

Nokia Mobile VPN

How to Configure Nokia
Mobile VPN for the Nokia IP
VPN Gateway with *Challenge-
Response Authentication*

NOKIA

Nokia for Business

Table of Contents

Introduction.....	3
Configuring remote client access using Challenge-Response authentication by NVM	4
Create an internal CA in Nokia IP VPN	4
Create device certificate for Nokia IP VPN gateway	4
Create device certificate for Nokia IP VPN gateway	5
Create VPN policy for Challenge-Response users	6
Define protected networks for Challenge-Response Authentication user policy.....	7
Define authentication method for Challenge-Response user policy	8
Configuring IPsec Client to use Internal Addressing	9
Configuring the IPsec Client to use internal DNS server.....	10
Create a user name/password for Challenge-Response users.....	10
Create a user name/password for Challenge-Response users.....	11
Create a remote client profile and policy for Challenge-Response authentication	12
Policy creation with Policy Tool using exported CA certificate	14

Introduction

This best-practices document describes how to configure Nokia Mobile VPN Client manually (without a separate device management product) using a Challenge-Response authentication 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.

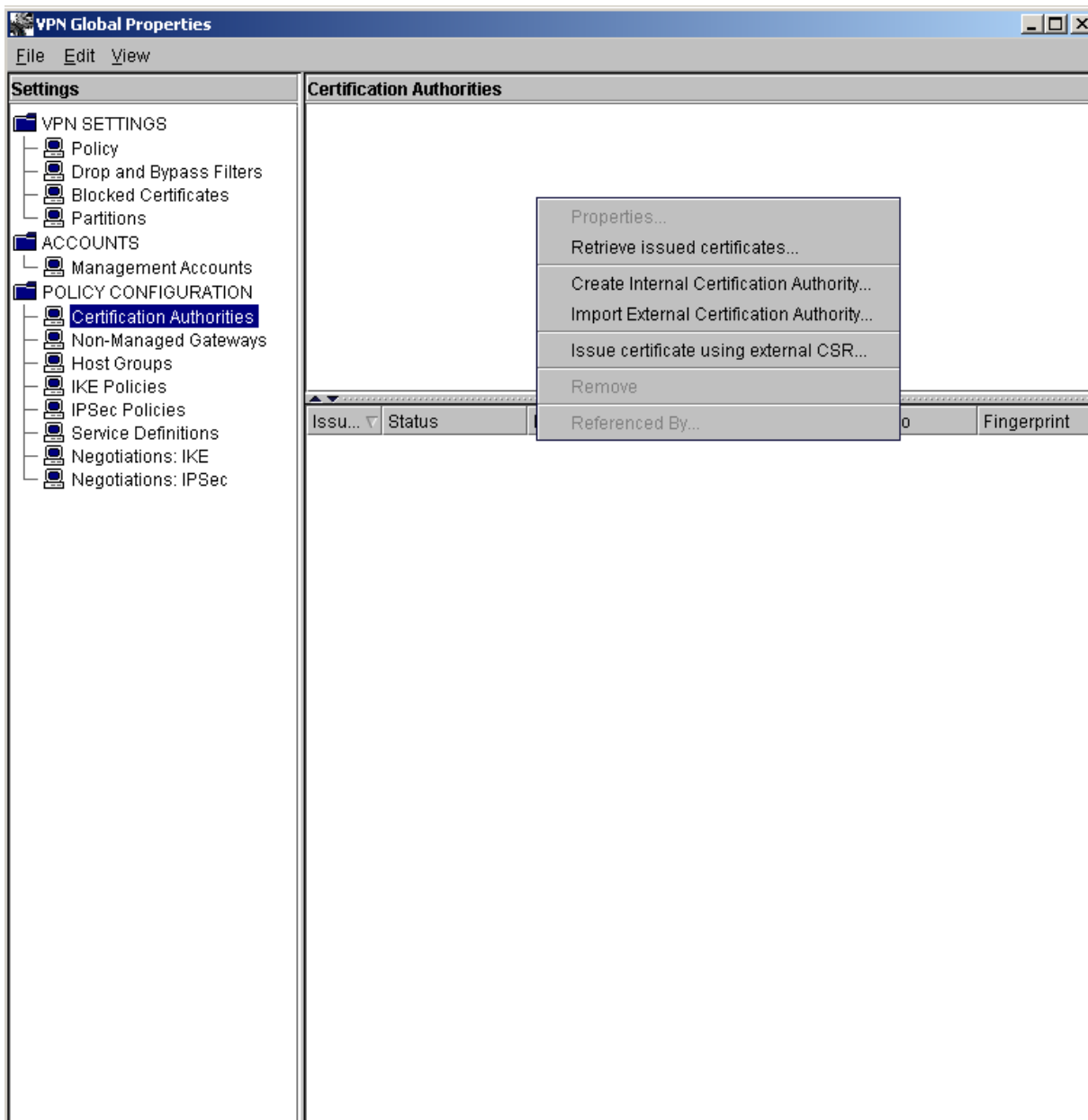
The assumption is that Nokia IP VPN, Nokia VPN Manager software, and Mobile VPN Client have been installed, and all post-installation tasks have been completed before continuing with the steps listed below. Use Nokia VPN Manager (NVM) to configure the Nokia IP VPN gateway. Start the Nokia VPN Manager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

Configuring remote client access using Challenge-Response authentication by NVM

Create an internal CA in Nokia IP VPN

Create an internal CA (if it has not been created yet) for the Nokia IP VPN gateway by Nokia VPN Manager in VPN Global Properties.

