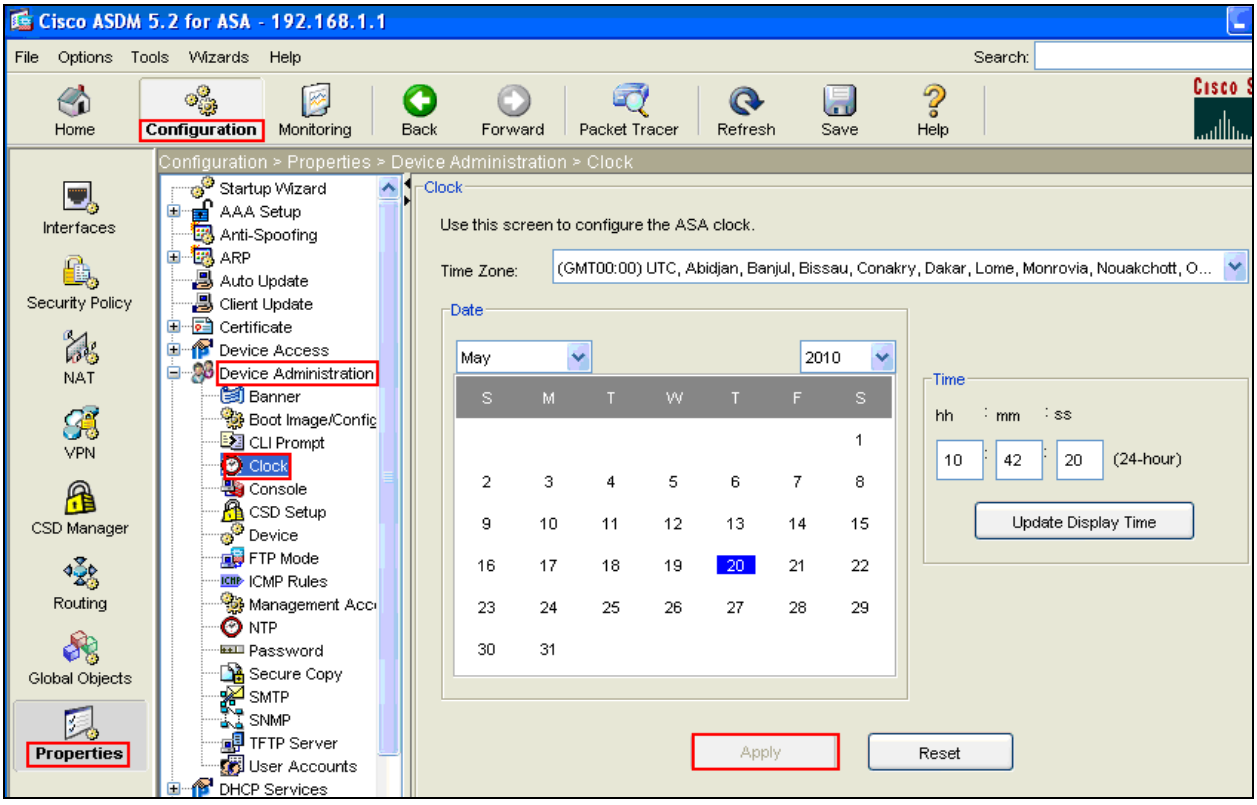
4.1. Access the Cisco 5510 Adaptive Security Device

The Adaptive Security Device Manager can be accessed by accessing the management interface of the Cisco 5510 Adaptive Security Appliance. The **IP Address** of the management interface 0/0 was **192.168.1.1**. Type the **Username** and **Password** and press the **OK** button.



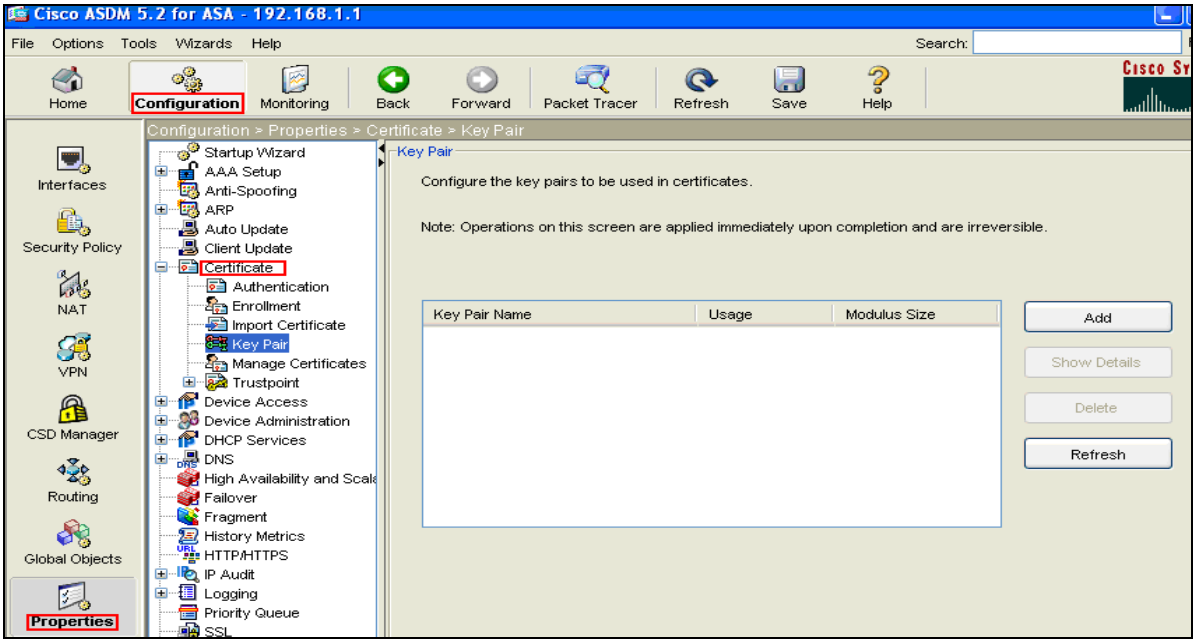
4.2. Set Date and Time on Cisco ASA

To set the date and time on the Cisco 5510 Adaptive Security Appliance, select **Configuration**, then **Properties**, then **Device Administration** and then select **clock.** Set the correct date and time on the system. Press the **Apply** button.

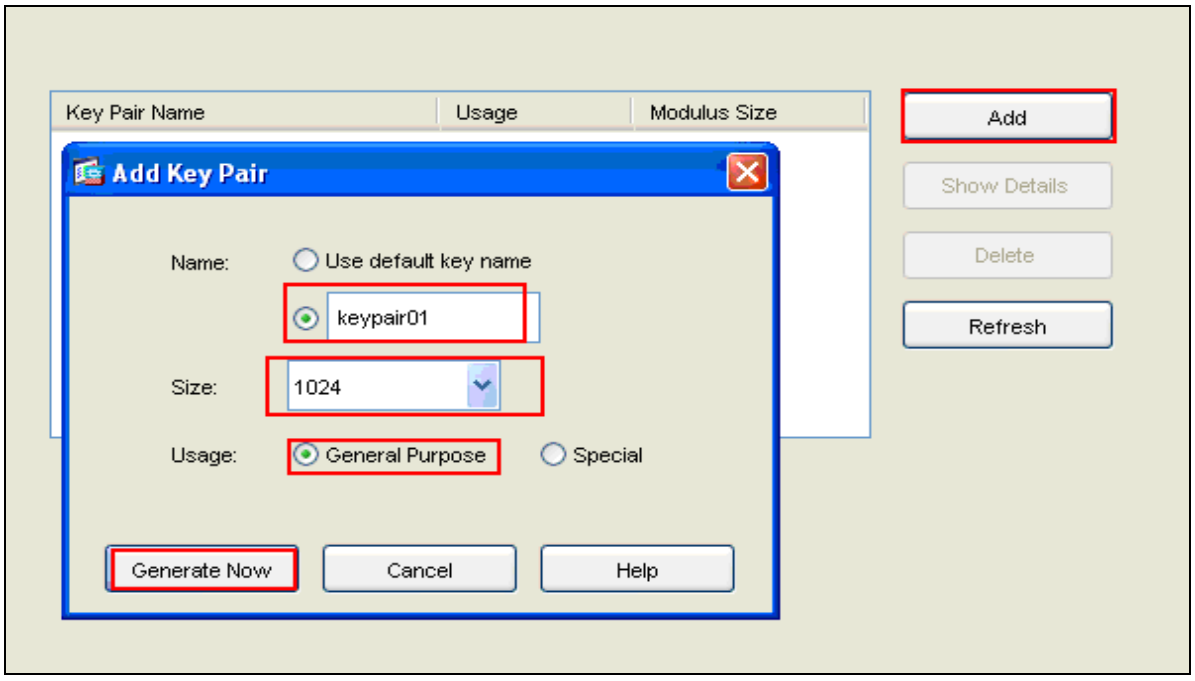


4.3. Generate Keypair

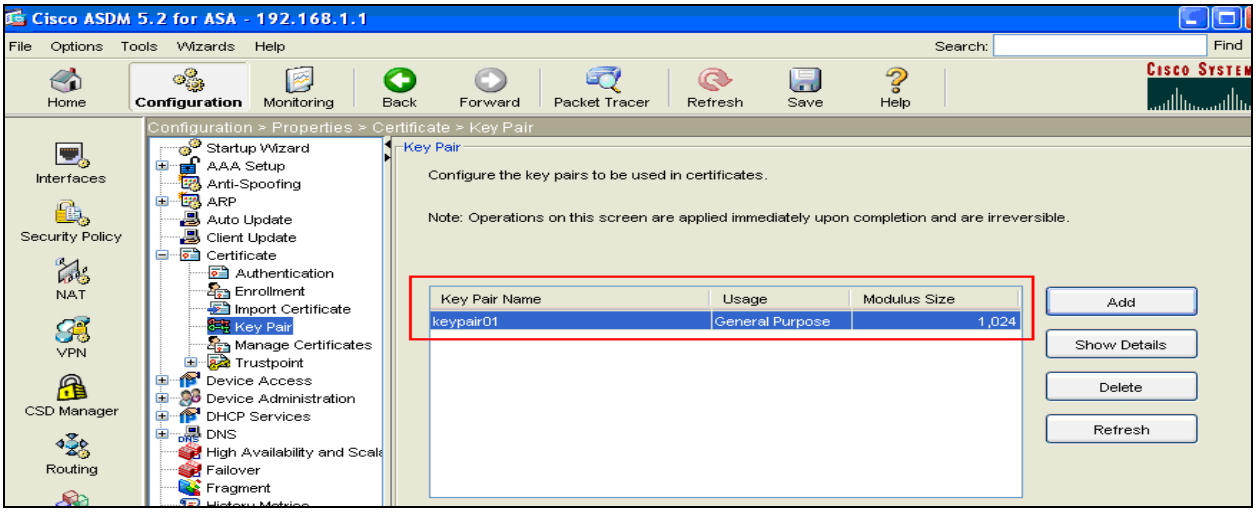
Configure the Cisco ASA key pair. The Cisco ASA must have its own private and public keys. The public key will be sent to the Microsoft CA during enrollment in **Section 4.6.** Select **Configuration**, then **Properties**, then **Certificate** then **Keypair.**



Select the **Add** button and set the keypair **Name** to **keypair01**, set the **Size** to **1024** and **Usage** to **General Purpose.** Press the **Generate Now** button

