



# Nokia Mobile VPN

How to Configure Nokia Mobile  
VPN for Nokia IP VPN  
with Certificate Authentication

**NOKIA**

**Nokia for Business**

## Table of Contents

Introduction.....	3
Configuring remote client access using Certificate Authentication by NVM .....	4
Import external CA to Nokia IP VPN.....	4
Create device certificate for Nokia IP VPN gateway .....	5
Create device certificate for Nokia IP VPN gateway .....	6
Create VPN policy for certificate users .....	10
Define protected networks for Certificate Authentication user policy.....	11
Define authentication method for certificate user policy.....	12
Configuring the IPsec Client to use Internal Addressing.....	13
Configuring the IPsec Client to use internal DNS server.....	14
Create a remote client profile and policy for Certificate Authentication .....	15
Policy creation with Policy Tool using exported CA certificate .....	17

# Introduction

This best-practices document describes how to manually configure Nokia Mobile VPN Client (without a separate device management product) using the Certificate Authentication (CA) method in Nokia IP VPN v6.3 environments. For further details on how to use Nokia Mobile VPN Client, error code documents, and the policy format document, please see <http://www.nokiaforbusiness.com/> > Security products > Nokia Mobile VPN > Resources.

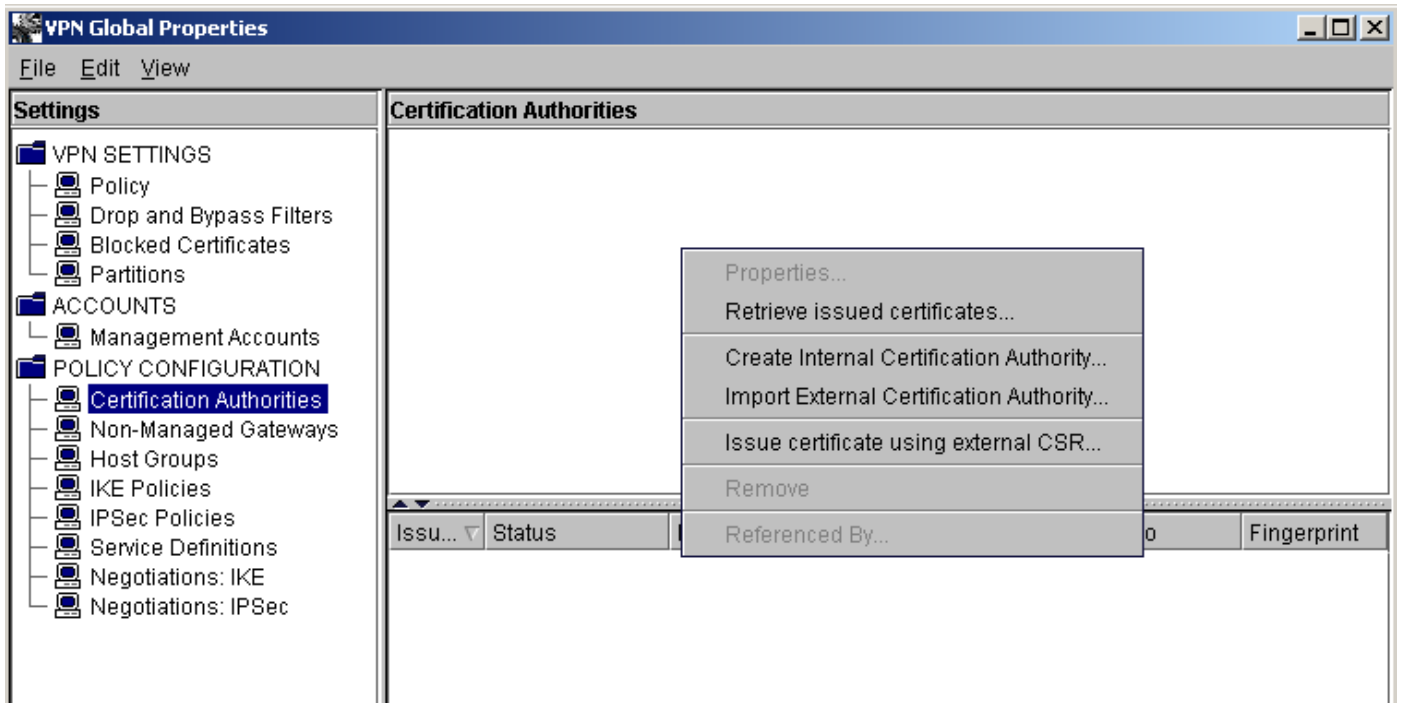
The assumption is that Nokia IP VPN, Nokia VPN Manager software, and Mobile VPN Client have been installed, and all post-installation tasks have been completed before continuing with the steps listed below. Use Nokia VPN Manager (NVM) to configure the Nokia IP VPN gateway. Start the Nokia VPN Manager software and log on as the Administrator. After completing the steps detailed below, remember to save the configurations before exiting the tool. In this example, external CA is used to get certificates for Nokia IP VPN and Nokia Mobile VPN Client.

# Configuring remote client access using Certificate Authentication by NVM

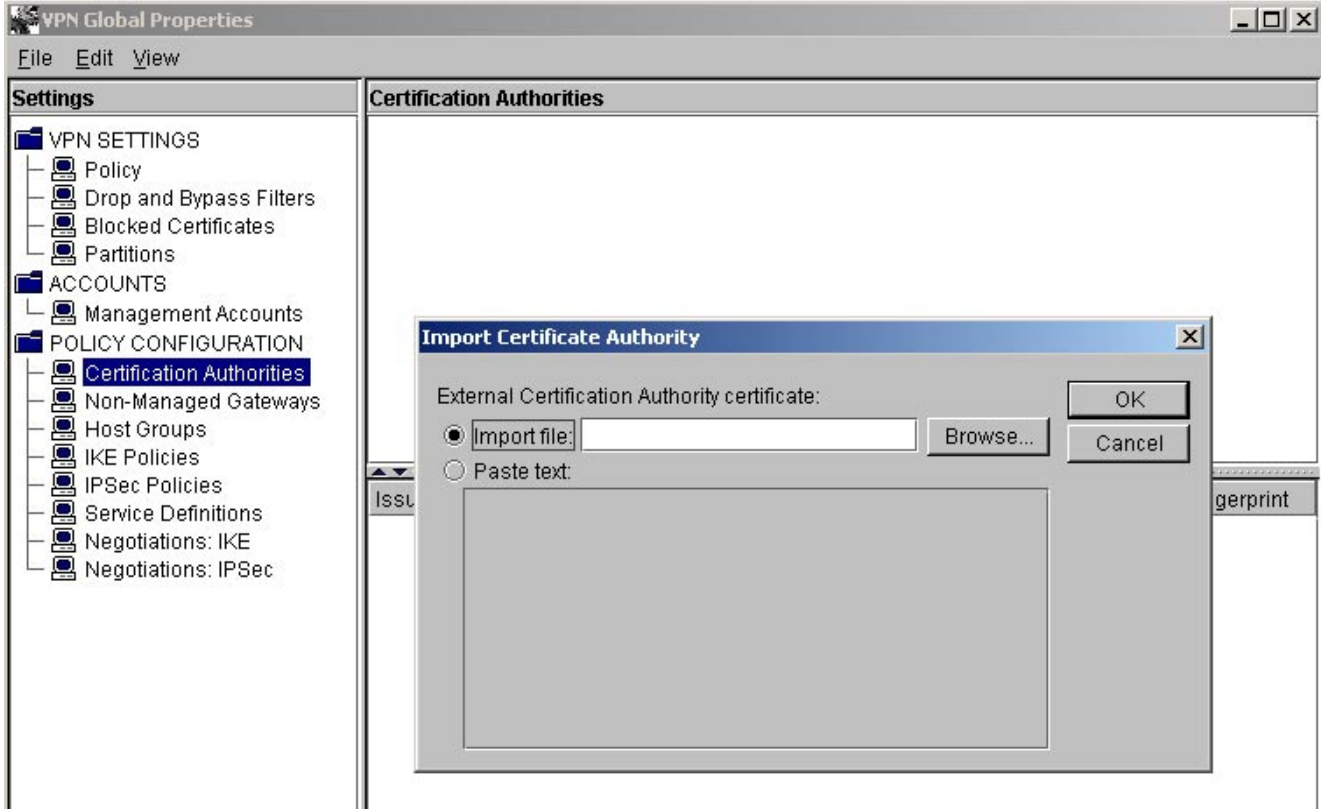
Import external CA to Nokia IP VPN

In this example, external CA is used to create certificates for Nokia IP VPN and Nokia Mobile VPN Client, so the first step is to import that external CA certificate to Nokia IP VPN:

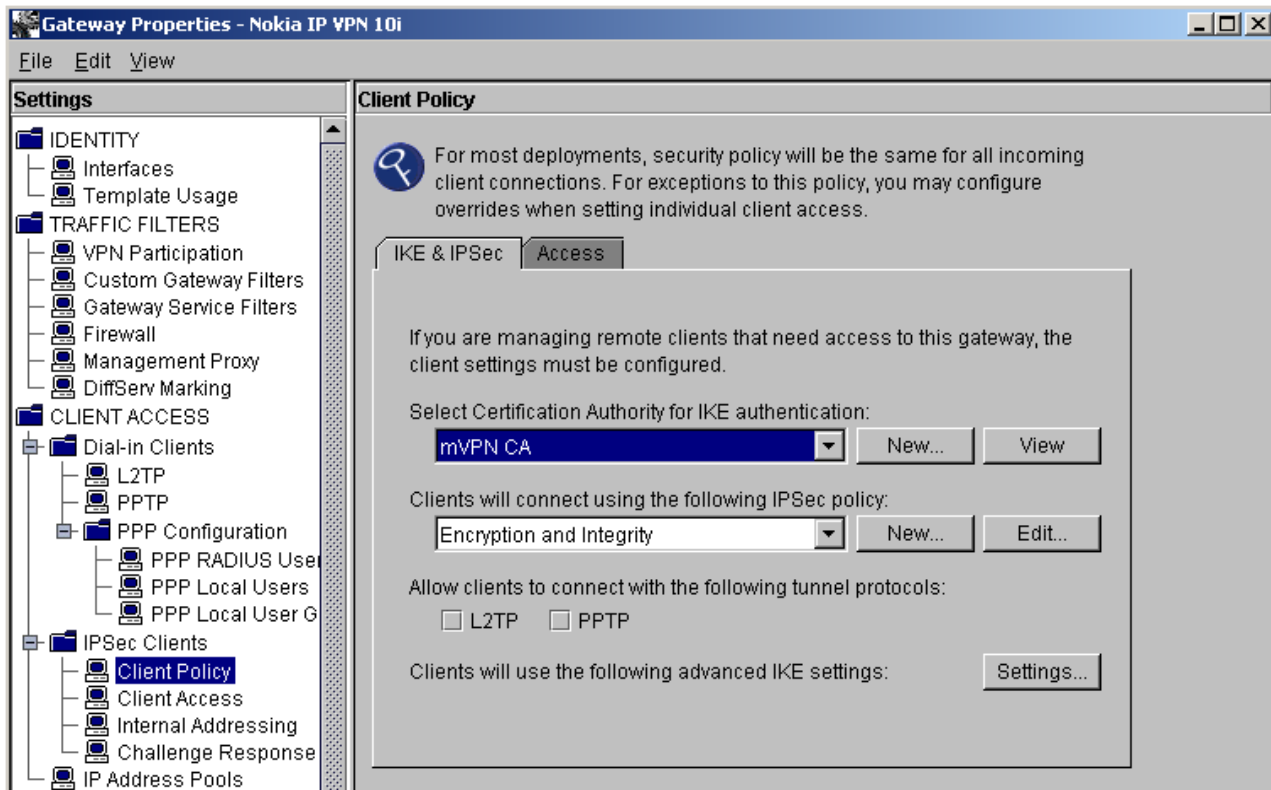
- Select POLICY CONFIGURATION -> Certificate Authorities -> Import External Certification Authority.



Select the CA certificate either by importing it via the Browse button or by dropping it to the Paste text dialog, and press OK. Select Action on the menu bar and Apply Changes to save the certificate settings to the Nokia IP VPN gateway.



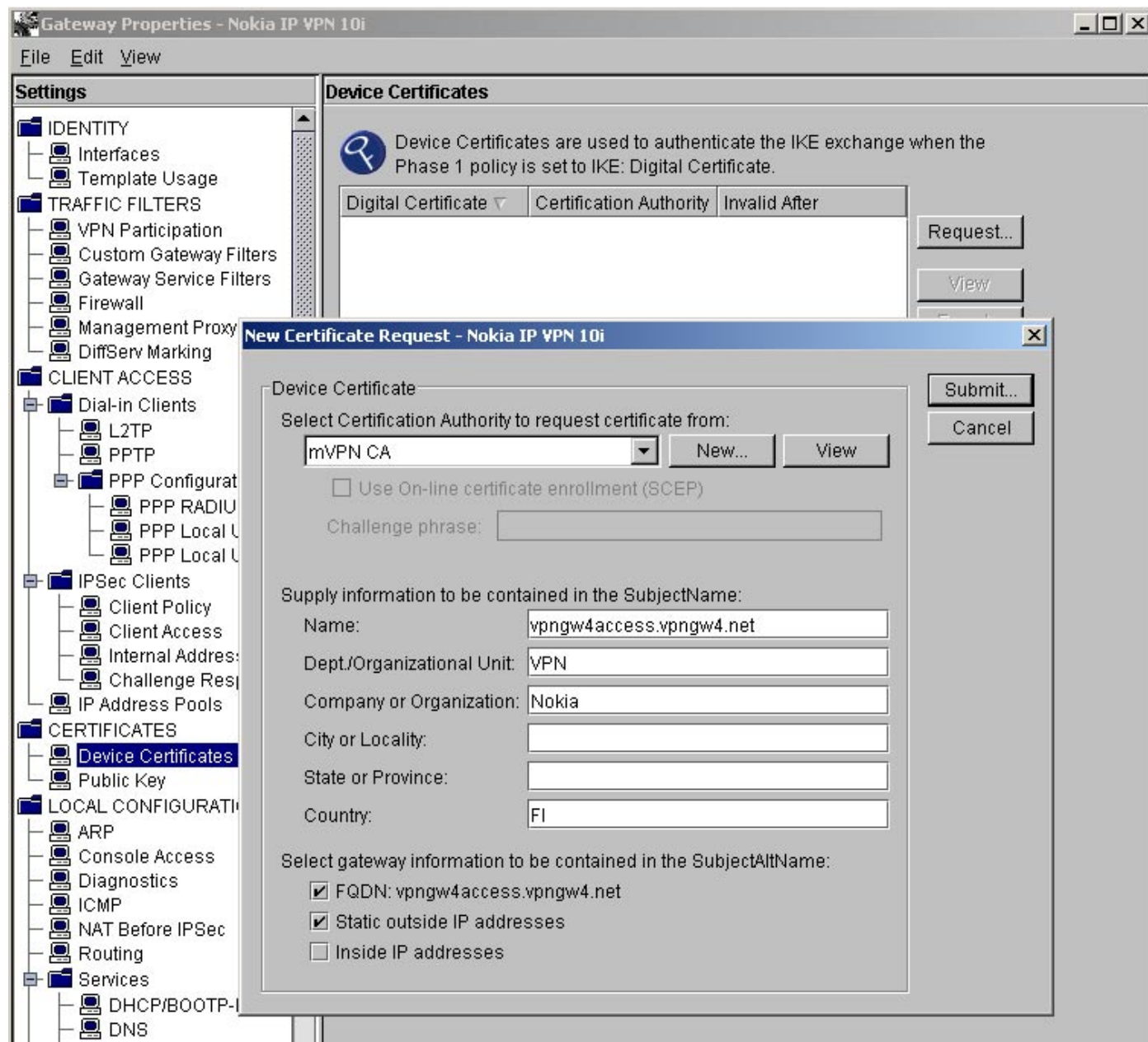
Go to the Client Policy dialog and select the imported CA certificate as the Certification Authority for IKE authentication.