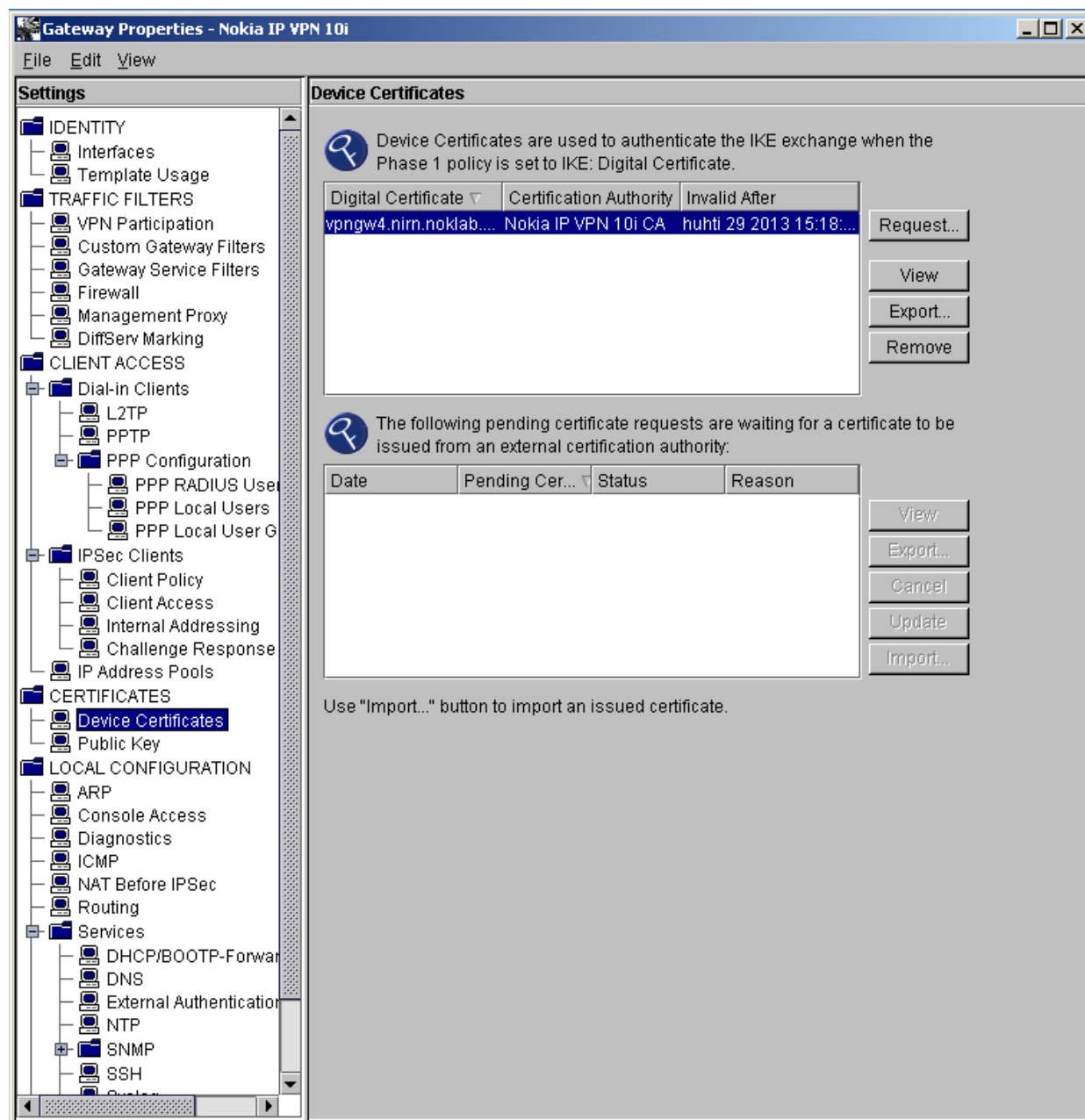
- To generate an internal Certificate Authority (CA), select POLICY CONFIGURATION -> Certification Authorities -> Create Internal Certification Authority.
- Select Gateway to Generate Certificate (if there are many).
- Supply the information to be contained in the root certificate, and specify the validity period (the default is 5 years).
- Press SUBMIT -> Accept -> OK ->Export->Save certificate for policy creation -> Close -> Close VPN Global Properties.
- Select Action on the menu bar and Apply Changes to save the internal CA to the Nokia IP VPN gateway.