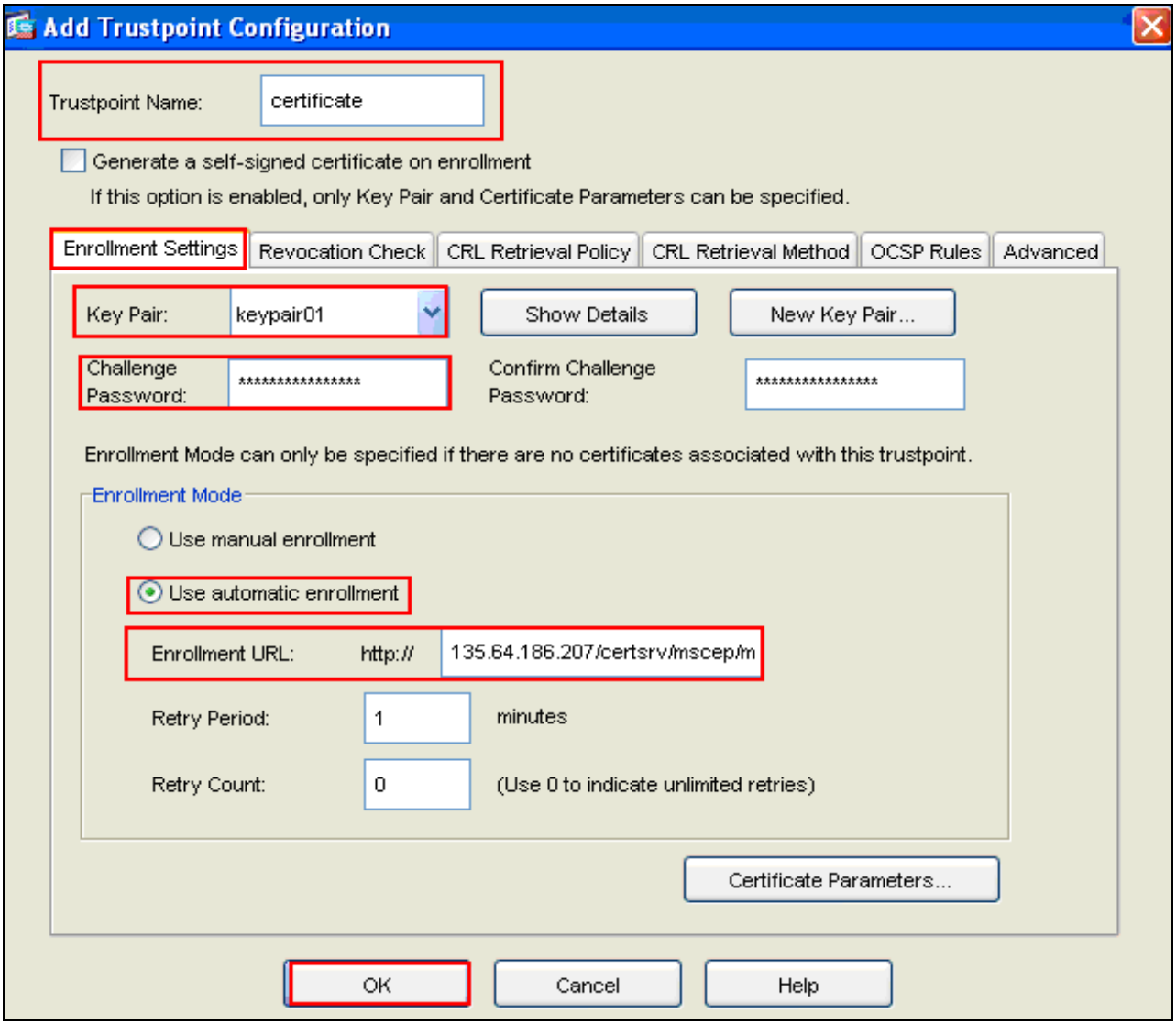


The following screenshot is shown with **keypair01** generated.

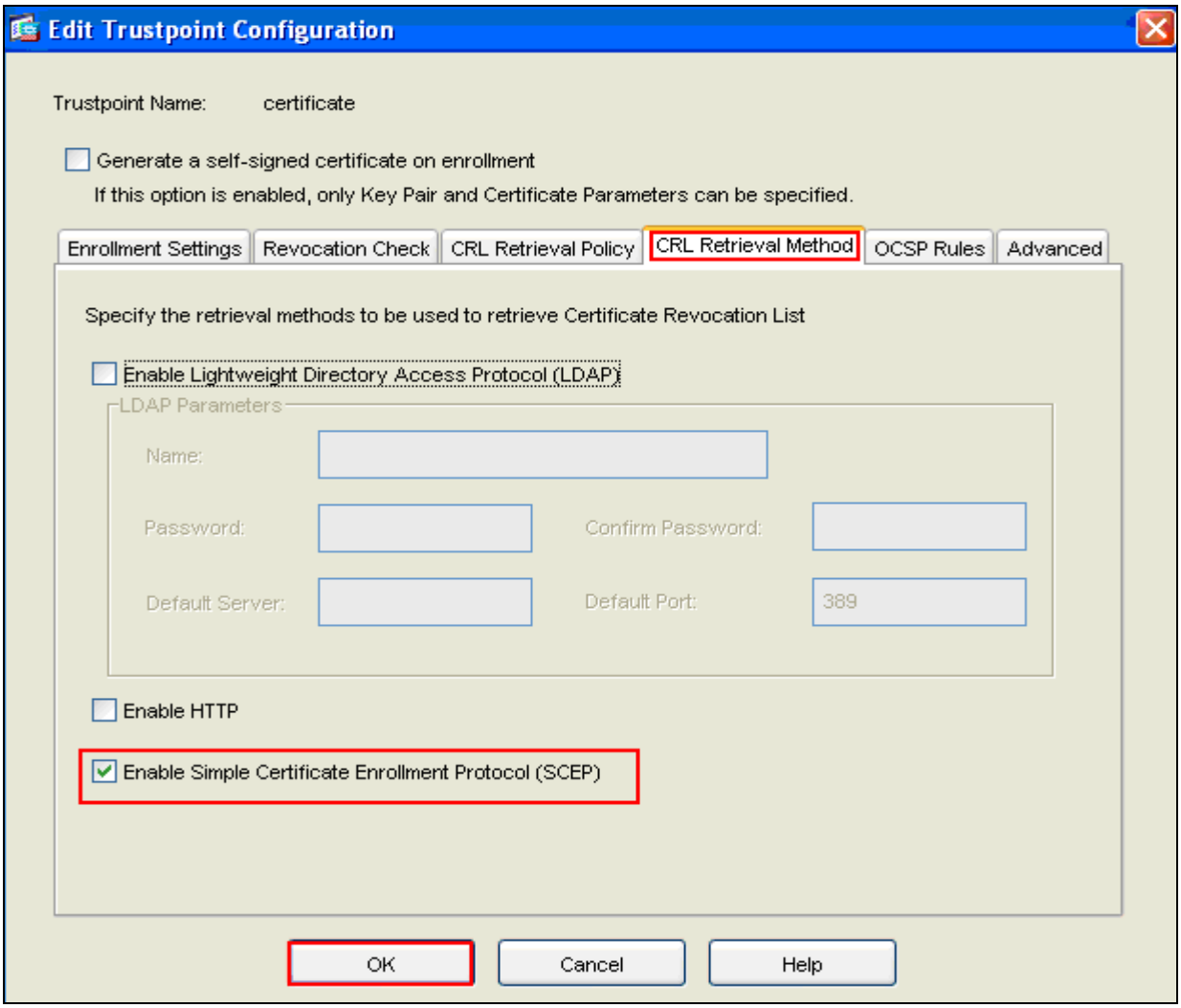


4.4. Create and Authenticate a TrustPoint

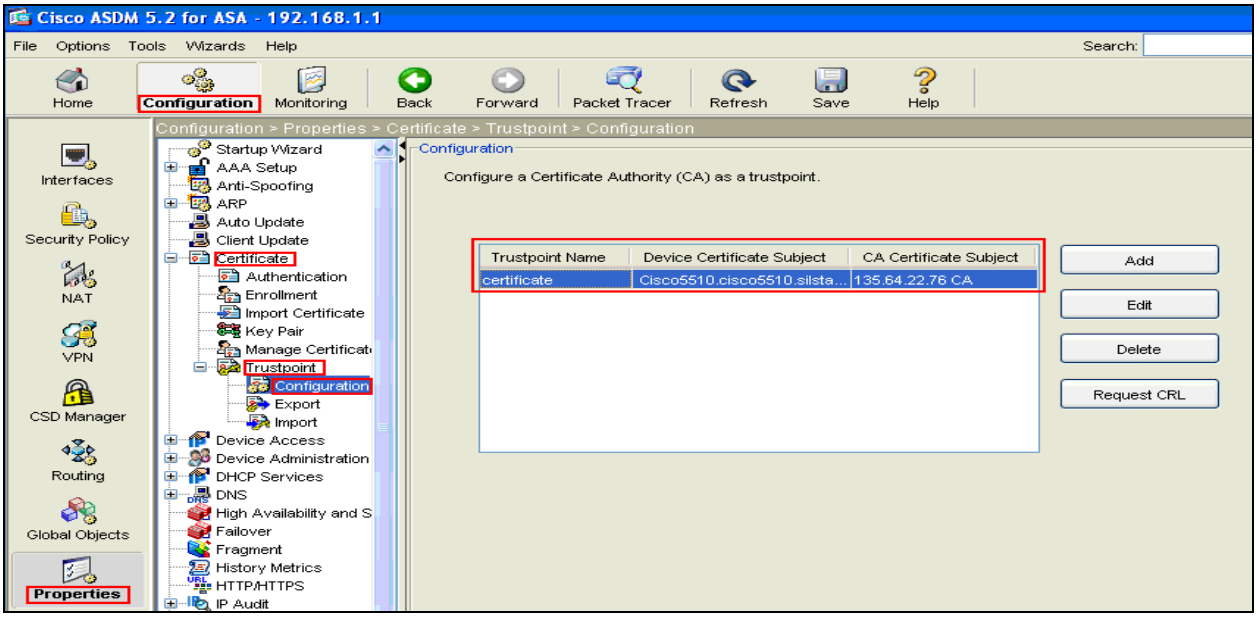
To add a new Trustpoint select **Configuration**, then **Properties**, then **Certificate** then **TrustPoint** then **Configuration.** The **Trustpoint name** was set to **Certificate.** Under **Enrollment Settings** set the **Key Pair** to **keypair01** as created in **Section 4.3**, set the **Challenge Password** to the password generated in **Section 3.2**. Choose the **Use automatic enrollment** and set the **Enrollment URL** to **http://135.64.186.207/certsrv.mscep/mscep.dll./135.64.186.207** is the IP Address of the Microsoft CA Server. Press the **OK** button.



Under the **CRL Retrieval Method,** set the **Enable Simple Certificate Enrollment Protocol (SCEP)** checkbox. Press the **OK** button.

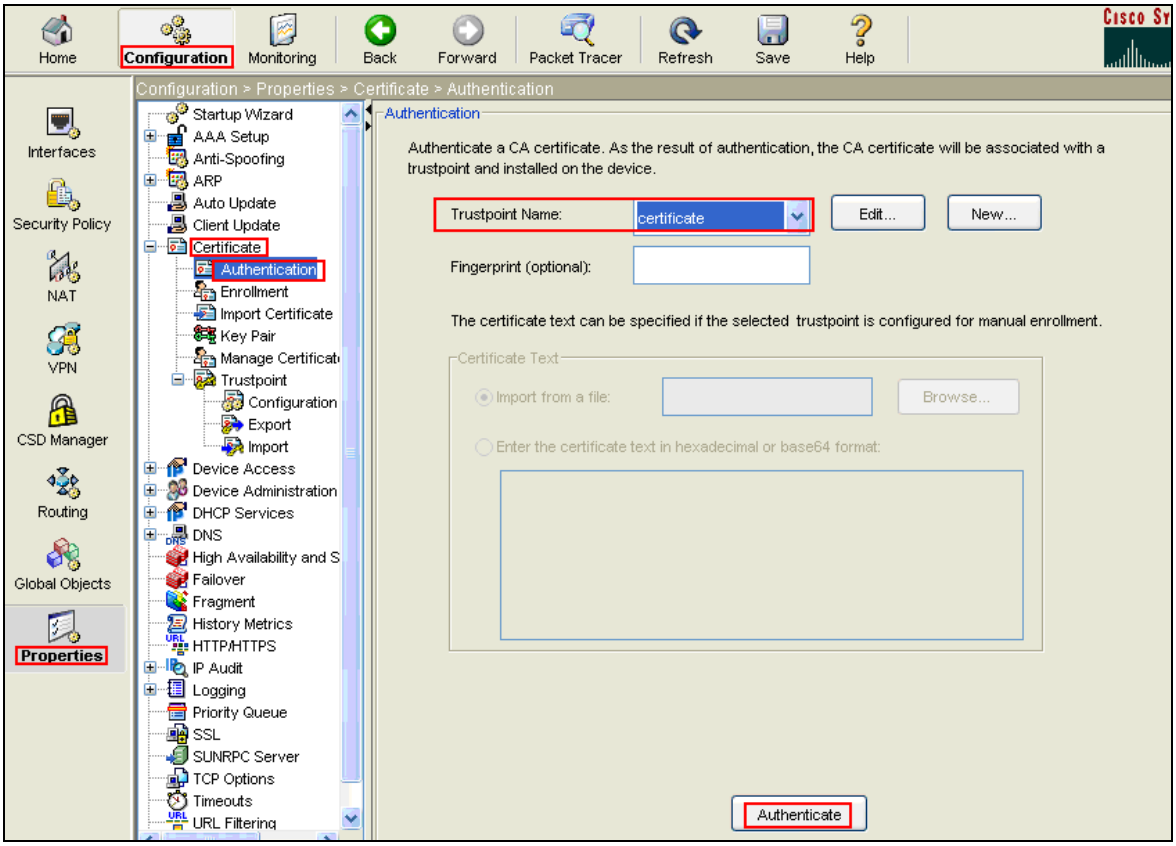


The following screenshot is displayed.