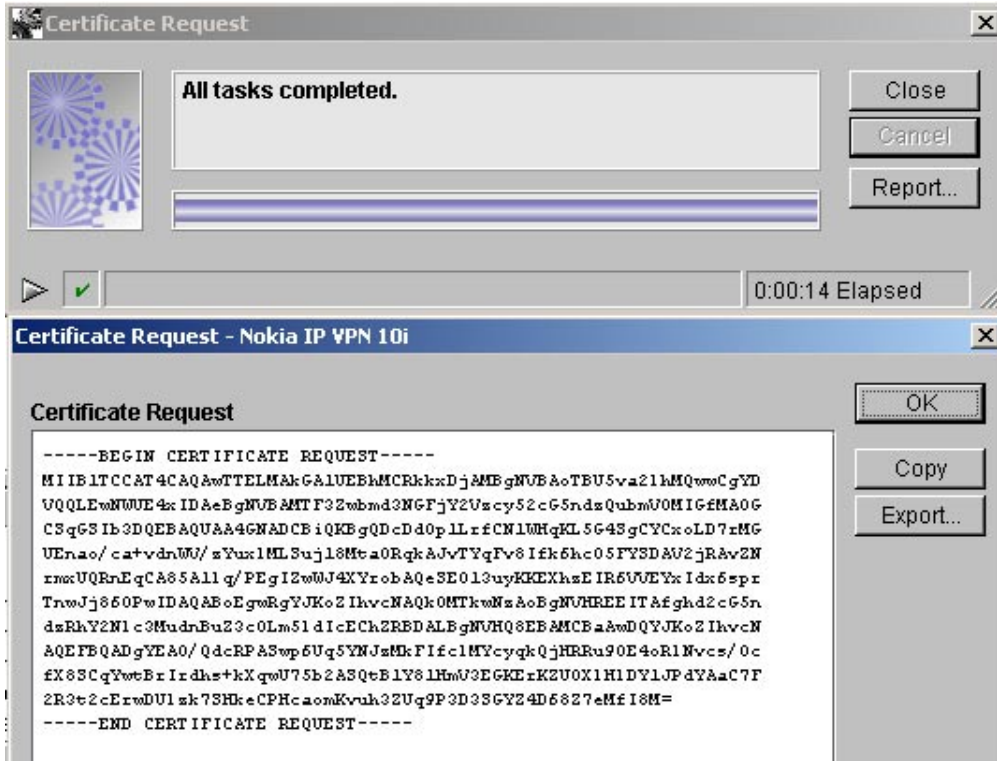
## Create device certificate for Nokia IP VPN gateway

Next, create the device certificate for the Nokia IP VPN gateway, if it has not already been created.

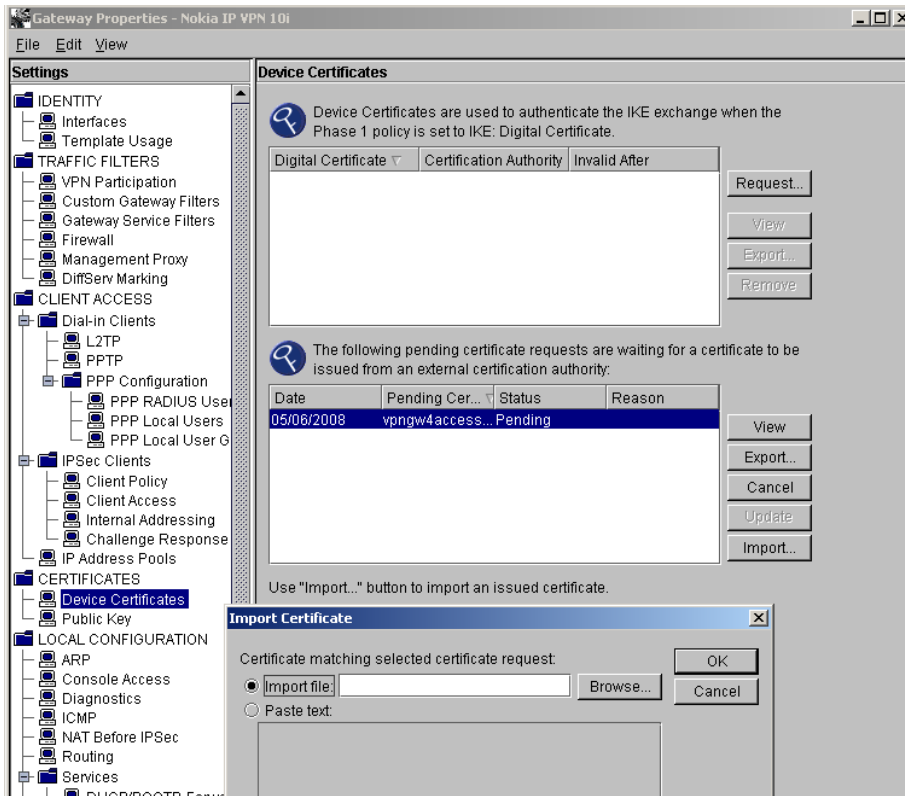
- Select Gateway Properties -> CERTIFICATES -> Device Certificates -> Request. In the "Select Certification Authority to request certificate from" field, select Imported CA Certificate. Supply the information needed in SubjectName and press Submit.
- Note: The SubjectAltName field must exist in the device certificate because it is used by the Nokia Mobile VPN Client.



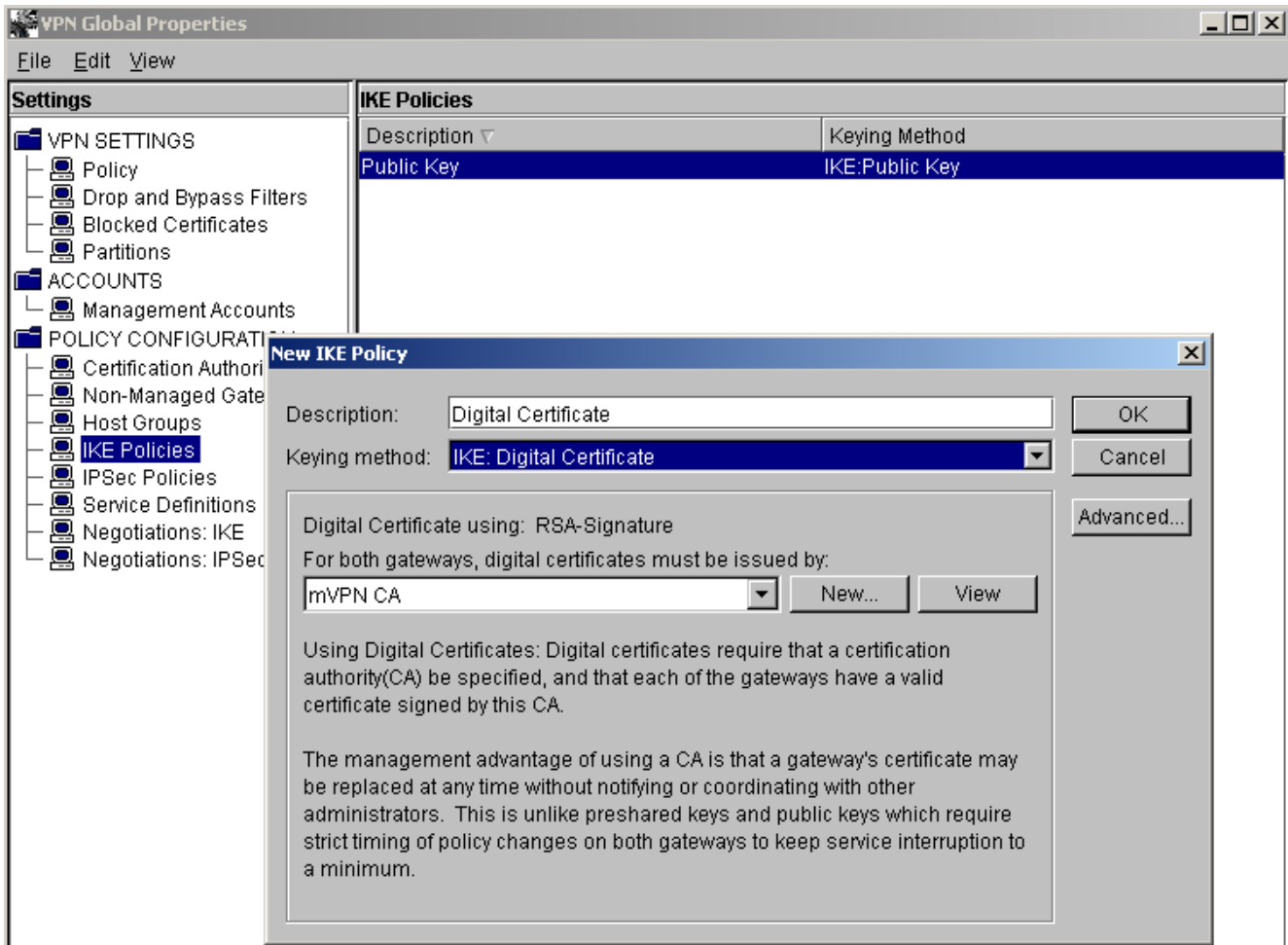
A new dialog is opened to save the certificate request. Save the request to the file and send it to the external CA for signing.