Create device certificate for Nokia IP VPN gateway

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

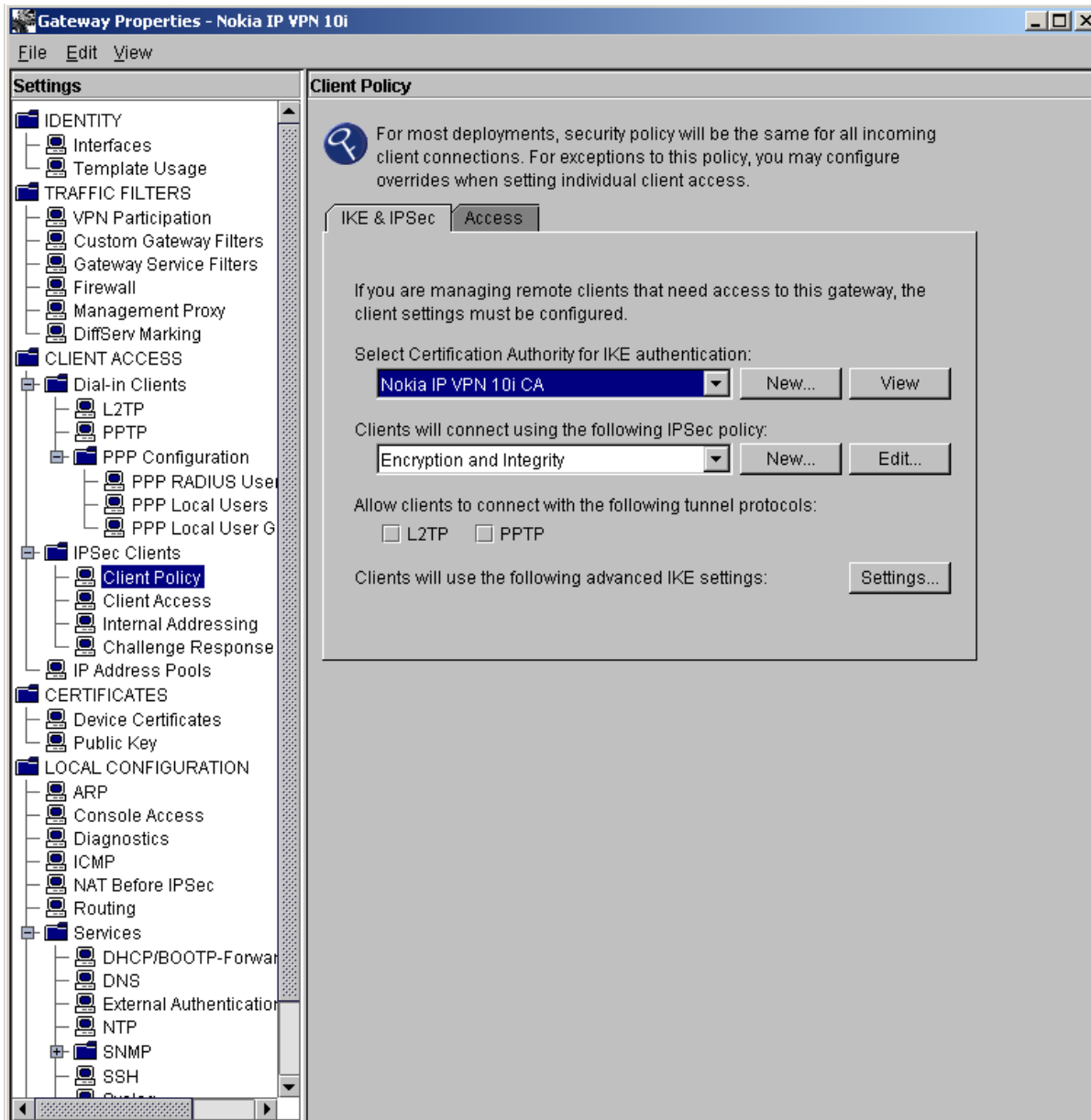
- Select Gateway Properties -> CERTIFICATES -> Device Certificates -> Request -> Select Internal CA certificate for Certificate Authority to request certificate.
- Supply the information required in SubjectName. Press SUBMIT and Accept, and then close Gateway Properties.
- Select Action on the menu bar and Apply Changes to save the device certificate.