4.5. Authenticate the TrustPoint

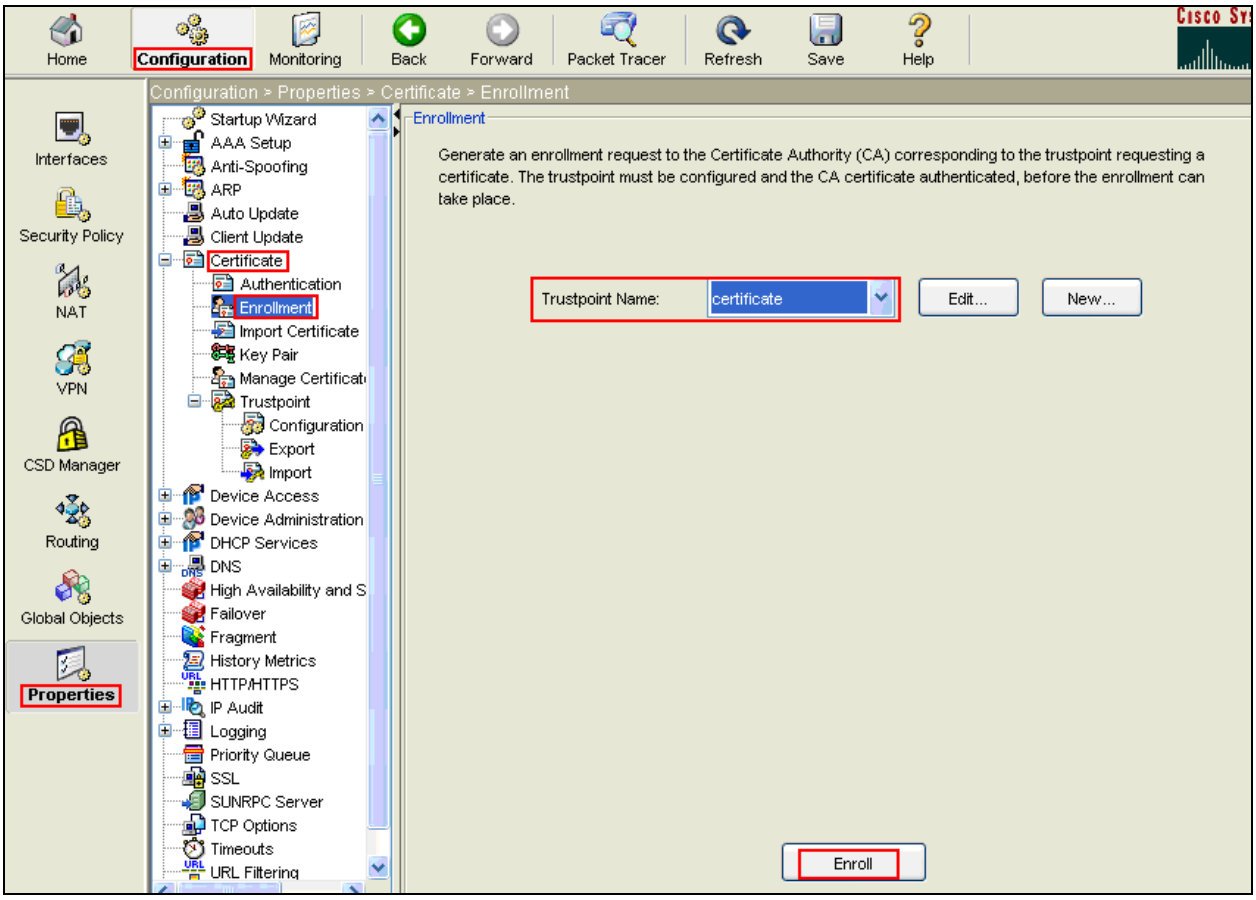
To authenticate the Trustpoint, select **Configuration, Properties, Certificate** then **Authentication**. Select the **Trustpoint Name** as **certificate** which was created in **Section 4.4** and click **Authenticate.**



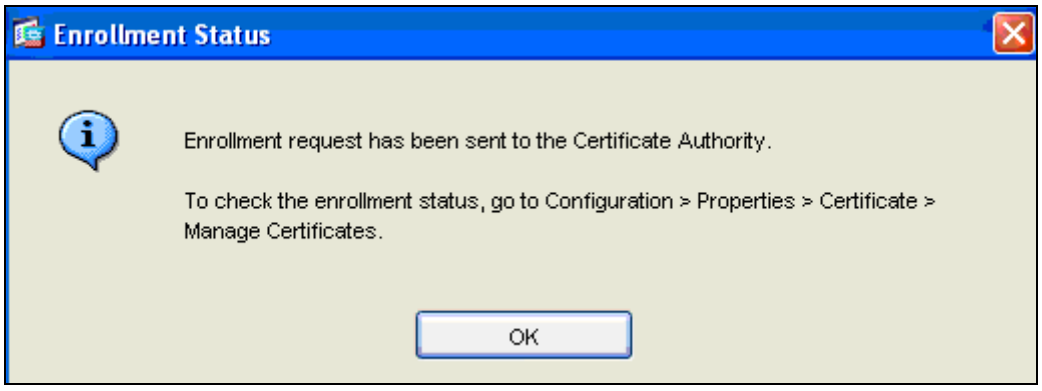
The following screenshot is displayed stating the authentication of the Trustpoint named **certificate** was successful.

4.6. Enroll a Trustpoint with Microsoft CA

To enroll a Trustpoint, select **Configuration, Properties, Certificate** then **Enrollment**. Select the **Trustpoint Name** as **certificate** which was created in **Section 4.4.** Press the **Enroll** button.

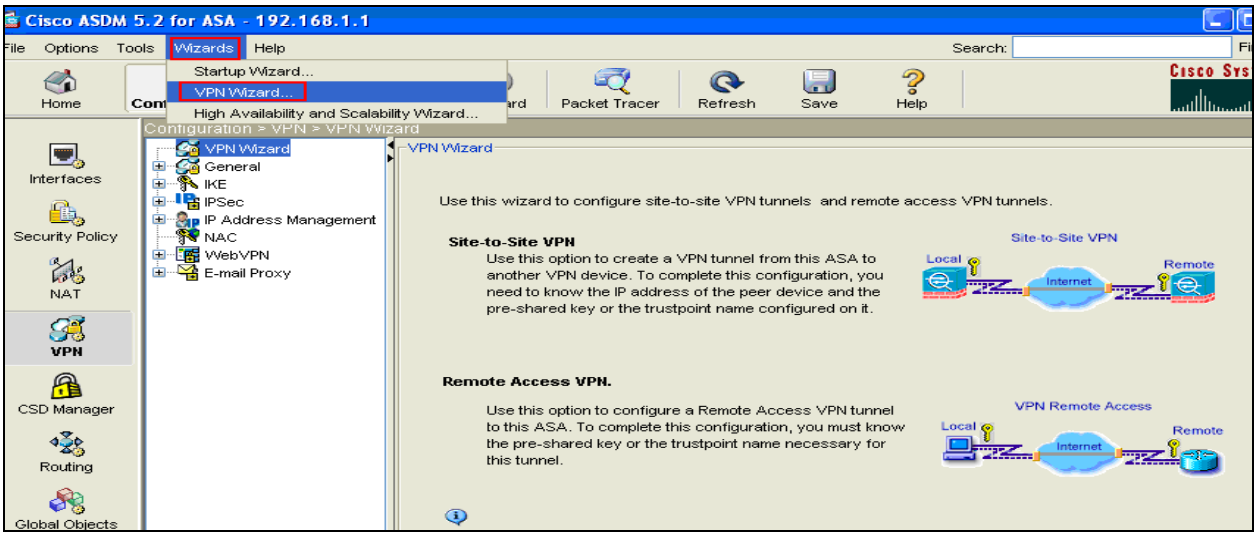


The following screenshot is displayed stating enrollment has been sent to CA.