Once the certificate signing request is received back as a signed certificate, import it by pressing the Import button below the pending certificates window.

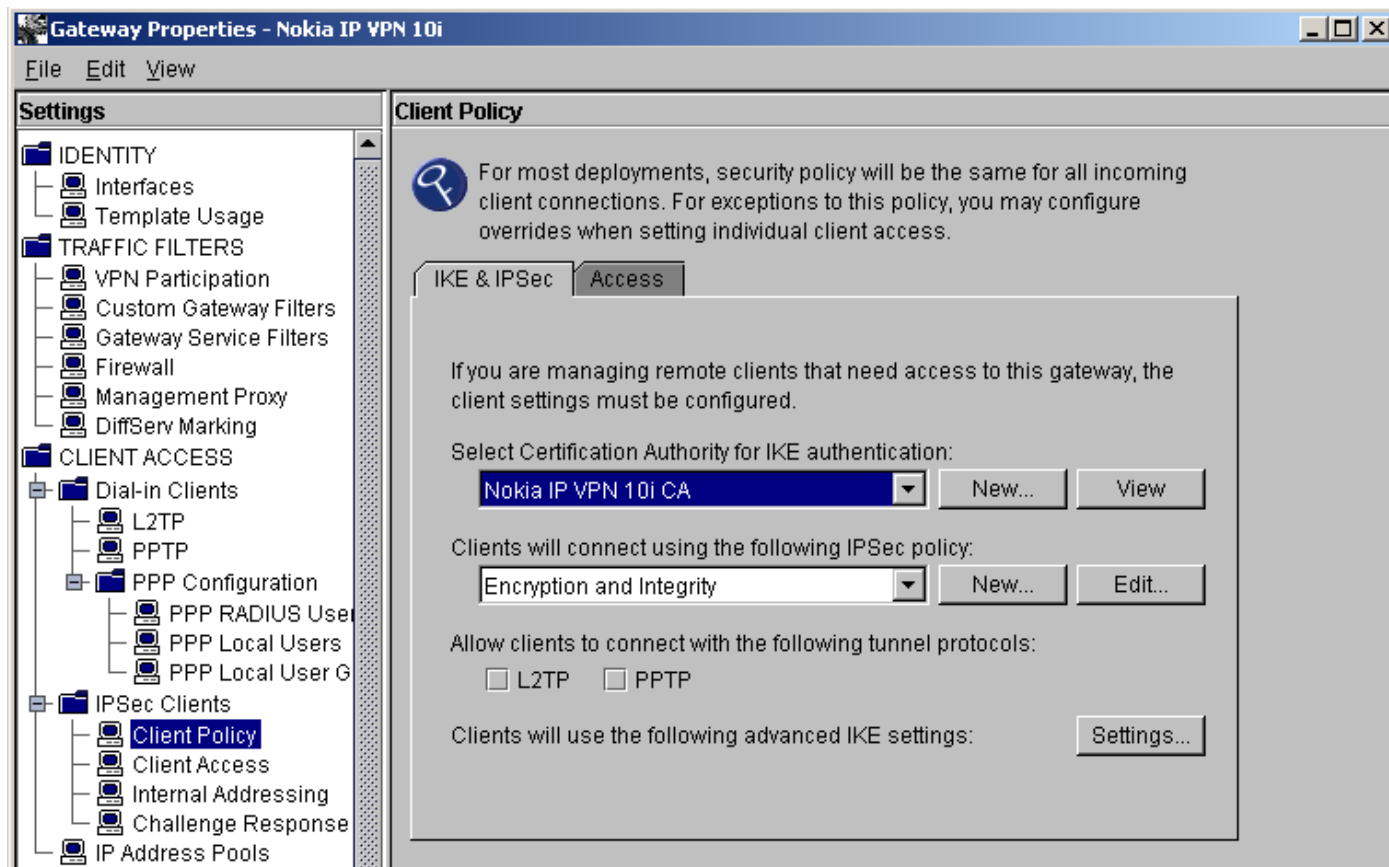


Check that in VPN Global Properties -> POLICY CONFIGURATION -> IKE Policies there is a Digital Certificate policy where the imported CA certificate is selected. Select Action on the menu bar and Apply Changes to save the certificate settings to the Nokia IP VPN gateway.



## Create VPN policy for certificate users

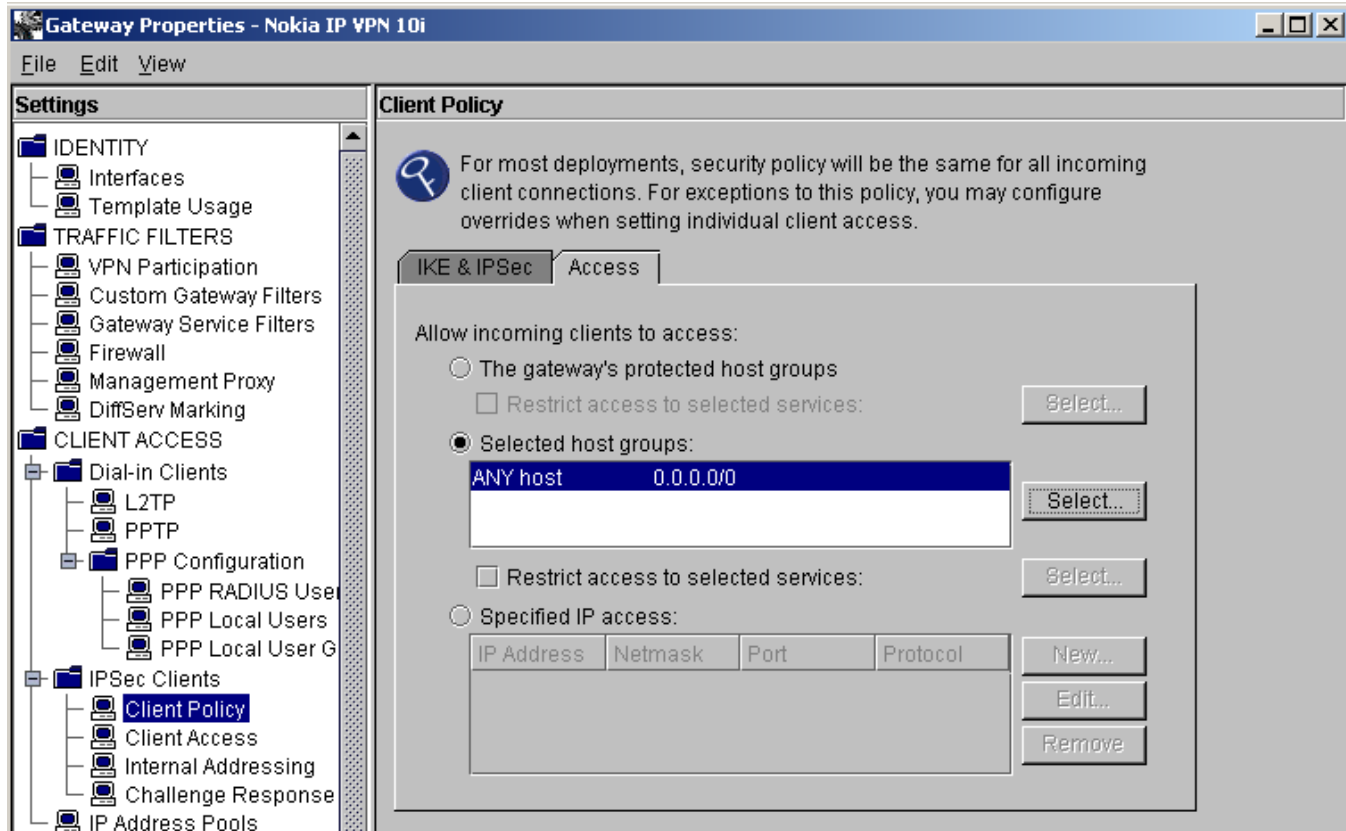
- Select Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Client Policy.
  - Select the imported CA as the Certification Authority for IKE authentication on the list.
  - Check the IPsec policy settings under “Clients will connect using the IPsec policy.” Default settings can be changed by selecting Edit or New.
  - The IKE policy settings for the Nokia Mobile VPN client policy can be changed from defaults in “Clients will use the following advanced IKE settings.”