Create VPN policy for Challenge-Response users

Create IKE/IPsec policies for Challenge-Response users in the following way:

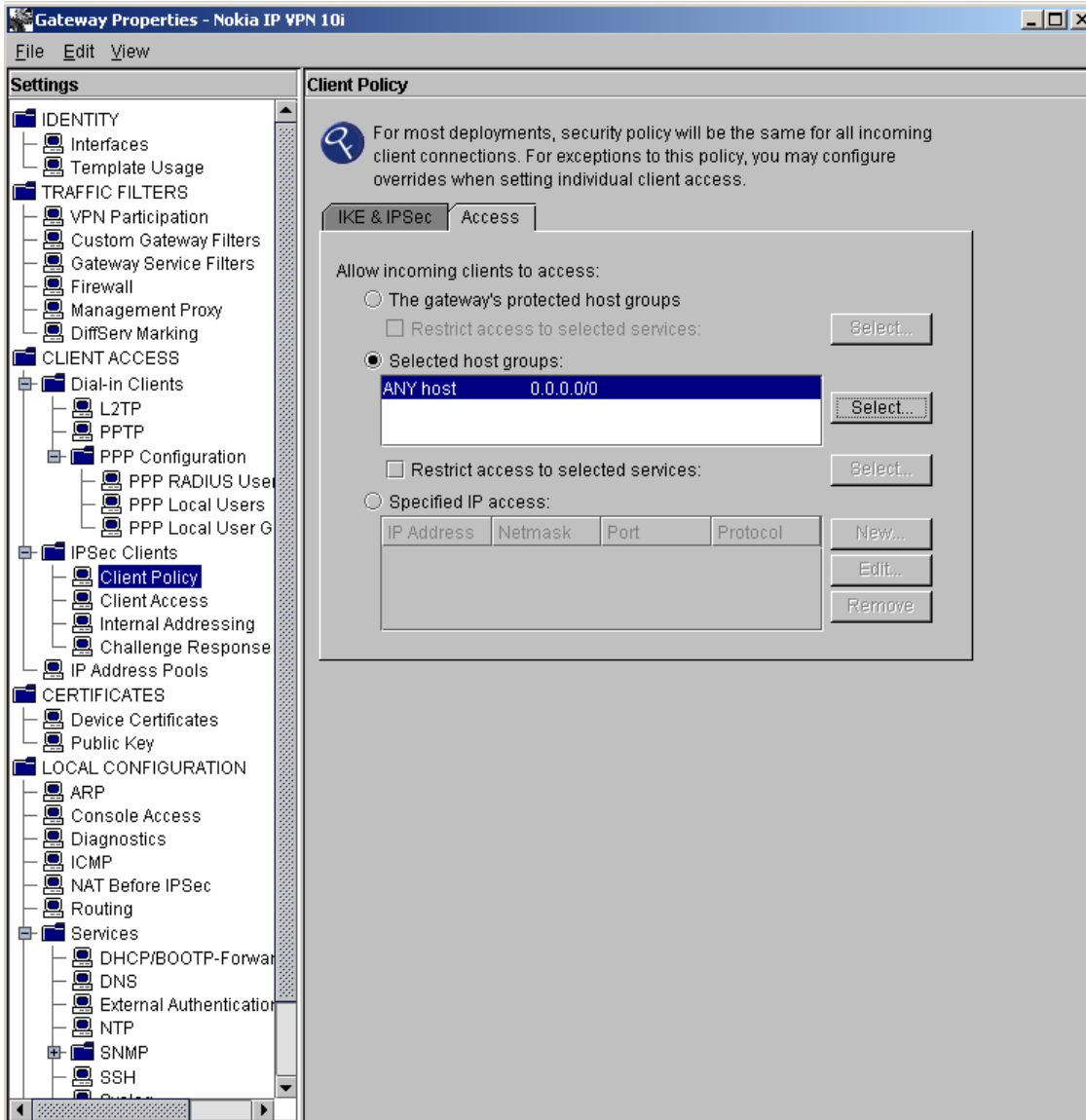
- Select Gateway properties -> CLIENT ACCESS -> IPsec Clients -> Client Policy.
 - Select Internal CA as the certification authority for IKE authentication on the list.
 - Next, check the IPsec policy settings under "Clients will connect using the IPsec policy." The default settings can be changed by selecting Edit or New.
 - The IKE policy settings for the Nokia Mobile VPN client policy can be changed from the defaults in "Clients will use the following advanced IKE settings."



Define protected networks for Challenge-Response 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 groups, so if that is not changed, "ANY host" must be selected here, too.



Define authentication method for Challenge-Response user policy

Now, create a client access policy for Challenge-Response users.

- Select Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Client policy -> IPsec Client -> Client Access. Check "Allow clients to connect Challenge Response authentication." Then check Password and/or SecurID.

The screenshot shows the 'Gateway Properties - Nokia IP VPN 10i' configuration window. The left pane shows a tree view of settings, with 'Client Access' under 'IPsec Clients' selected. The right pane displays the 'Client Access' configuration for 'IPsec Clients'.

Client Access

You may enable incoming client connections to this gateway, using either certificate or challenge response authentication.

Note: This policy is also enforced for any L2TP or PPTP connections requiring IPsec.

Certificate Clients

Allow clients to connect using certificate based authentication:

Clients	Policy	
---------	--------	--

New...
Edit...
Remove
Move Up
Move Down

Challenge Response Clients

Allow clients to connect using Challenge Response authentication:

Password SecurID

Override client policy settings: Settings...