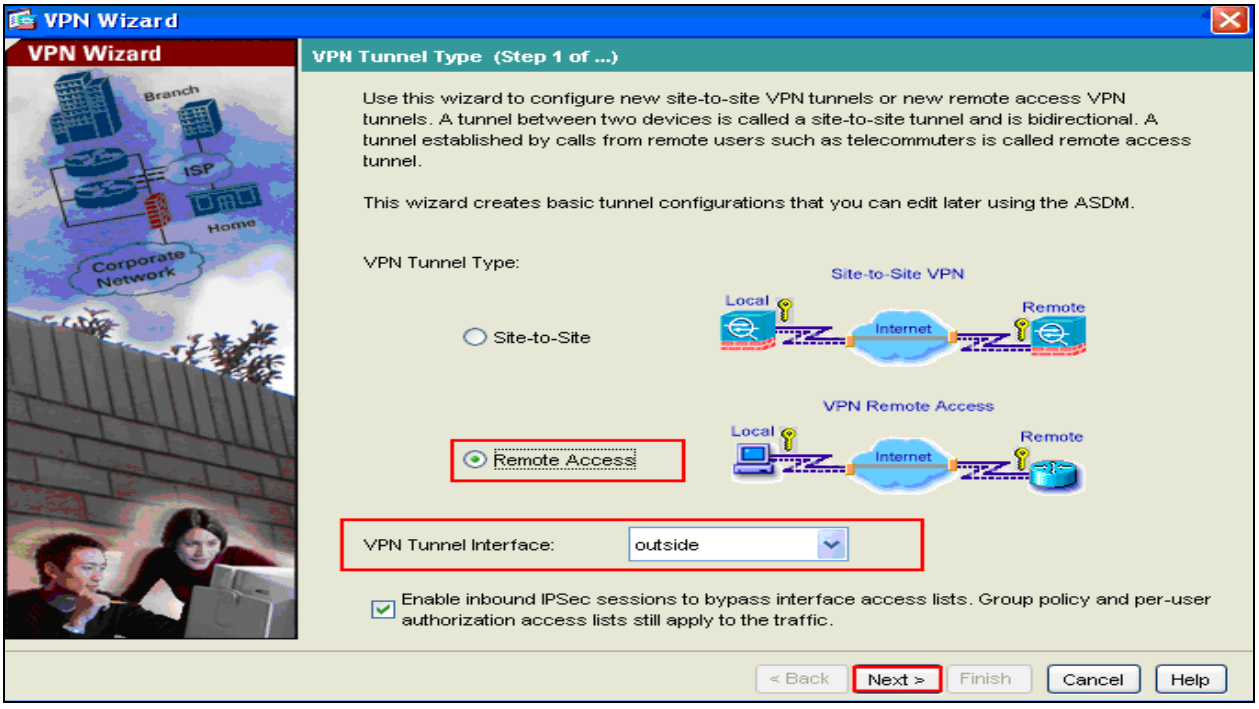


4.7. Create IPSec VPN Tunnel

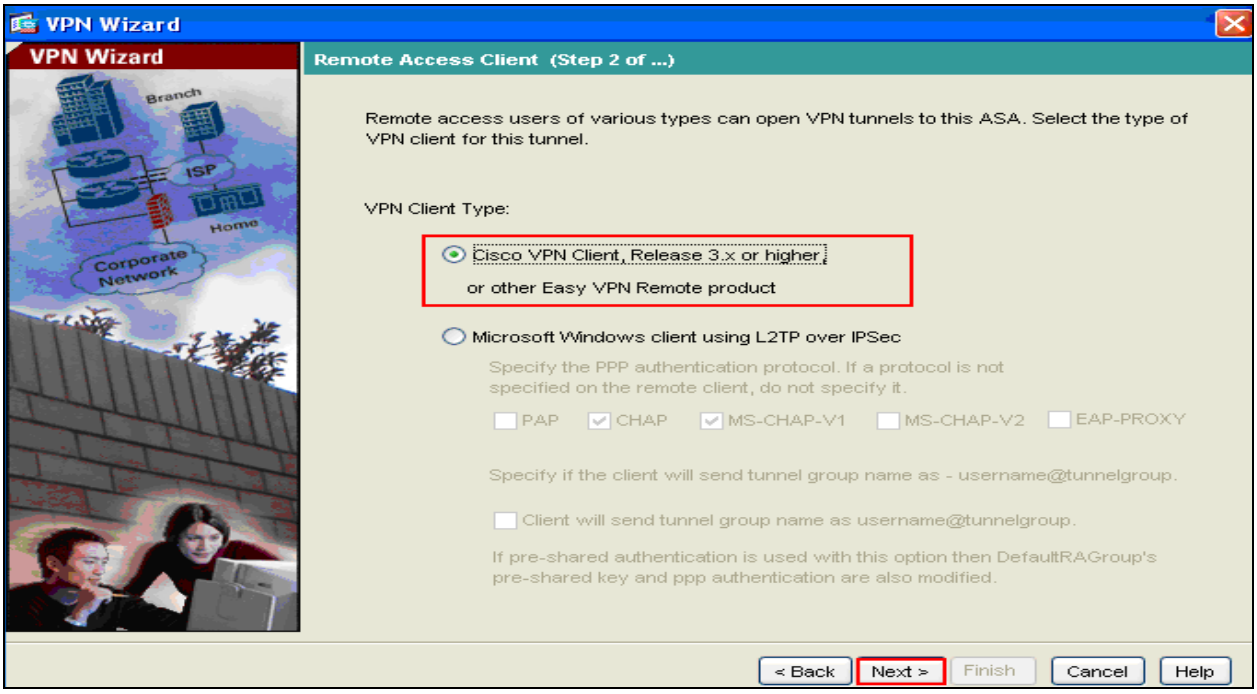
This section describes the steps to create the IPSec VPN and VPN user accounts using the Adaptive Security Device Manager VPN Wizard of the Adaptive Security Device Manager application. The user accounts are created in the user authentication database local to the Cisco 5510 Adaptive Security Appliance. Access the **Wizards** heading and sub heading **VPN Wizard.**



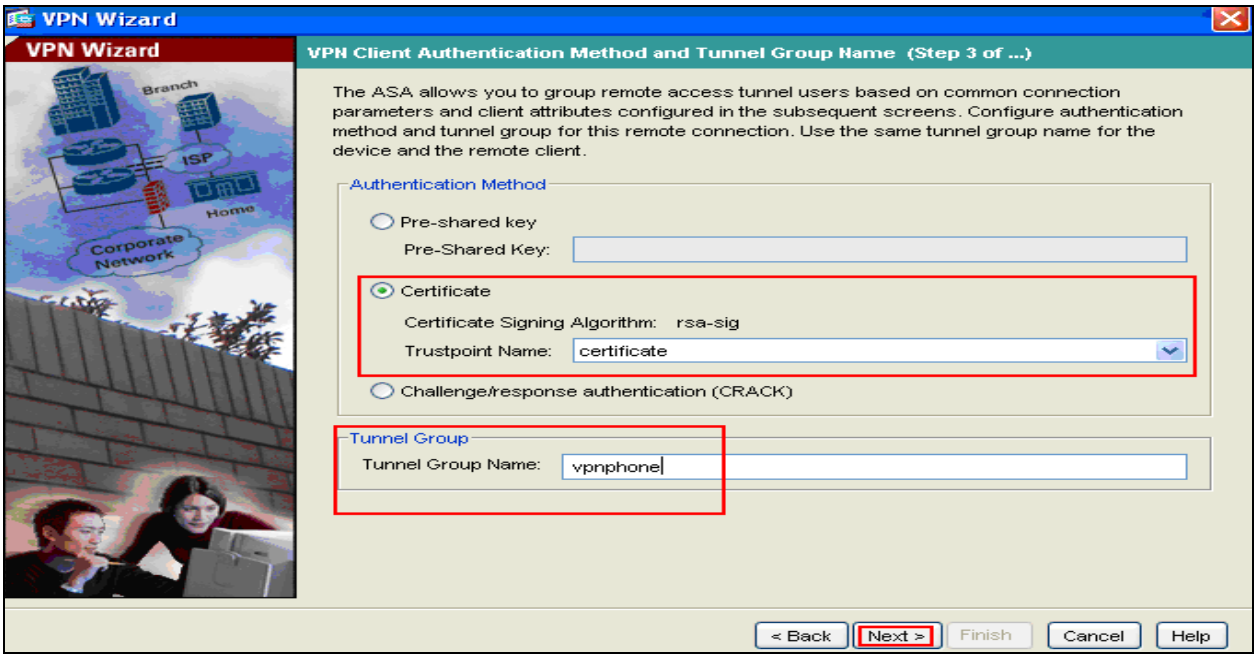
The following screenshot is displayed. Select **Remote Access** and set the **VPN Tunnel Interface** to **outside.** Press the **Next** button.



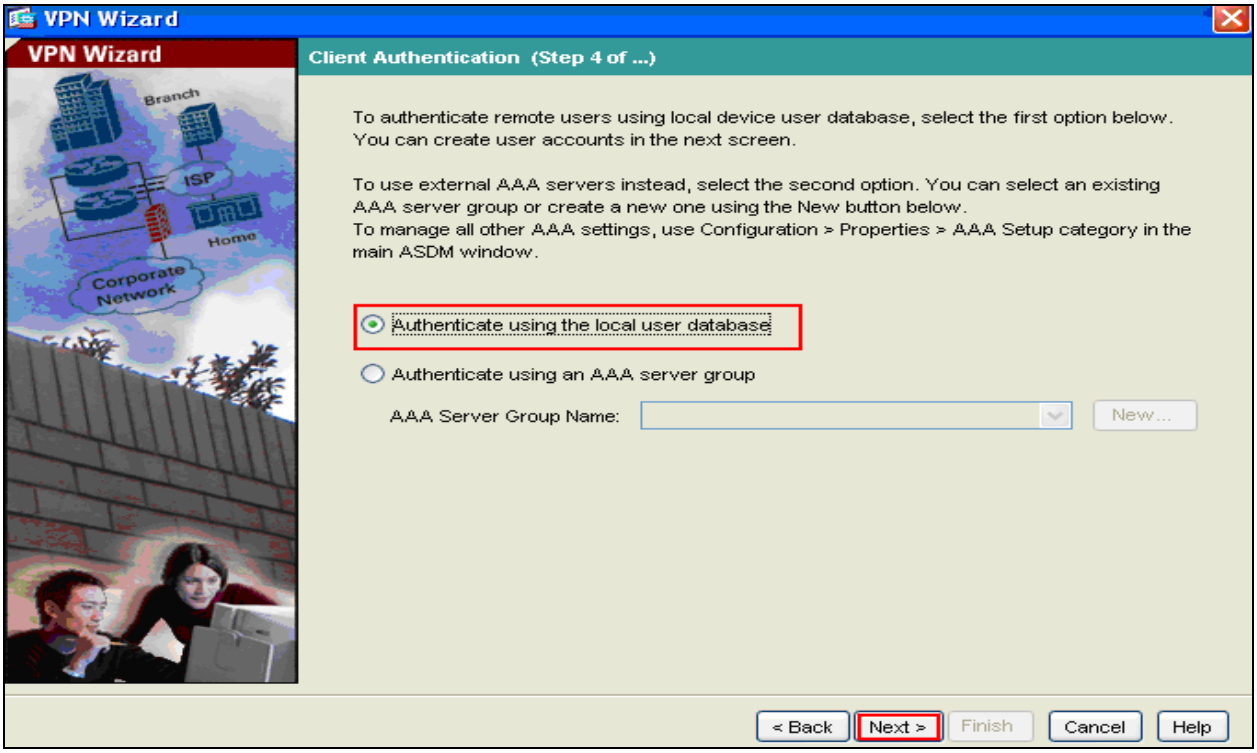
Set **VPN Client type** to **Cisco VPN Client, Release3.x or higher.** Press the **Next** button.



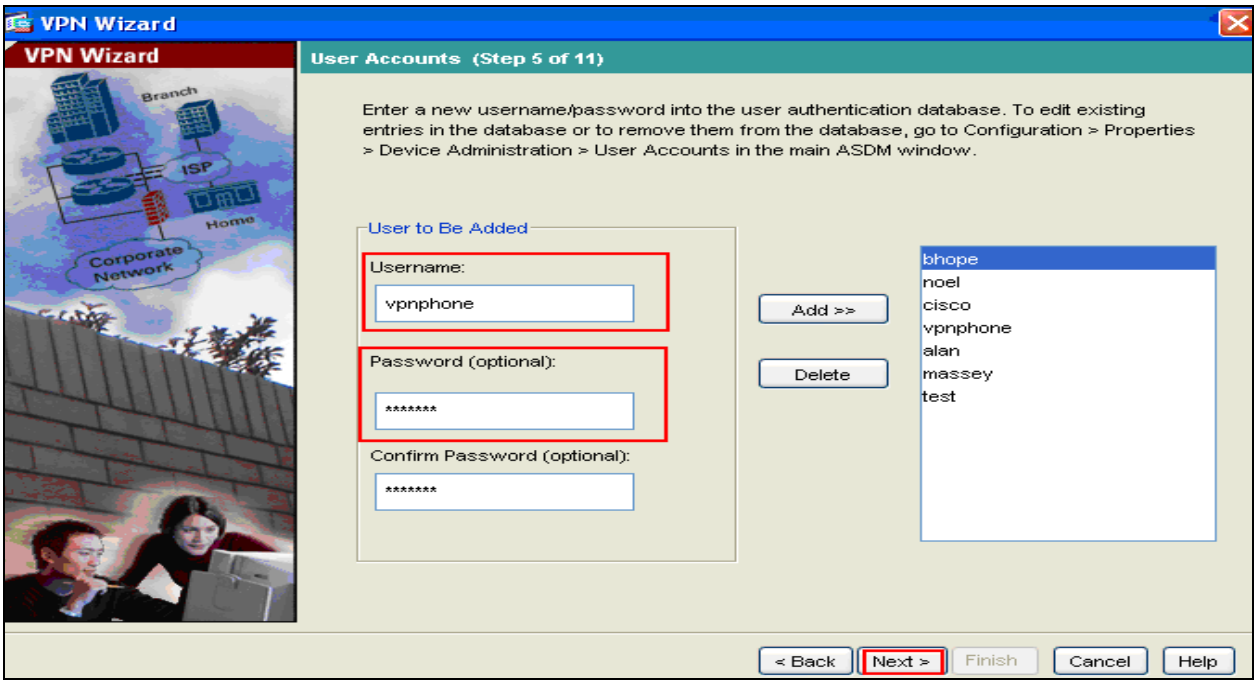
Set the **Authentication Method** to **Certificate** and select from the drop down menu the **Trustpoint Name** named **certificate** created in **Section 4.4**. It was decided to set the **Tunnel Group Name** to **vpnphone.** Press the **Next** button.