## Define protected networks for Certificate Authentication user policy

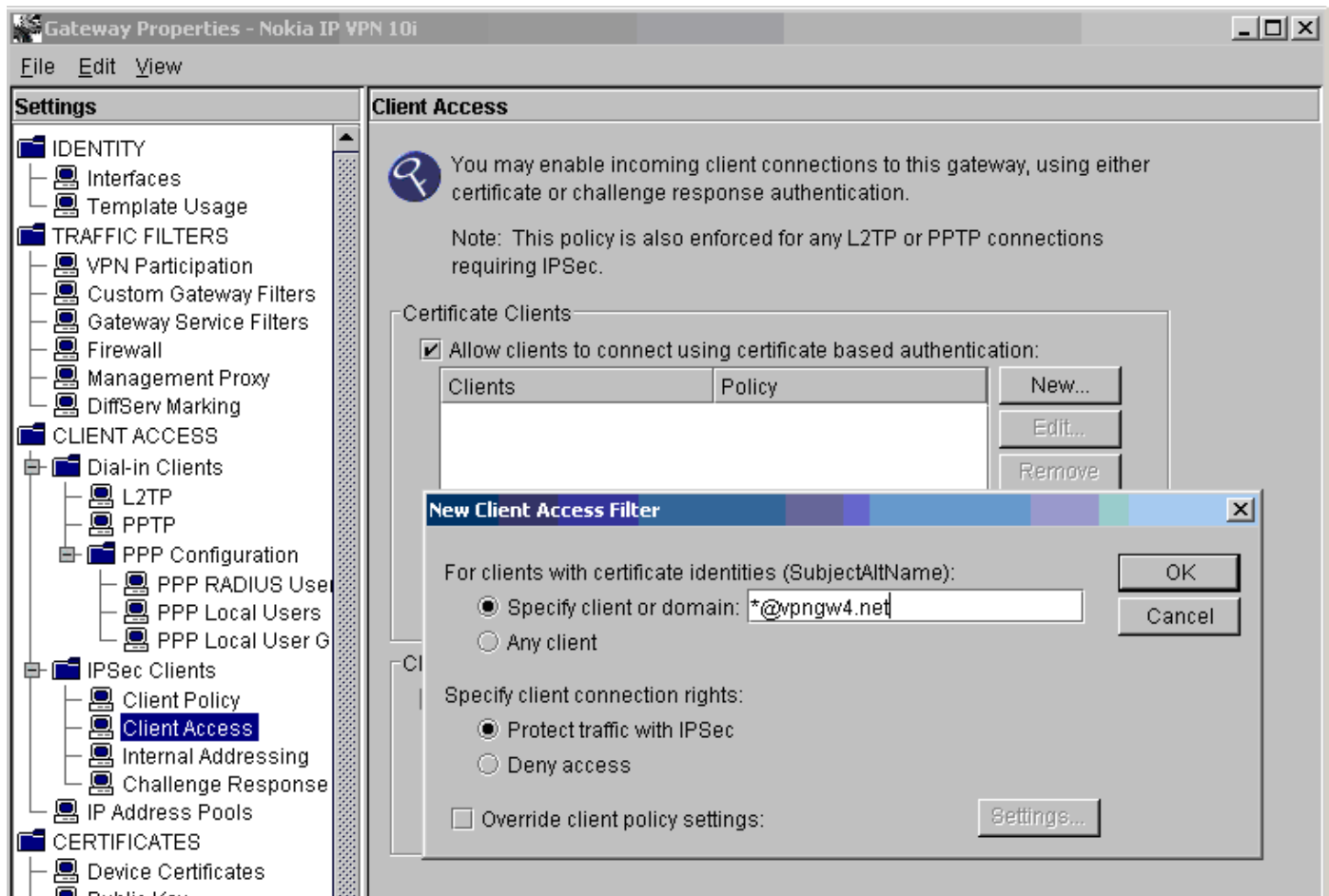
The protected network is defined either in VPN participation or under the Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Client Policy -> Access.

- **Either** define a predefined host group "ANY host" to the "Selected host groups" list,
- **Or** create protected host groups and select them. The default Nokia Mobile VPN Client Policy tool template used the "Any host" host group so if that is not changed, "ANY host" must be selected here, too.



## Define authentication method for certificate user policy

- Select Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Client policy -> IPsec Client -> Client Access.
- Check "Allow clients to connect using certificate based authentication" and press New.
- Define the filter to clients that are allowed access.