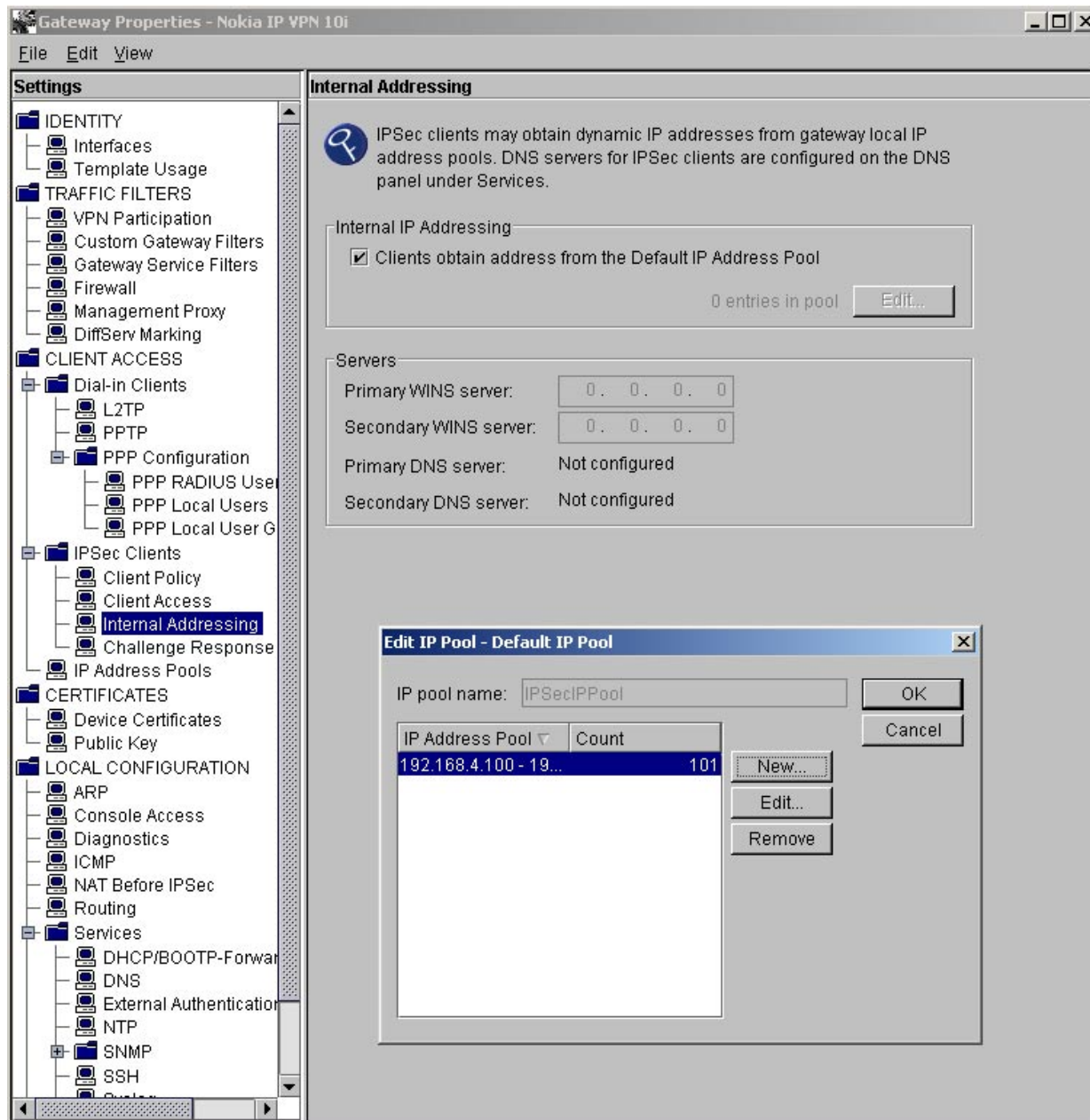
You must configure External Authentication servers or the Local User list.

Configuring 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." Next, select New to define the Internal Address Pool. Press OK, and OK.

Note: Define the Internal Address pool so that it does not overlap with the subnets of physical interfaces. Check also that the routing is 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.