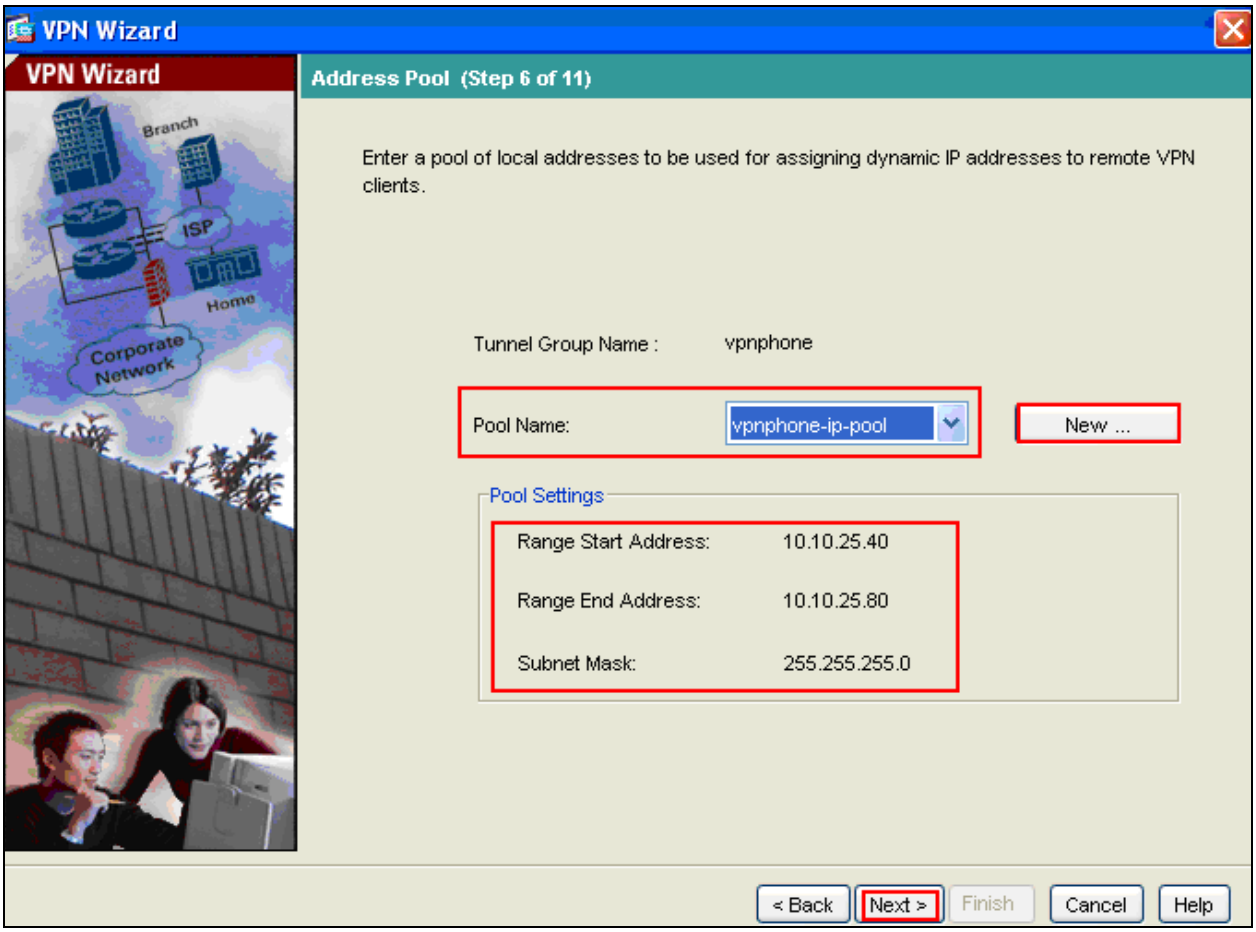
Select **Authenticate using the local user database**. Press the **Next** button.



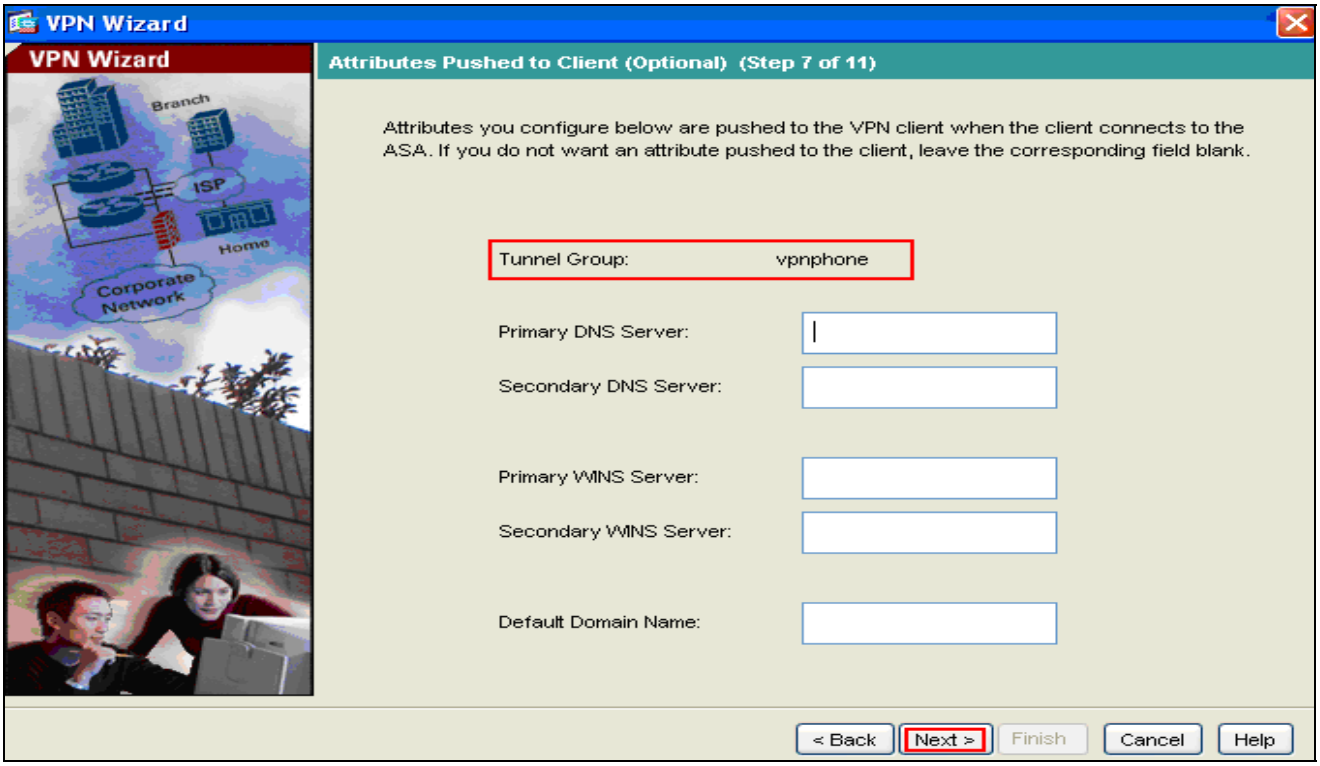
Enter **vpnphone** as the **Username** and an appropriate **Password.** Press the **Next** button.



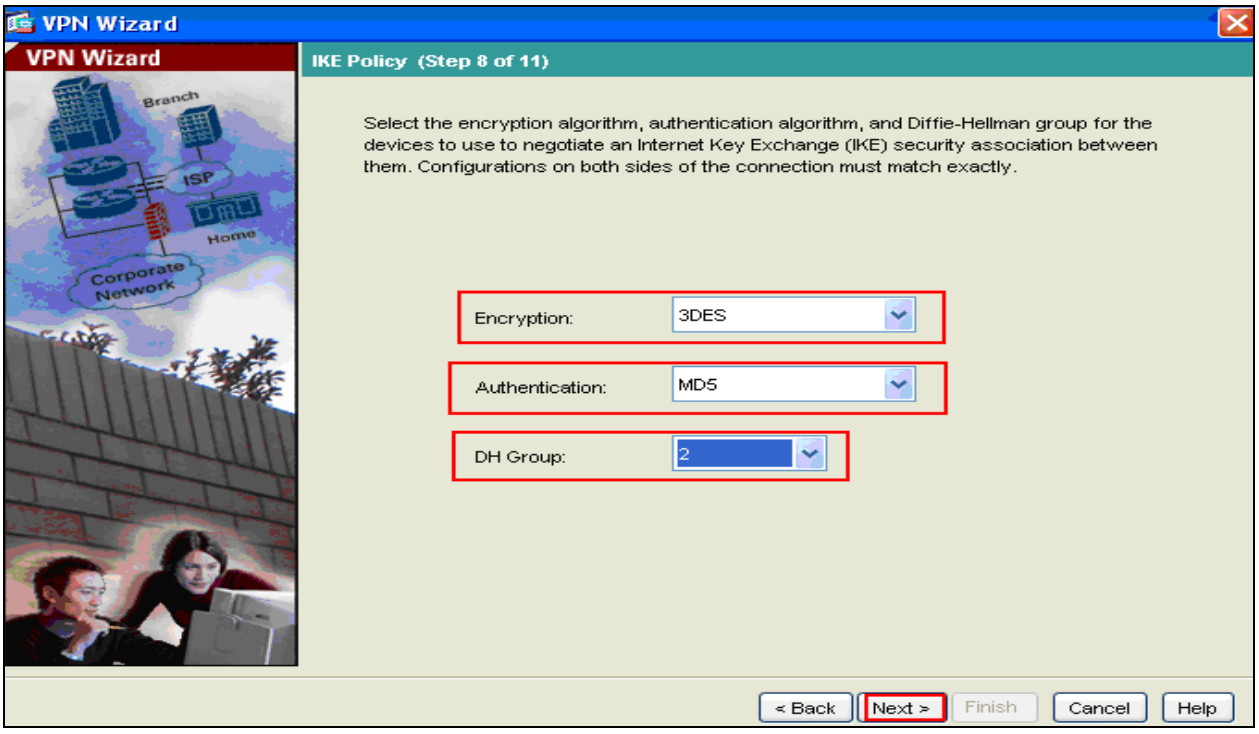
Select the **New** button to create a new pool of local IP Addresses. It was decided to set the IP Address pool range name as **vpnphone-ip-pool.** Set the IP Address pool range from **10.10.25.40 to 10.10.25.80.** This is the range of IP addresses the VPN telephone will take its IP Address from. Press the **Next** button.



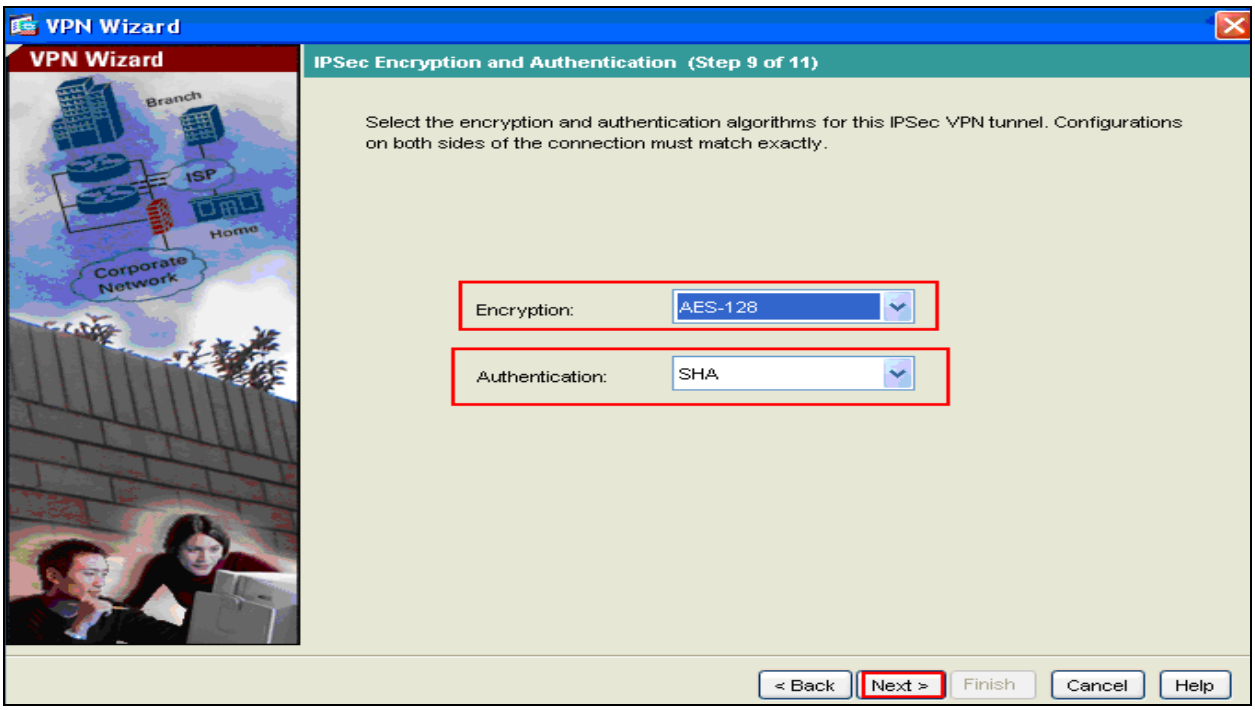
No values were needed for DNS Server or WNS Server. Press the **Next** button.