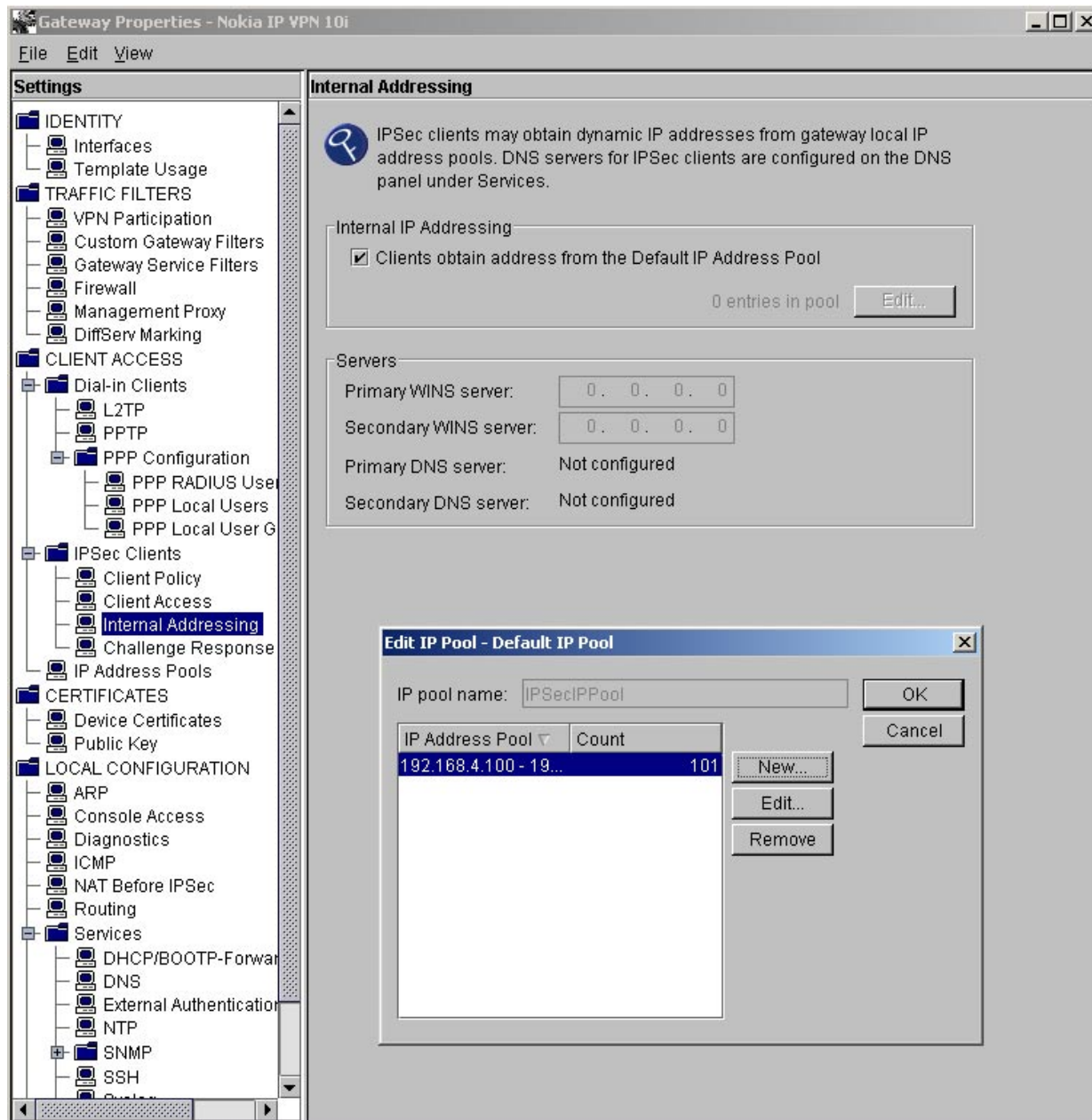


## Configuring the IPsec Client to use Internal Addressing

Select Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Internal Addressing.

- Check the box "Clients obtain address from the Default IP Address Pool. Select New to define the Internal Address Pool, press OK, and press OK again.

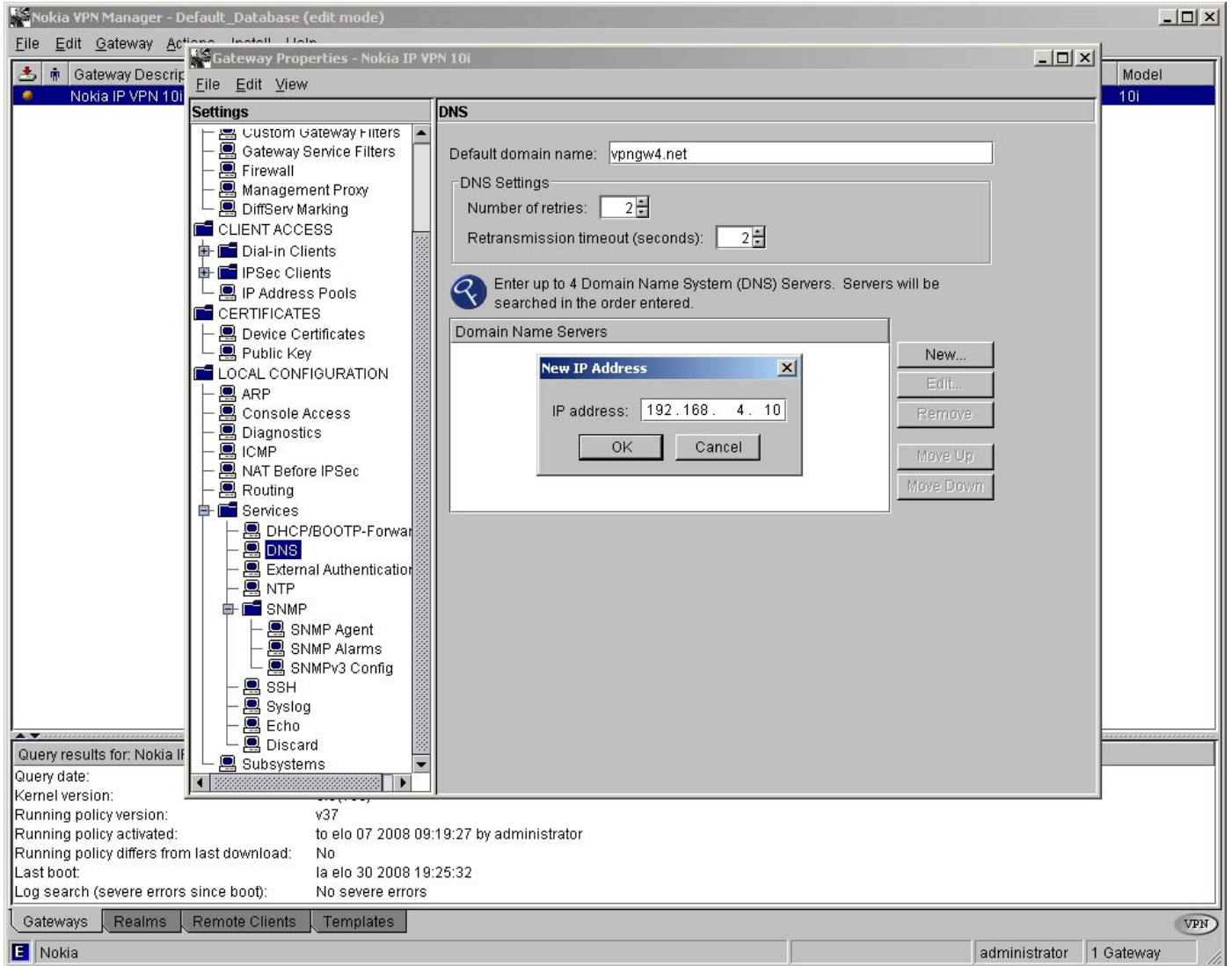
Note: Be sure to define an Internal Address pool that does not overlap with the subnets of physical interfaces. Also check to make sure that the routing has been properly configured for the Internal Address pool in the protected network.



## Configuring the IPsec Client to use internal DNS server

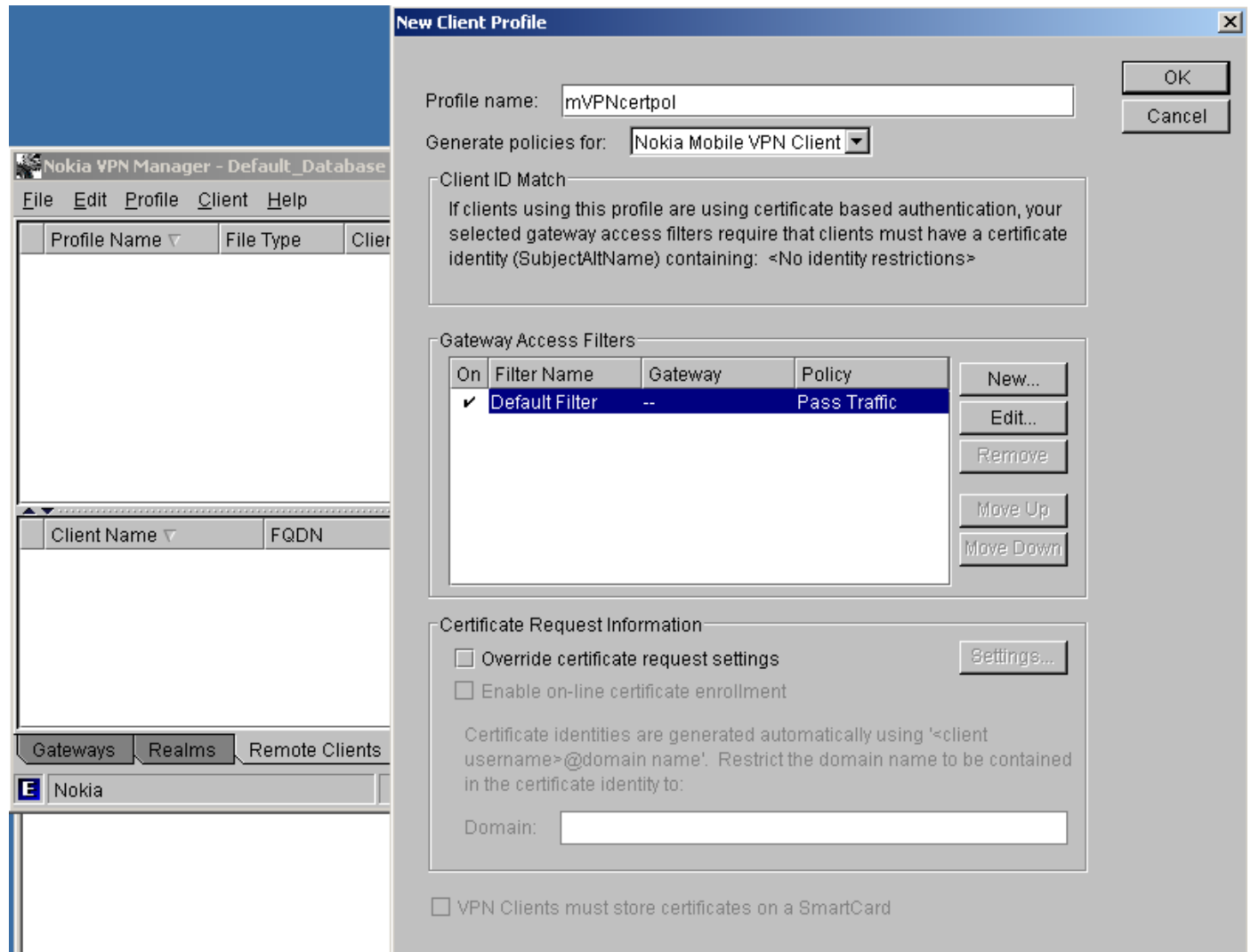
Select Gateway Properties -> Services -> DNS