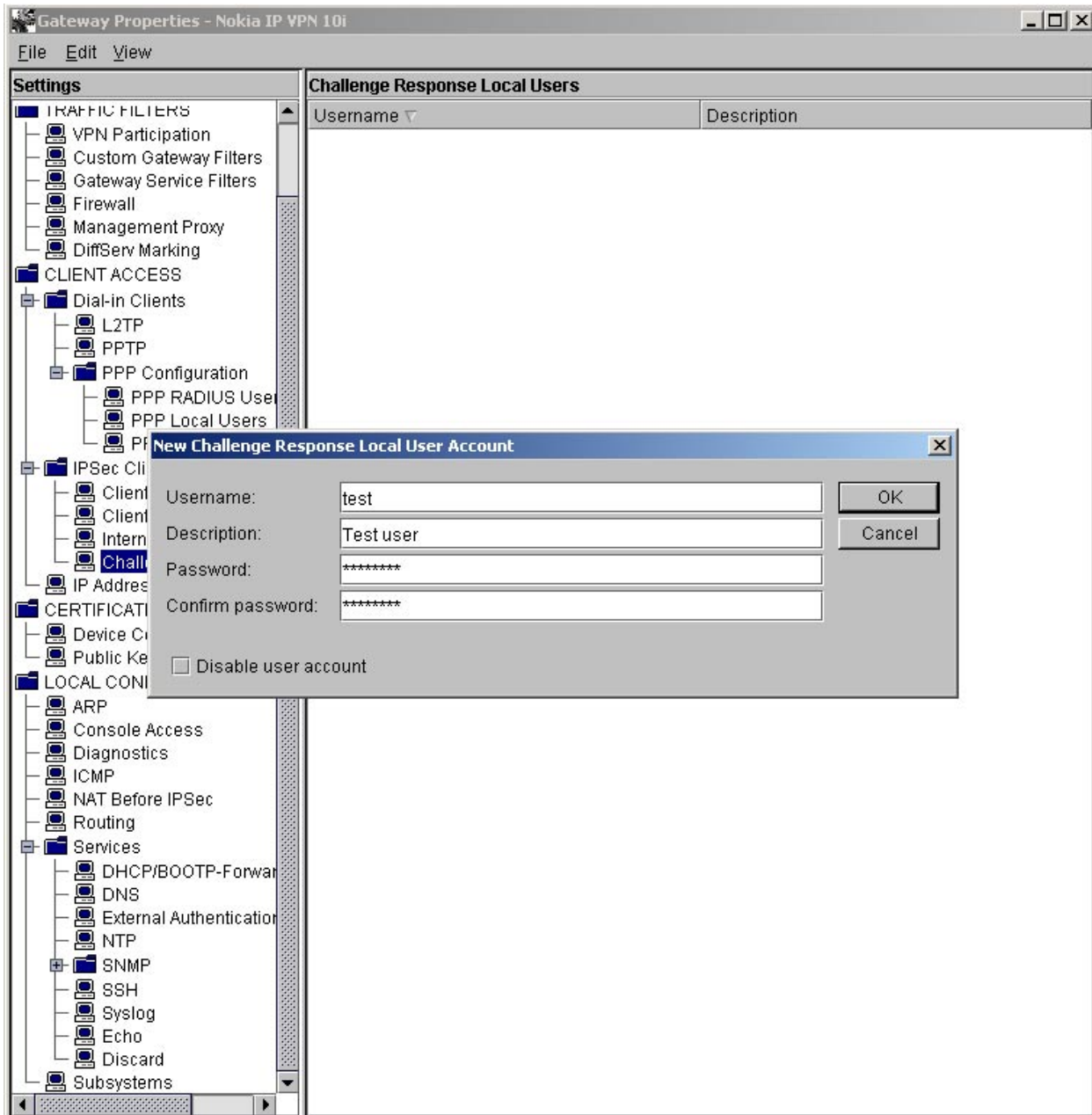
The screenshot displays the Nokia VPN Manager interface in edit mode. The main window is titled "Gateway Properties - Nokia IP VPN 10i". The left sidebar shows a tree view of settings, with "Services" expanded and "DNS" selected. The main pane shows the "DNS" configuration for the selected gateway. The "Default domain name" is set to "vpngw4.net". Under "DNS Settings", the "Number of retries" is set to 2 and the "Retransmission timeout (seconds)" is also set to 2. A help icon indicates that up to 4 DNS servers can be entered. A "New IP Address" dialog box is open, showing the IP address "192.168.4.10". The bottom status bar shows "Nokia administrator 1 Gateway".