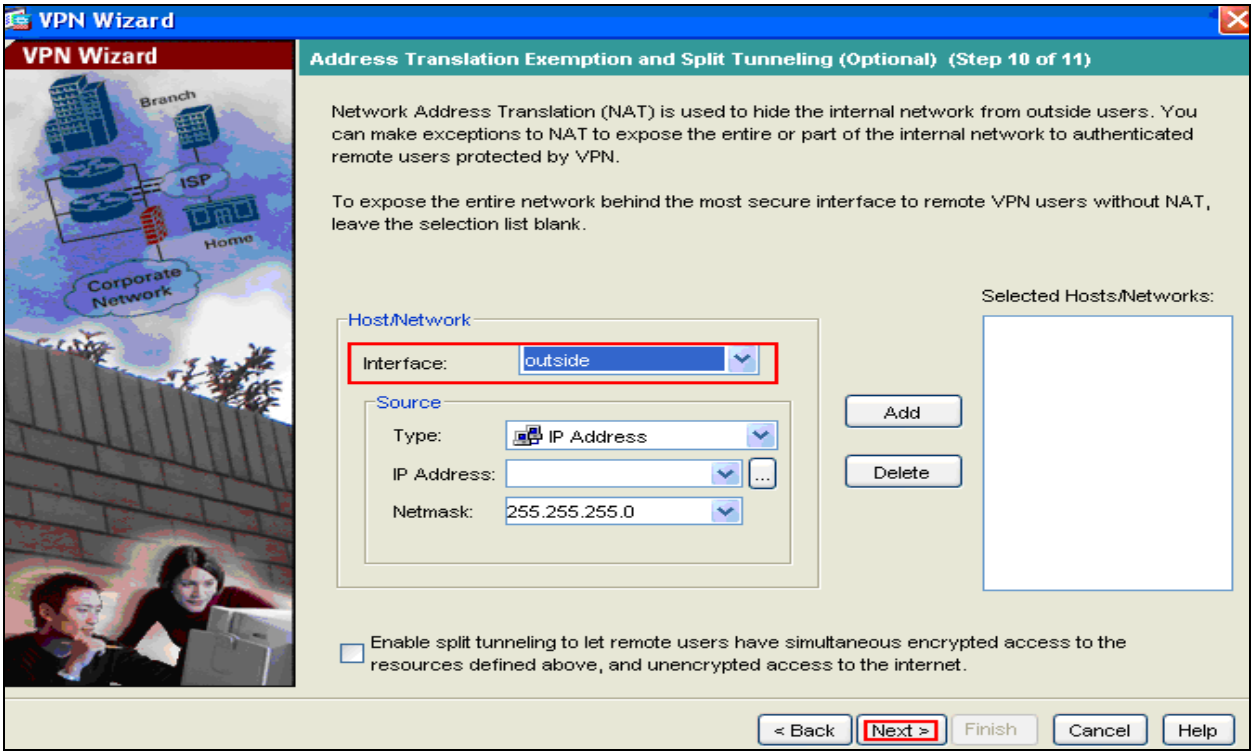
Set the IKE **Encryption** to **3DES,** set the IKE **Authentication** to **MD5** and set the **DH Group** to **2.** Press the **Next** button.



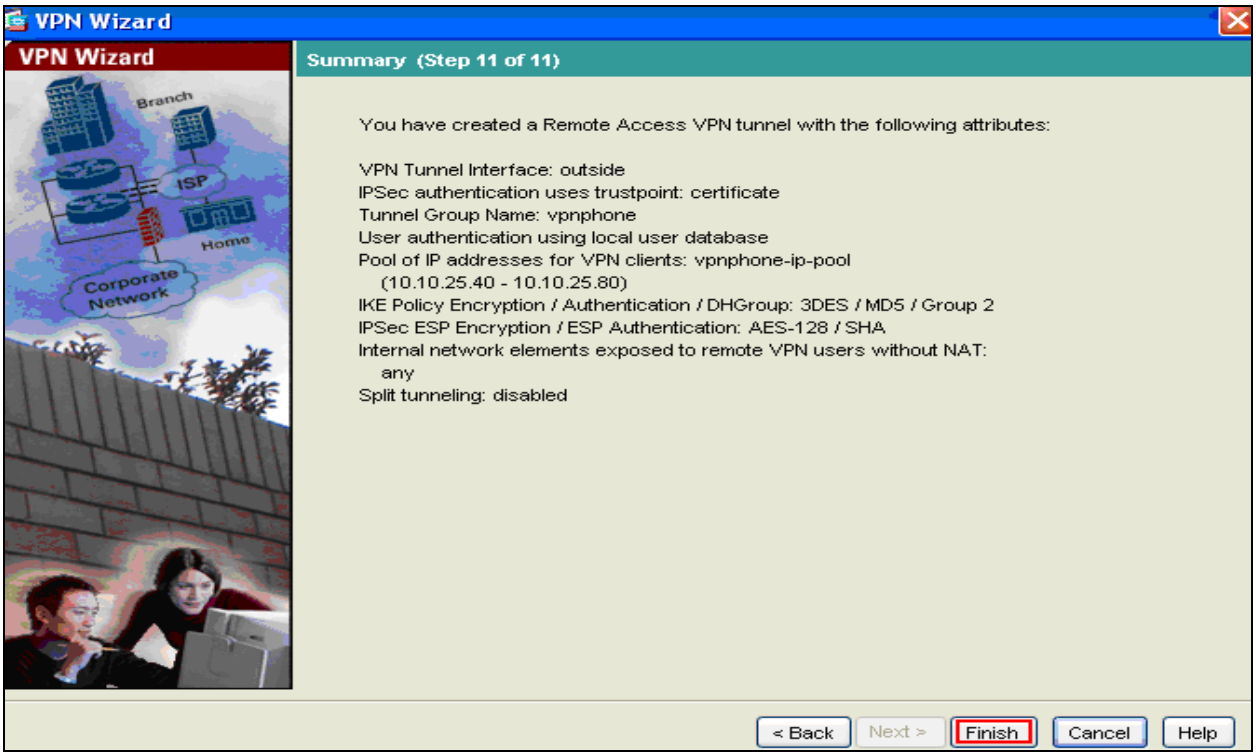
Set the IPSec **Encryption** to **AES-120** and IPSec **Authentication** to **SHA**. Press the **Next** button.



Set the **Interface** to **outside**. All other fields are not required. Press the **Next** button.

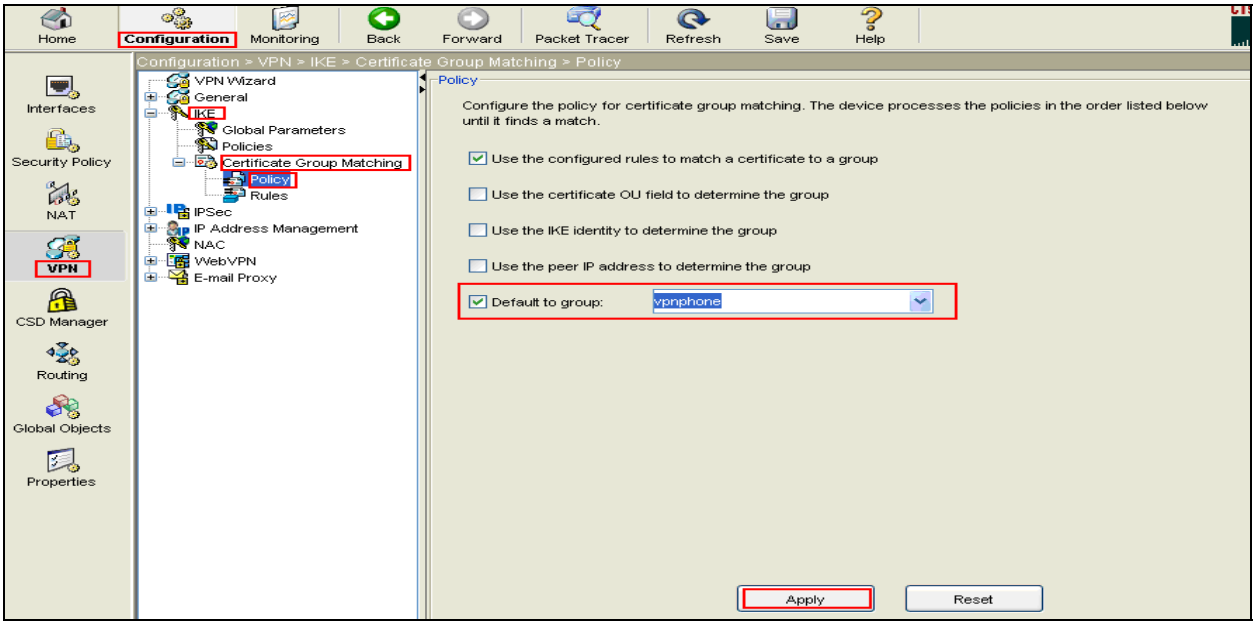


Press the **Finish** button.