- Click "New..." and enter the IP address of the internal DNS server. You can add multiple addresses if you have secondary DNS servers
- Click OK to close the "New IP Address" dialog.



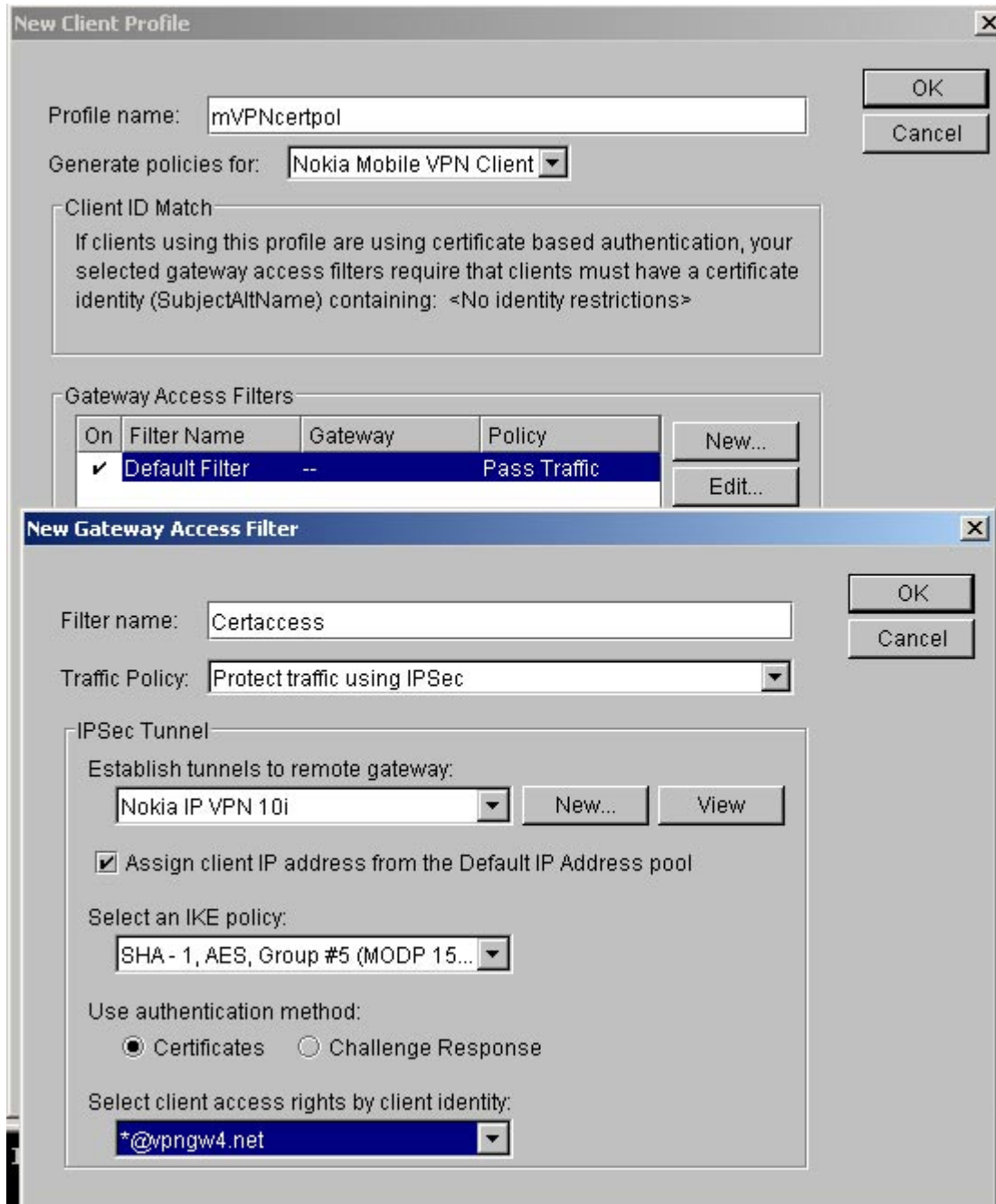
## Create a remote client profile and policy for Certificate Authentication

From the bottom of the VPN Manager, select the Remote Clients tab. Right-click and select New to create a profile.



Enter the name for the profile and select Nokia Mobile VPN Client in the "Generate policies for" list. Then select New in Gateway Access Filters. Enter the name for the filter and then check "Assign client IP address from the Default IP Address pool." Select the IKE policy from the list. In the Authentication method, select Certificates and choose the appropriate identity from "Select client access rights by client identity." Press OK, and then press OK again.

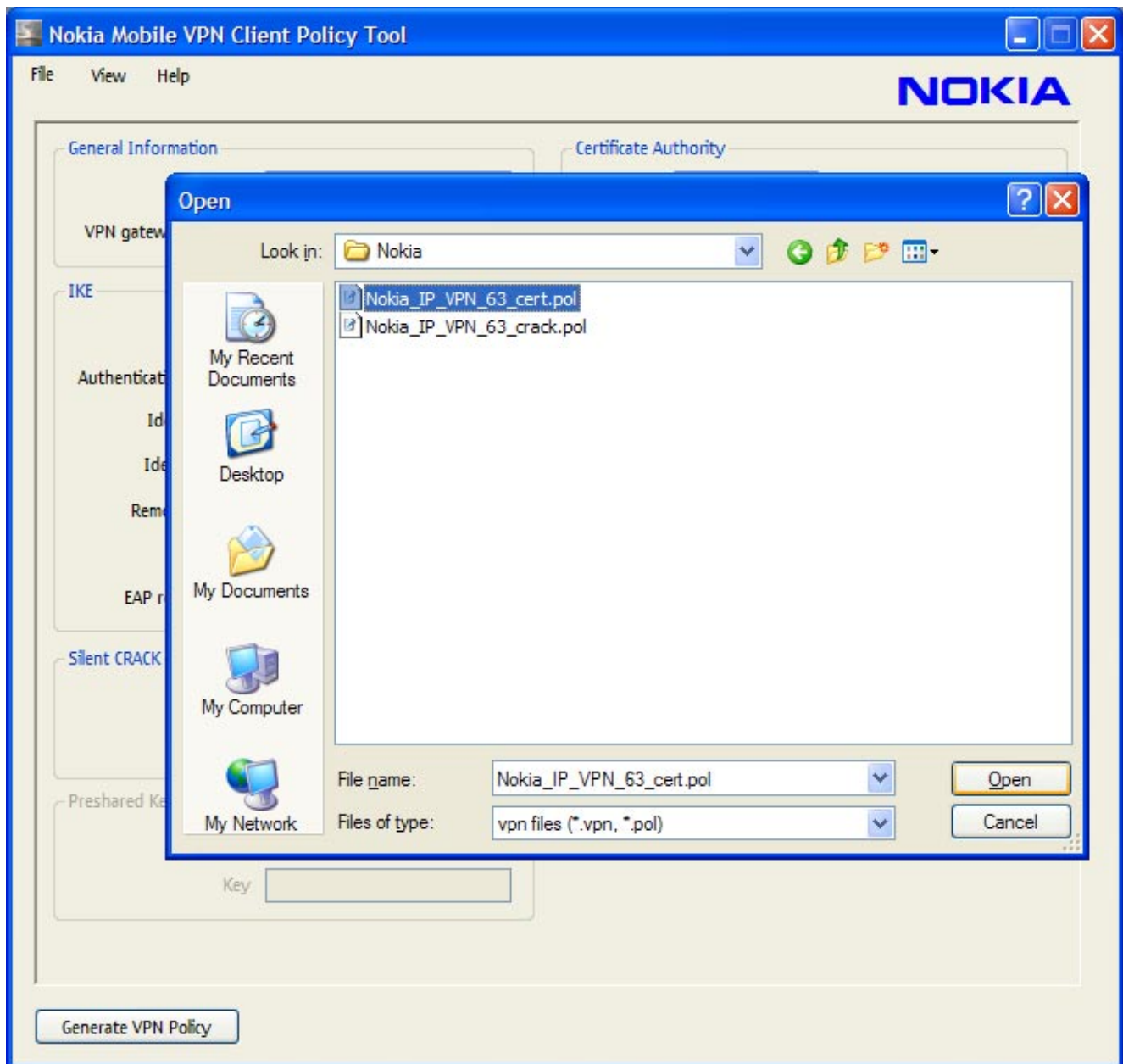
Select Action on the menu bar and Apply Changes to save the certificate to the Nokia IP VPN gateway and to finish the gateway configuration.