Create a user name/password for Challenge-Response users

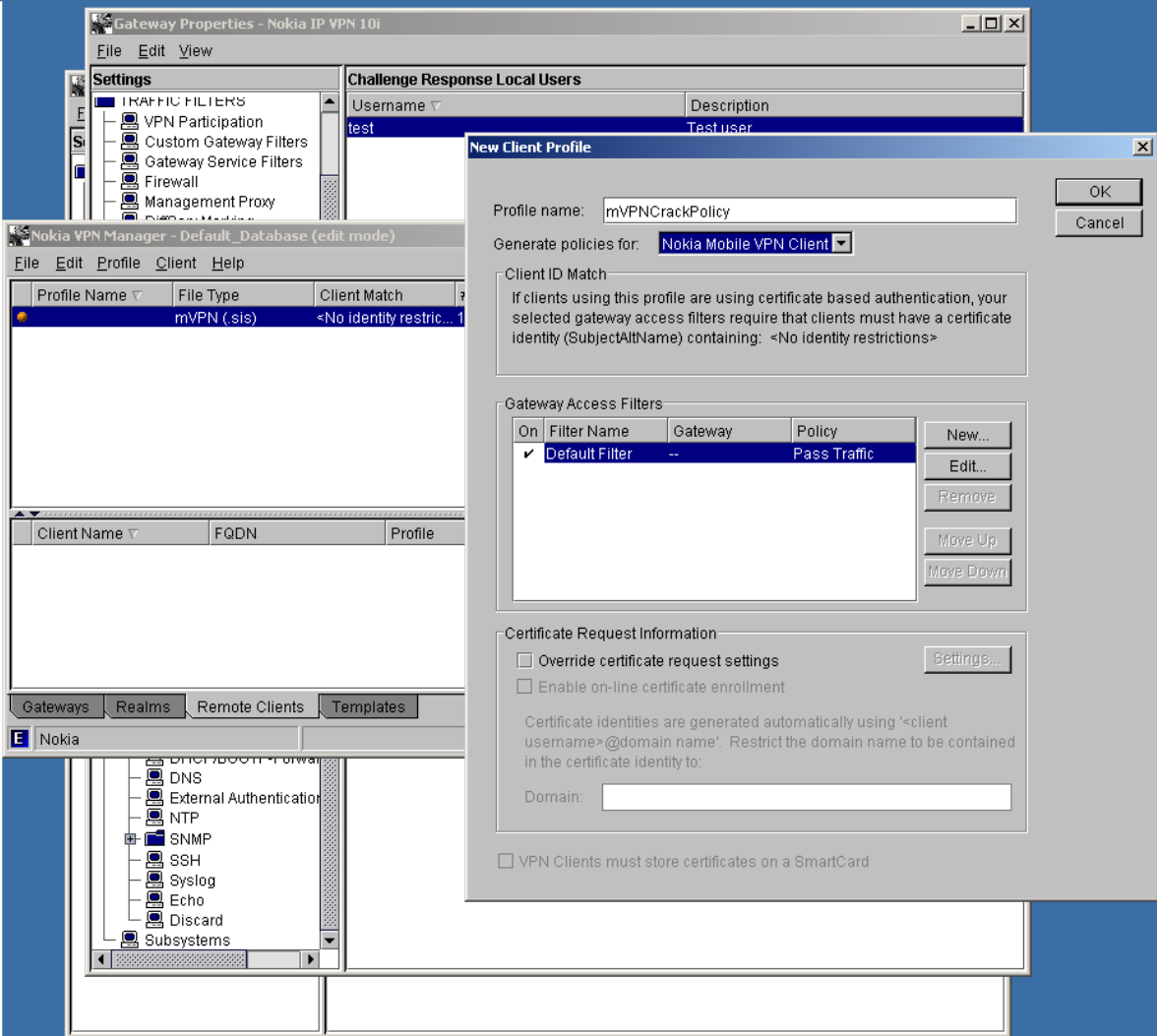
If there are no external authentication servers (Radius/LDAP) available, create users to the local database.

- Select Gateway Properties -> CLIENT ACCESS -> IPsec Clients -> Challenge Response Local Users ->Edit -> New, to create local users using the Challenge-Response authentication method.
- Next, do Apply Changes by the Nokia VPN Manager -> Menu bar -> Action -> Apply Changes.

External authentication (RADIUS/LDAP) servers can be defined in Gateway Properties -> Services -> External Authentication.



Create a remote client profile and policy for Challenge-Response authentication
From the bottom of the VPN Manager, select the Remote Clients tab. Then 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. Select New in Gateway Access filters. In New Gateway Access Filter, 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 Challenge Response and Authenticate using a password (or SecurID). Press OK, and OK.

The image shows two overlapping configuration windows from a network management interface.

New Client Profile (top window):