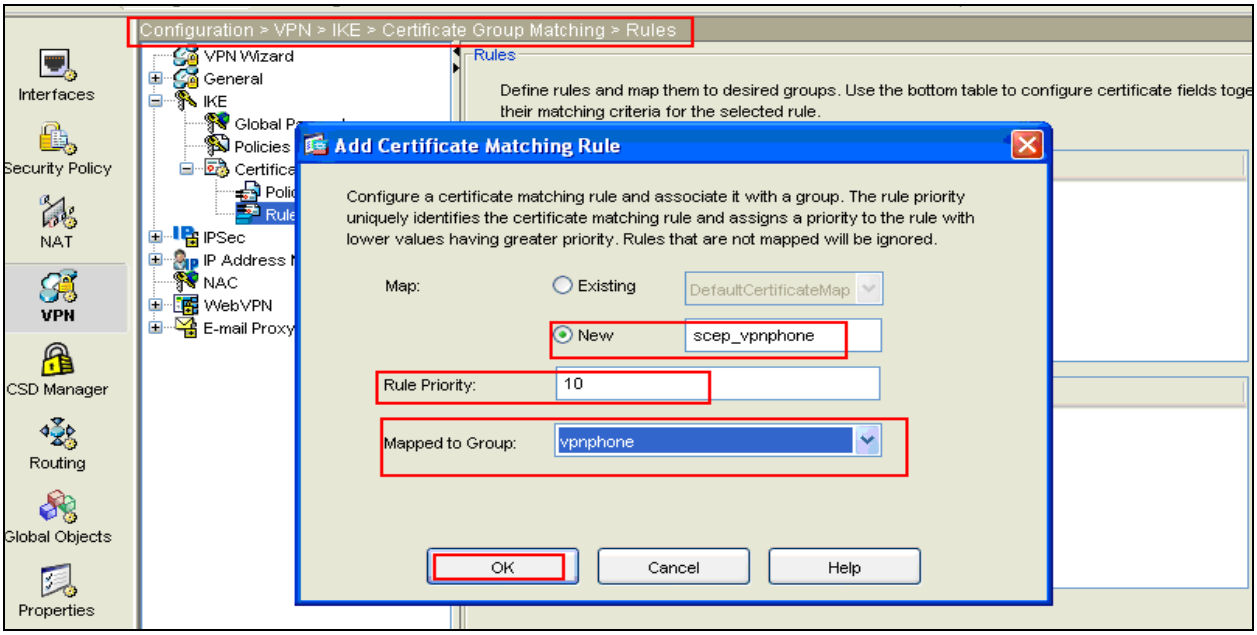
4.8. Create VPN Policy

For an added layer of security when using certificate based authentication, the Certificate Group Matching feature of the Cisco 5510 Adaptive Security Appliance can be used with Avaya VPN telephones. Certificate Group Matching allows a rule to be created to match an Avaya VPN telephone certificate based on fields of the certificate. The rule created in the sample configuration requires the Common Name attribute of the certificate to contain a specified string value. The string value used is the first three octets of the MAC address of the Avaya 9600 Series IP Telephone, 00-04-0d. These first three octets of a MAC address are designated as the Organizationally Unique Identifier and common across all 9600 Series IP Telephones. This rule verifies that the device the certificate is associated with is an Avaya Telephone. To populate the Common Name attribute of the certificate with the MAC address of the Avaya VPN telephone, the variable MYCERTCN must be set to $MACADDR in the 46xxsetting.txt file. Select **Configuration**, **VPN, IKE**, **Certificate Group Matching** and select **vpnphone** as the **Default to group** as created in **Section 4.7**. Press the **Apply** button.

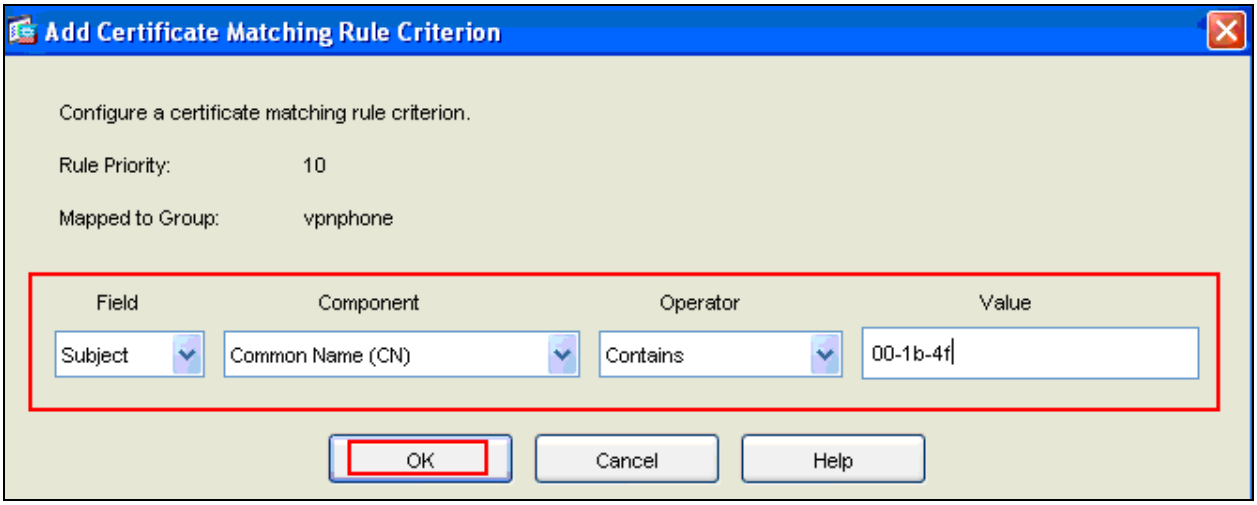


4.9. Create VPN Rule

To create a new VPN Rule, select **Add** (not shown) and enter the **New** rule name **SCEP_vpnphone**. Set the **Rule Priority** to **10.** Set **Mapped to Group** to **vpnphone**, the vpn tunnel group name created in **Section 4.7.** Press the **OK** button.



In the subsequent screen set the first three octets of the MAC address of the 9600 IP telephone.



5. 46xxSettings File

The 46xxsetting.txt file contains Virtual Private Network specific variables for the Avaya 9600 IP telephone to use during the setup of the IPSec VPN tunnel. Variables specific to digital certificate authentication and the Cisco 5510 Adaptive Security Appliance are listed below. Descriptions of each variable and the values used in the sample configuration are shown.

SET NVVPNMODE 1
This variable dictates when the VPN Client is started. If it's value is 1, VPN Client is started immediately after TCP/IP stack is initialized, If it's value is 0, VPN Client is disabled

SET NVVPNSVENDOR 2
Specifies the security gateway Vendor to be used.
1 = Juniper PSK with Authentication or Juniper Certificate with Authentication
2 = Cisco PSK with Authentication or **Cisco Certificate with Authentication**
3 = Checkpoint Security Gateway
4 = Generic PSK
5 = Nortel Contivity

SET NVVPNENCAPS 0
Specifies type of UDP encapsulation method to use if there is a NAT device between phone and the security gateway. By default UDP Encapsulation 4500-4500 is used.

SET NVVPNCOPYTOS 2
The value of this variable decides whether TOS bits should be copied from inner header to outer header or not. If it's value is 1, TOS bits are copied otherwise not. By default TOS bits are not copied from inner header to outer header. Some Internet Service Provider don't route the IP packets properly if TOS bits are set to anything other than 0.

SET NVVPNAUTHTYPE 5
RSA Signature with Authentication
3 = PSK
4 = PSK with Authentication
5 = RSA Signature with Authentication
6 = Hybrid Authentication
7 = RSA Signature

SET NVVPNUSERTYPE 1
Specifies whether the user can change the VPN username.

SET NVVPNUSER "vpnuser"
This variable contains the VPN User Name. In most cases this value will be unique to each phone hence should not be specified here. However it is possible to force the VPN client in the phone to use phone's mac address or serial number as user name thus eliminating the need to

enter user name by the phone user via phone keypad. In such cases you need to add each phone's serial number or mac address in your authentication

SET NVVPNPSWDTYPE 1
This variables determines how password should be treated. By default, password type is set to 1. You must set this variable to 3 or 4 if using One Time Password such as SecureID from RSA.

SET NVIKEID "vpnphone"
Phone uses this string as IKE Identifier during phase 1 negotiation. Some XAuth documentation refers to this variable as group name because the same IKE Id is shared among a group of users. Individual user authentication is done using XAuth after establishing IKE phase 1 security association.

SET NVIKEIDTYPE 11
Phone uses this variable as the IKE Identifier type for the IKE-ID specified via NVIKEID variable.

SET NVVPNCFGPROF 8
For Cisco authentication with certificates choose option number 8.

The following variables are set to specified value when **NVVPNCFGPROF** is set to **8**

NVIKECONFIGMODE 1
NVIKEIDTYPE 11
NVIKEXCHGMODE 1

SET NVIKEDHGRP 2
This variable contains the value of the DH group to use during phase 1 negotiation. By default phone uses Group 2.

SET NVIKEP1ENCALG 2
Security Gateway picks the algorithm mandated by administrator.
0 ANY
1 AES-128
2 3DES
3 DES
4 AES-192
5 AES-256

SET NVIKEP1AUTHALG 0
0 ANY
1 MD5
2 SHA1

SET NVPFSDHGRP 2
This variable contains the value of DH group to use during phase 2 negotiation for establishing IPsec security associations also known as perfect forward secrecy. By default PFS is disabled.

SET NVIKEP2AUTHALG 0
0 ANY
1 MD5
2 SHA1

SET NVIKEOVERTCP 0
Specifies whether and when to use TCP as a transport protocol for IKE.

SET MCIPADD 135.64.186.81
The Call Server Addresses which is the processor IP Address of the MBT.

SET TRUSTCERTS "46vpn_cert.cer"
List of trusted certificates to download to phone. This parameter may contain one or more certificate filenames, separated by commas without any intervening spaces. Files may contain only PEM-formatted certificates.

SET MYCERTWAIT 1
Specifies whether the telephone will wait until a pending certificate request is complete, or whether it will periodically check in the background.

SET MYCERTURL http://135.64.186.207/certsrv/mscep/mscep.dll
URI used to access SCEP server.

SET MYCERTCN $MACADDR
Common Name specified for SUBJECT of SCEP certificate request.

SET SCEPPASSWORD "9B5F04D7D3FCEBFD "
The string specified here is used by phone as the SCEP challenge pass phrase for SCEP certificate enrollment. If left unspecified and SCEPPASSWORDREQ is SET to 0, phone uses it's SERIAL number as the challenge pass phrase.

6. Administer Avaya Aura™ Communication Manager

This section highlights the important commands for registering the Avaya 9600 IP telephone within Communication Manager and administering an IP network region and IP codecs to carry calls between Avaya IP endpoints.

6.1. Verify OPS Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Concurrently Registered IP Stations** has been set to the value that has been licensed, and that this value will accommodate addition of IP telephones. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya Sales representative to obtain additional capacity.

```
display system-parameters customer-options                      Page   2 of  11
                               OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 8000  12
          Maximum Concurrently Registered IP Stations: 18000 5
            Maximum Administered Remote Office Trunks: 8000  0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 100   3
                       Maximum Administered SIP Trunks: 5000  80
  Maximum Administered Ad-hoc Video Conferencing Ports: 8000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

6.2. Administer Dial Plan Analysis

This section describes the **Dial Plan Analysis** screen**.** This is Communication Manager's way of translating digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The **Dialed String** beginning with the number **4** and with a **Total Length** of **5** digits will be used to administer the **extension** range used for the IP telephones.

```
display dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location:  all          Percent Full:    0

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    0            1    fac
    1            5    ext
    2            5    aar
    209          5    ext
    3            5    aar
    4            5    ext
    5            5    ext
    6            5    ext
    7            5    aar
    8            5    aar
    9            1    fac
    *            3    dac
    #            3    dac
```

6.3. Administer IP Node-Name

This section describes **IP Node-Name** form. This is where Communication Manager assigns the IP Address and node-name to the SIP Enablement Server. The node-name of the SIP Enablement Server is **ses1** and the IP Address of the SIP Enablement Server is **135.64.186.89** within Communication Manager. Communication Manager automatically populates a processor node name to the IP Address of Communication Manager. This node name is **procr** with IP Address **135.64.186.81**.

```
list node-names all

                        NODE NAMES

Type     Name              IP Address
IP       AES1              135.64.186.88
IP       CMM               135.64.186.82
IP       MedSvcsMedpro1    135.64.186.84
IP       MedSvcsMedpro2    135.64.186.85
IP       MedSvcsMedpro3    135.64.186.86
IP       MedSvcsMedpro4    135.64.186.87
IP       procr             135.64.186.81
IP       ses1              135.64.186.89
```

6.4. Administer IP Network Region

This section describes **IP Network Region** screen**.** The sample configuration places all IP endpoints in the one network region. The **Authoritative Domain** must mirror the domain name of the SIP Enablement Server. This was **silstack.com**.The codecs used on the IP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes.**

```
display ip-network-region 1                                   Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: silstack.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

6.5. Administer IP Codec Set

This section describes the **IP Codec Set** screen. It was decided to use IP Codecs **G.711MU, G.711A** and **G.729** for testing purposes with the IP endpoints.

```
display ip-codec-set 1                                        Page   1 of   2

                         IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.711A            n         2        20
 3: G.729             n         2        20
 4:
```

6.6. Administer Station Screen

This screen describes the **station** form setup for the IP telephone in Communication Manager as shown. The **Extension** used was **40125** with phone **Type 9630**. The **Name** of the phone was set to **VPN test** and the **IP SoftPhone** parameter was set to **yes.** All other values on **Page 1** of the station form were left as default.

```
display station 40125                                        Page   1 of   5
                                   STATION

Extension: 40125                       Lock Messages? n               BCC: 0
     Type: 9630                        Security Code:                  TN: 1
     Port: S00010                    Coverage Path 1:                 COR: 1
     Name: VPN test                  Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19           Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 40030
           Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                                        IP Video? n
```

7. Verification Steps

The following verification steps were tested using the sample configuration.