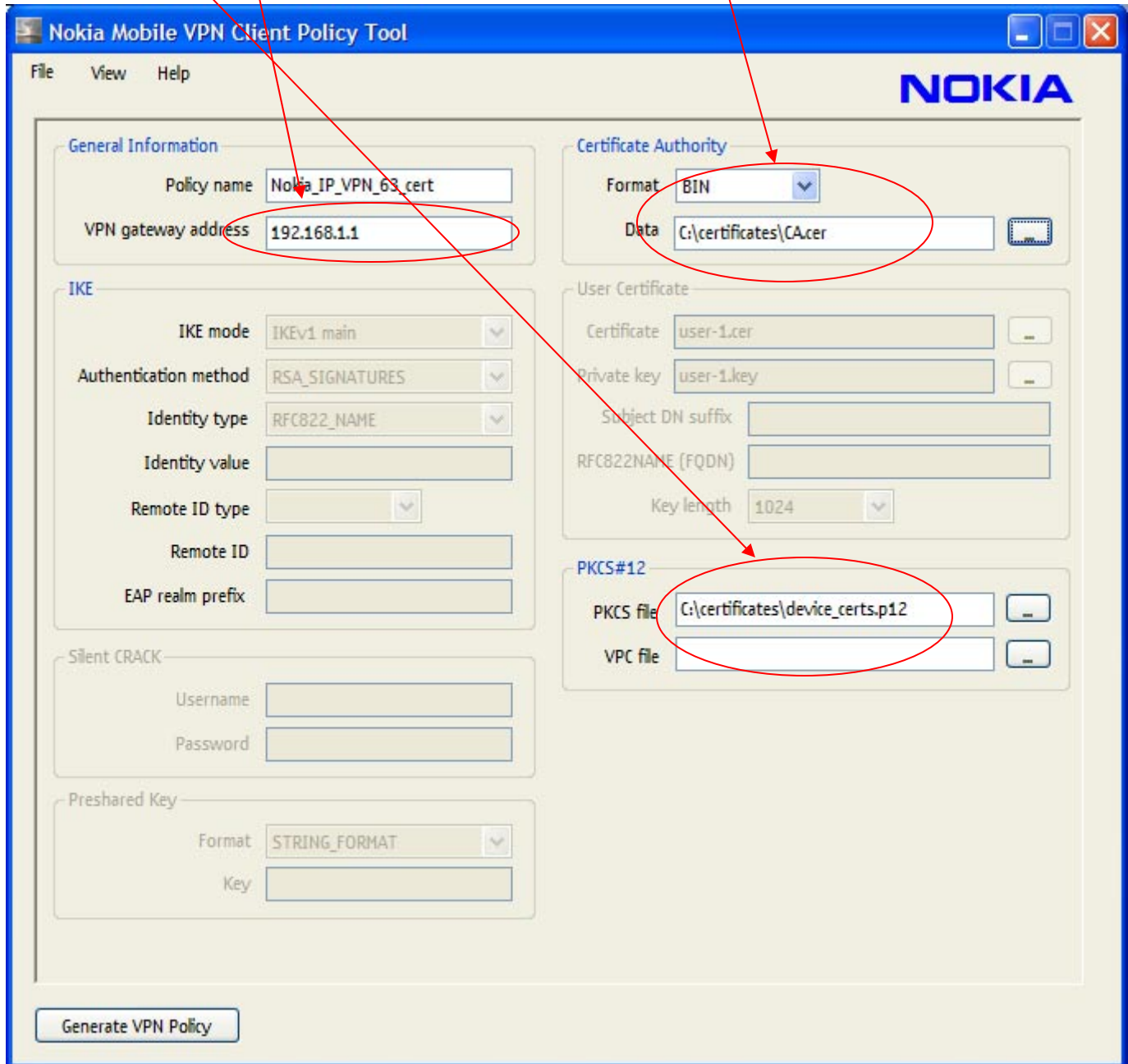
# Policy creation with Policy Tool using exported CA certificate

Before the Nokia Mobile VPN Client policy can be created, a device certificate and CA certificate for Nokia Mobile VPN Client must be available. In this example, the PKCS#12 packet is used to deliver the device certificate, and the CA certificate is delivered separately in its own file.

Start Nokia VPN Client Policy Tool and press the Load Template button. Select the Nokia\_IP\_VPN\_63\_cert.pol policy from the Nokia directory.



Add the correct VPN gateway address and get the path to your CA certificate (not needed if the CA certificate is part of the PKCS#12 packet). Make sure that the Format in Certificate Authority selection is set to BIN. Do the same to the PKCS#12 packet. If silent authentication is desired (the PIN code for the certificate is not requested), this option needs to be activated from the Advanced View. Go to Advanced View, open the IKE tree, and select "Cert store" to be DEVICE instead of USER. Note that only selected S60 3<sup>rd</sup> Edition, Feature Pack 1 devices support Device store. See the release note for more information.



To export the VPN policy, press the Generate VPN Policy button, and store Nokia\_IP\_VPN\_cert.vpn to your PC. Consult the *Nokia Mobile VPN Client User's Guide*, Chapter 6.1, for details on how to install a given policy file to your device.

## Legal Notice

Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Nokia and Nokia Connecting People are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

Nokia operates a policy of continuous development. Nokia reserves the right to make changes and improvements to any of the products described in this document without prior notice.

Under no circumstances shall Nokia be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Nokia reserves the right to revise this document or withdraw it at any time without prior notice.

## Work together. Smarter.

**Nokia Inc.** 102 Corporate Park Drive, White Plains, NY 10604 USA

**Americas** Tel: 1 877 997 9199 • Email: [usa@nokiaforbusiness.com](mailto:usa@nokiaforbusiness.com)

**Asia Pacific** Tel: +65 6588 33 64 • Email: [asia@nokiaforbusiness.com](mailto:asia@nokiaforbusiness.com)

**Europe** France +33 170 708 166 • UK +44 161 601 8908 • Email: [europa@nokiaforbusiness.com](mailto:europa@nokiaforbusiness.com)

**Middle East and Africa** Dubai +971 4 3697600 • Email: [mea@nokiaforbusiness.com](mailto:mea@nokiaforbusiness.com)

[www.nokiaforbusiness.com](http://www.nokiaforbusiness.com)

© 2008 Nokia. All rights reserved. Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other trademarks mentioned are the property of their respective owners. Nokia operates a policy of continuous development, therefore, reserves the right to make changes and improvements to any of the products described in this document without prior notice.

# NOKIA

**Nokia for Business**