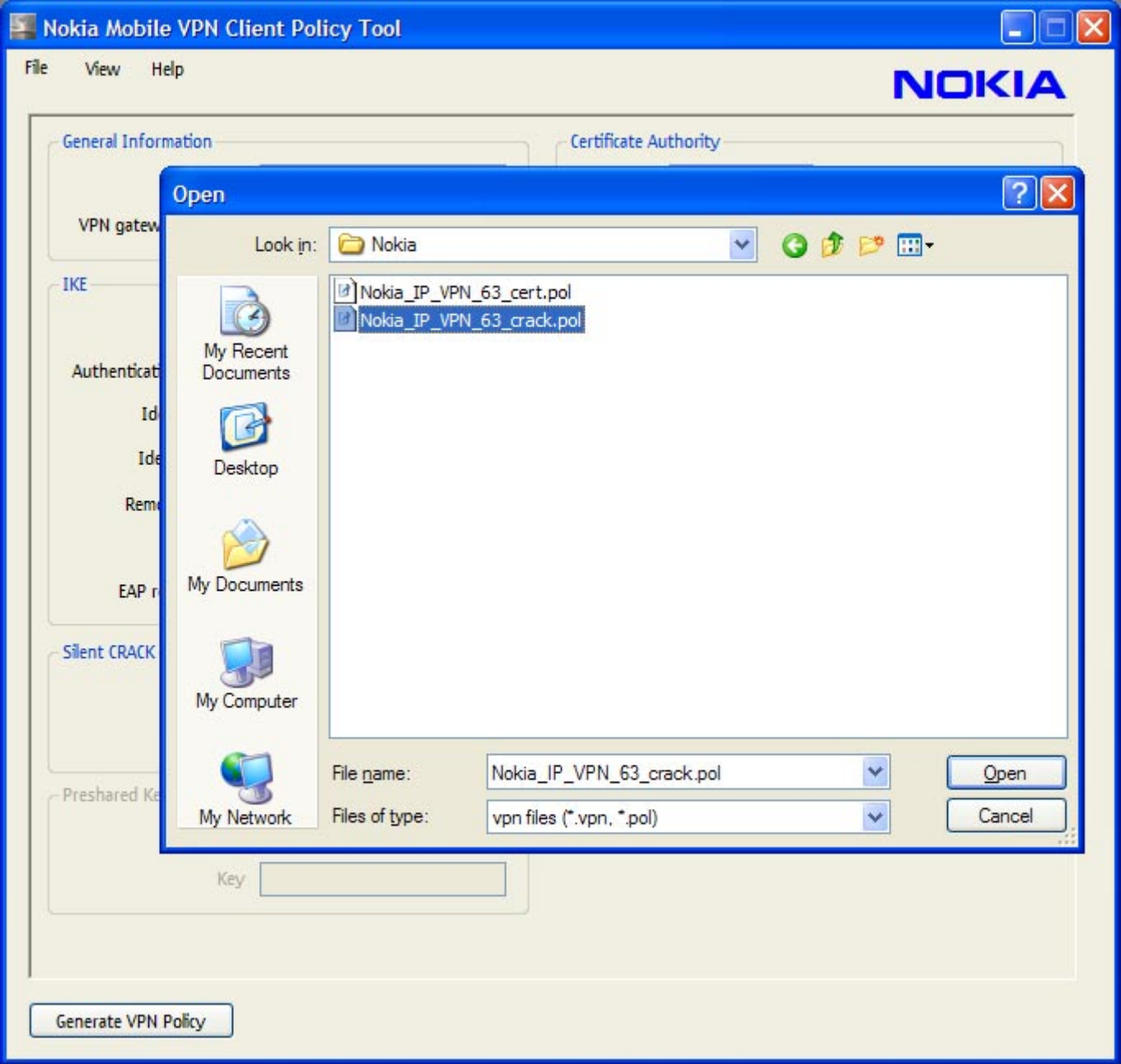
- Profile name:
- Generate policies for:
- Client ID Match:
- Buttons: OK, Cancel

New Gateway Access Filter (bottom window):

- Filter name:
- Traffic Policy:
- IPSec Tunnel section:
 - Establish tunnels to remote gateway:
 - Assign client IP address from the Default IP Address pool
 - Select an IKE policy:
 - Use authentication method:
 - Certificates
 - Challenge Response
 - Authenticate using:
 - Password
 - SecurID
- in the certificate identity to.
- Domain:
- VPN Clients must store certificates on a SmartCard
- Buttons: OK, Cancel

Policy creation with Policy Tool using exported CA certificate

Before the Nokia Mobile VPN client policy can be created, the CA certificate must be exported from Nokia IP VPN. Then, start Nokia VPN Client Policy Tool and press the Load Template button. Select Nokia_IP_VPN_63_crack.pol policy from the Nokia directory.



Add the correct VPN gateway address and get the path to the DER encoded CA certificate. Make sure that the Format in the Certificate Authority selection is set to BIN.

Export the VPN policy by pressing the Generate VPN Policy button. Store Nokia_IP_VPN_63_crack.vpn to your PC. Consult the *Nokia Mobile VPN Client User's Guide*, Chapter 6.1, for details on how to install the given policy file to your device.

The screenshot displays the Nokia Mobile VPN Client Policy Tool interface. The window title is "Nokia Mobile VPN Client Policy Tool" and the Nokia logo is in the top right corner. The interface is divided into several sections:

- General Information:** Policy name: Nokia_IP_VPN_63_crack; VPN gateway address: 192.168.1.1.
- Certificate Authority:** Format: BIN; Data: C:\certificates\CA.cer.
- IKE:** IKE mode: IKEv1 main; Authentication method: IKE-CRACK; Identity type: Nokia IP VPN CRACK; Identity value: (empty); Remote ID type: (empty); Remote ID: (empty); EAP realm prefix: (empty).
- User Certificate:** Certificate: (empty); Private key: (empty); Subject DN suffix: (empty); RFC822NAME (FQDN): (empty); Key length: 1024.
- PKCS#12:** PKCS file: (empty); VPC file: (empty).
- Silent CRACK:** Username: (empty); Password: (empty).
- Preshared Key:** Format: STRING_FORMAT; Key: (empty).

A "Generate VPN Policy" button is located at the bottom left of the interface.

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

Asia Pacific Tel: +65 6588 33 64 • Email: asia@nokiaforbusiness.com

Europe France +33 170 708 166 • UK +44 161 601 8908 • Email: europaenokiaforbusiness.com

Middle East and Africa Dubai +971 4 3697600 • Email: mea@nokiaforbusiness.com

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