From Communication Manager, verify the IP telephones registered to Communication Manager as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
40020         9640      IP_Phone    y  10.10.99.11
              1         3.1000         135.64.186.81
40125         9640      IP_Phone    y  10.10.25.40
              1         3.1000         135.64.186.81
40126         9630      IP_Phone    y  10.10.25.41
              1         3.1000         135.64.186.81
```

Verify calls can be made with clear audio from the Avaya VPN telephone to a second VPN telephone. The VPN telephone extension 40125 registered with IP Address 10.10.25.40 and VPN telephone extension 40126 registered with IP Address 10.10.25.41. Verify the calls are seen to be active within Communication Manager. Verify supplementary features such as Call Hold, Call Forward, Conference and Transfer can be completed between the Avaya endpoints.

```
status station 40125                                          Page   1 of   8
                            GENERAL STATUS
     Administered Type: 9630              Service State: in-service/off-hook
        Connected Type: 9630          TCP Signal Status: connected
             Extension: 40126

status station 40126                                          Page   4 of   8
                              CALL CONTROL SIGNALING
Port: S00025         Switch-End IP Signaling Loc: PROCR    H.245 Port:
            IP Address                                 Port  Node Name       Rgn
Switch-End: 135.64.186.81                              61444                 1
   Set End: 10.10.25.40                                 1720                  1
H.245 Near:
 H.245 Set:

status station 40126                                          Page   5 of   8

                          AUDIO CHANNEL Port: S00025
G.711MU       Switch-End Audio Location:
            IP Address                                 Port  Node Name       Rgn
Other-End: 10.10.25.41                                  2192                  1
  Set-End: 10.10.25.40                                  3034                  1
Audio Connection Type: ip-direct
```

8. Conclusion

These Application Notes describe the administration steps required to configure an Avaya 9600 IP Telephone VPN feature for Certificate Authentication using Cisco Adaptive Appliance and Microsoft Certificate Authority with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services running on Avaya Aura™ Midsize Enterprise Single Server.

9. Additional References

This section references the Avaya documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] Cisco Security Appliance Configuration Guide using ASDM 5.2 Configuring Certificates, available at http://www.cisco.com

[2] Selected ASDM VPN Configuration Procedures for the Cisco ASA 5510 Series, Version 5.2, available at http://www.cisco.com

[3] VPN Setup Guide for 9600 Series IP Telephones Release 3.1, November 2009, Document Number 16-602968

[4] Administering Avaya Aura™ Communication Manager, Document Number 03-300509

[5] Catalyst 3750 Switch Software Configuration Guide 12.2(35) SE Configuring VoiceVLANs, available at www.cisco.com

[6] Configuring 802.1Q Trunking between a Catalyst 3550/3560/3570 and Catalyst Switches that run Cisco IOS software, available at www.cisco.com

Appendix A

Cisco 5510 Adaptive Security Appliance Configuration File

The Cisco 5510 Adaptive Security Appliance was configured using Adaptive Security Device Manager software. The configuration highlighted in bold shows the configuration of the VPN settings explained in **Section 4**.

ASA Version 7.21
hostname Cisco5510
domain-name cisco5510.silstack.com
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
interface Ethernet0/0
nameif inside
security-level 100
ip address 135.64.186.13 255.255.255.224
interface Ethernet0/1
nameif outside
security-level 100
ip address 172.16.1.5 255.255.0.0
interface Ethernet0/2
no nameif
no security-level
no ip address
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
boot system disk0:/asa721-k8.bin
ftp mode passive
dns domain-lookup inside
dns domain-lookup management
dns server-group DefaultDNS
domain-name cisco5510.silstack.com
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list inside.200_access_in extended permit icmp any any
access-list inside_access_in extended permit icmp any 135.64.186.0 255.255.255.224

access-list inside_access_in extended permit ip any ippool_anycoonect 255.255.255.0
access-list outside_access_in extended permit icmp any 172.16.1.0 255.255.255.0
access-list inside_access_in_1 remark test inside mgmt
access-list inside_access_in_1 extended permit ip any any
access-list inside_nat0_outbound extended permit ip ippool_anycoonect 255.255.255.0 any
access-list Inside_nat0_outbound extended permit ip any 10.10.25.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any 10.10.25.0 255.255.255.128
access-list outside_cryptomap extended permit ip any 10.10.25.0 255.255.255.128
pager lines 24
logging enable
logging asdm debugging
mtu inside 1500
mtu outside 1500
mtu management 1500
ip local pool vpnphone-ip-pool 10.10.25.40-10.10.25.80 mask 255.255.255.0
icmp unreachable rate-limit 1 burst-size 1
icmp permit any management
asdm image disk0:/asdm-521.bin
asdm history enable
arp timeout 14400
nat (inside) 0 access-list Inside_nat0_outbound
nat (inside) 101 0.0.0.0 0.0.0.0
nat (management) 0 0.0.0.0 0.0.0.0
access-group inside_access_in in interface inside
route inside 0.0.0.0 0.0.0.0 135.64.186.1 1
dynamic-access-policy-record DfltAccessPolicy
nac-policy DfltGrpPolicy-nac-framework-create nac-framework
default-acl unused
reval-period 36000
sq-period 300
http server enable
http 172.16.1.0 255.255.255.0 management
http 135.64.186.0 255.255.255.0 management
http 135.64.0.0 255.255.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac

crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set TUNNEL_ESP_AES-128_SHA esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 40 set pfs
crypto dynamic-map Outside_dyn_map 40 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 60 set pfs
crypto dynamic-map Outside_dyn_map 60 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 80 set pfs
crypto dynamic-map Outside_dyn_map 80 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 100 set pfs
crypto dynamic-map Outside_dyn_map 100 set transform-set ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 20 set transform-set TUNNEL_ESP_AES-128_SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map
crypto map outside_map 65535 ipsec-isakmp dynamic
crypto map outside_map0 20 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map0 interface outside
crypto ca trustpoint certificate
enrollment url http://135.64.186.207:80/certsrv/mscep/mscep.dll
password *
keypair keypair01
crl configure
no protocol http
no protocol ldap
crypto ca certificate map scep_vpnphone 10
crypto ca certificate map DefaultCertificateMap 10
subject-name attr cn co 00-1b-4f
crypto ca certificate chain certificate
certificate ca 29a52eb91e363e98409640e72b2e9ffd
30820384 3082026c a0030201 02021029 a52eb91e 363e9840 9640e72b 2e9ffd30
0d06092a 864886f7 0d010105 0500301a 31183016 06035504 03130f31 33352e36
342e3232 2e373620 4341301e 170d3039 30393032 31393230 35385a17 0d313430
39303231 39323035 385a301a 31183016 06035504 03130f31 33352e36 342e3232
2e373620 43413082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082
010a0282 010100ad 14014058 52ac4133 99b734b9 f1620594 1a32be3c a5f6c68c
c77dd51e 1de2e169 3ab039c7 21069c22 678db430 c08856c6 9dd4ca5e 87ff54cb
0aa551a6 d4242c07 910cb5ec 1bb3d509 c7ce7c61 14e533b4 fadccfe6 a4b052d3
d48db972 6888425e f5894d9f 733b189f 6a0be646 d8d435fa 6bcbd40b be79ac75
18caecee 2c4a888e 1f549f73 4cd1d546 37df7944 241f82bc 49b32a1b 07f50778
3c5dde1f fb3c8716 ebb645a4 1299ac53 76100c7a d66805fc 577bb5e2 c3a87894
bc76cc1a 77a73da7 778f510c 3aa7b535 54764e91 01685e4b 5e1e84c2 b1b47d64
dc085a52 8a351735 95ce7f99 8b995436 7cead122 30341cf8 4af156b9 f8e2d367
9fe1fd0e 8c283902 03010001 a381c530 81c2300b 0603551d 0f040403 02018630

0f060355 1d130101 ff040530 030101ff 301d0603 551d0e04 160414dd 6cf6f948 096d0094 65e8ca46 0b07d2ef 21936d30 71060355 1d1f046a 30683066 a064a062 862f6874 74703a2f 2f617372 2d747473 2f436572 74456e72 6f6c6c2f 3133352e 36342e32 322e3736 25323043 412e6372 6c862f66 696c653a 2f2f5c5c 6173722d 7474735c 43657274 456e726f 6c6c5c31 33352e36 342e3232 2e373620 43412e63 726c3010 06092b06 01040182 37150104 03020100 300d0609 2a864886 f70d0101 05050003 82010100 2a8ec8be b002ef89 d4fbad2a 93c8eeed 6fc14f2e fcea98b4 e2ccdced 94189e7a f0ab90da 0f4b9f2b 01e7d175 75757b1c a6ad9322 21f558fa f66c0098 58f93982 97a7c32f ec7ef3ea 284607cb 60cbaa35 d9042060 02475754 7ec1a245 56900b59 4f6ab0fb ac0c01b0 e51265f6 a2bd0df0 53e0f62c 6647c442 cf9387f2 5bb4cb28 43f38fd3 636f3443 5068d82a 5b1c8246 c90fa637 4830c4d5 f73b347d 06f65fbd d043608b 377f11ea 4e7f4c14 812a2e6e 944ccc44 8651ae29 19e38869 a2085bd0 9eef0ac8 d01a8b53 8f7a6cc8 20e866f0 7f28bf4f a780e8e1 9645f60d bdeeb705 e1c3d263 e80836ac 4d14b5a3 bde3f3bb 74b56079 39bce91d ec65839a c94f18e9

quit
crypto isakmp enable inside
crypto isakmp enable outside
crypto isakmp enable management
crypto isakmp policy 1
authentication rsa-sig
encryption 3des
hash md5
group 2
lifetime 86400
crypto isakmp policy 30
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400
no crypto isakmp nat-traversal
client-update enable
telnet timeout 5
ssh timeout 5
console timeout 0
management-access inside
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
webvpn
enable outside
svc image disk0:/sslclient-win-1.1.4.179.pkg 1
svc enable
tunnel-group-list enable
group-policy DfltGrpPolicy attributes
vpn-idle-timeout 3

vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
nac-settings value DfltGrpPolicy-nac-framework-create
webvpn
svc keepalive none
svc dpd-interval client none
svc dpd-interval gateway none
svc compression deflate
customization value DfltCustomization
group-policy GrpPolicyAnyConnect internal
group-policy GrpPolicyAnyConnect attributes
vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
webvpn
url-list none
group-policy GroupPolicy1 internal
group-policy VPNPHONE internal
group-policy VPNPHONE attributes
dns-server value 135.64.186.207
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-session-timeout none
vpn-tunnel-protocol IPSec
default-domain value cisco5510.silstack.com
group-policy vpnphone internal
group-policy vonphone internal
group-policy vonphone attributes
vpn-tunnel-protocol IPSec
vpn-group-policy GrpPolicyAnyConnect
username vpnphone password FnqTF5SUU/uCoIrj encrypted privilege 0
username vpnphone attributes
vpn-group-policy vpnphone
vpn-group-policy VPNPHONE
vpn-group-policy VPNPHONE
tunnel-group DefaultRAGroup general-attributes
address-pool vpnphone-ip-pool
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool vpnphone-ip-pool
default-group-policy GrpPolicyAnyConnect
tunnel-group vpnphone type remote-access
tunnel-group vpnphone general-attributes
address-pool vpnphone-ip-pool
tunnel-group vpnphone ipsec-attributes
trust-point certificate
default-group-policy GrpPolicyAnyConnect
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id

```
no tunnel-group-map enable peer-ip
tunnel-group-map default-group vpnphone
tunnel-group-map scep_vpnphone 10 vpnphone
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
imap4s
default-group-policy DfltGrpPolicy
authentication aaa
pop3s
default-group-policy DfltGrpPolicy
 authentication aaa
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com