Nokia Mobile VPN Client Policy Tool User's Guide

NOKIA

Nokia for Business

Table of Contents

Introduction 3
Purpose of this document 3
References 3
Abbreviations and definitions 3
Installation 5
Uninstallation 5
Usage 6
Wizard view 6
General Information 7
IKE 7
Silent CRACK 7
Preshared Key 8
Certificate Authority 8
User Certificate 8
PKCS#12 9
Advanced view 10
Information-node 10
SAs-node 11
Selectors-node 13
IKE-node 14
IKE proposals-node 15
CAs-node 16
User certificates-node 17
Intermediate CAs-node 18
Using templates 19
Generating VPN policy 19
Clearing All 20
Policy Tool version 20

Introduction

Purpose of this document

Nokia Mobile VPN Client Policy Tool is used to generate VPN policy files (*.vpn). Generated VPN policy files can be transferred to an end device and installed by Nokia Mobile VPN client. See [MVPN_USER_GUIDE] for more details.

Users can create policy files from scratch or use predefined templates provided by the tool. In addition, the tool can be used to modify existing policies by loading pol-files or vpn-files.

All the parameters provided by the tool are specified in [POLICY_SPEC].

References

[POLICY_SPEC]	Nokia Mobile VPN Policy Specification
[.NET_FRAMEWORK]	http://msdn.microsoft.com/en-us/netframework/default.aspx
[MVPN_USER_GUIDE]	Nokia Mobile VPN Client User's Guide

Abbreviations and definitions

AES	Advanced Encryption Standard, known also as Rijndael: symmetric cryptography chipper
AKA	Authentication and Key Agreement: EAP mechanism for authentication and session key distribution
CA	Certificate Authority: an entity that issues digital certificates
CBC	Chipper Block Chaining: a Block chipper operating mode
CRACK	Challenge/Response Authentication of Cryptographic Keys: an authentication extension
DER	Distinguished Encoding Rules: data encoding method.
DNS	Domain Name System
DPD	Dead Peer Detection
EAP	Extensible Authentication Protocol, : a universal authentication framework
ESP	Encapsulated Security Payload: an operating mode of IPSec. May also mean IP packet extension header used by IPSec.
FQDN	Fully Qualified Domain Name
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security protocol
NAT	Network Address Translation
pin-file	Text formatted file containing policy information
PKCS#12	Public Key Cryptography Standards 12
pol-file	Text formatted file containing policy parameters
PEM	Base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
PSK	Preshared Key
RSA	An algorithm for public-key encryption
SA	Security Association: a set of parameters that define the properties an

	active "connection" between IPSec or IKE peers
SIM	Subscriber Identity Module: a removable smart card used for identification
SHA-1	Secure Hash Algorithm: cryptographic hash function
UDP	User Datagram Protocol: one of the core protocols of the IP protocol suite
VPN	Virtual Private Network
vpn-file	Zip-formatted file containing pin- and pol-files. Vpn-file can also contain certificates, private key and PKCS#12 packet.

Installation

Nokia Mobile VPN Client Policy Tool can be installed by double clicking “Nokia Mobile VPN Client Policy Tool.msi” installer file. The tool is built on .NET Framework 2.0 [.NET_FRAMEWORK] and the installer file will instruct how to setup the framework.

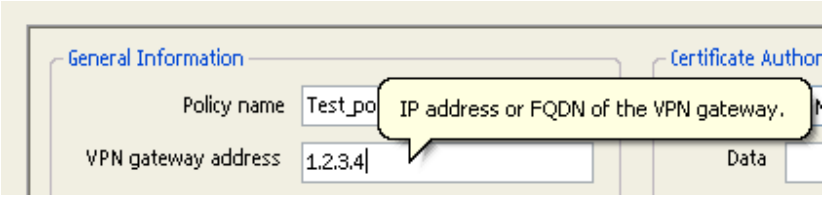
After installation the tool can be launched from start menu-> All programs -> Nokia Mobile VPN Client Policy Tool.

Uninstallation

Nokia Mobile VPN Client Policy Tool can be uninstalled from Control Panel -> Add or Remove Programs.

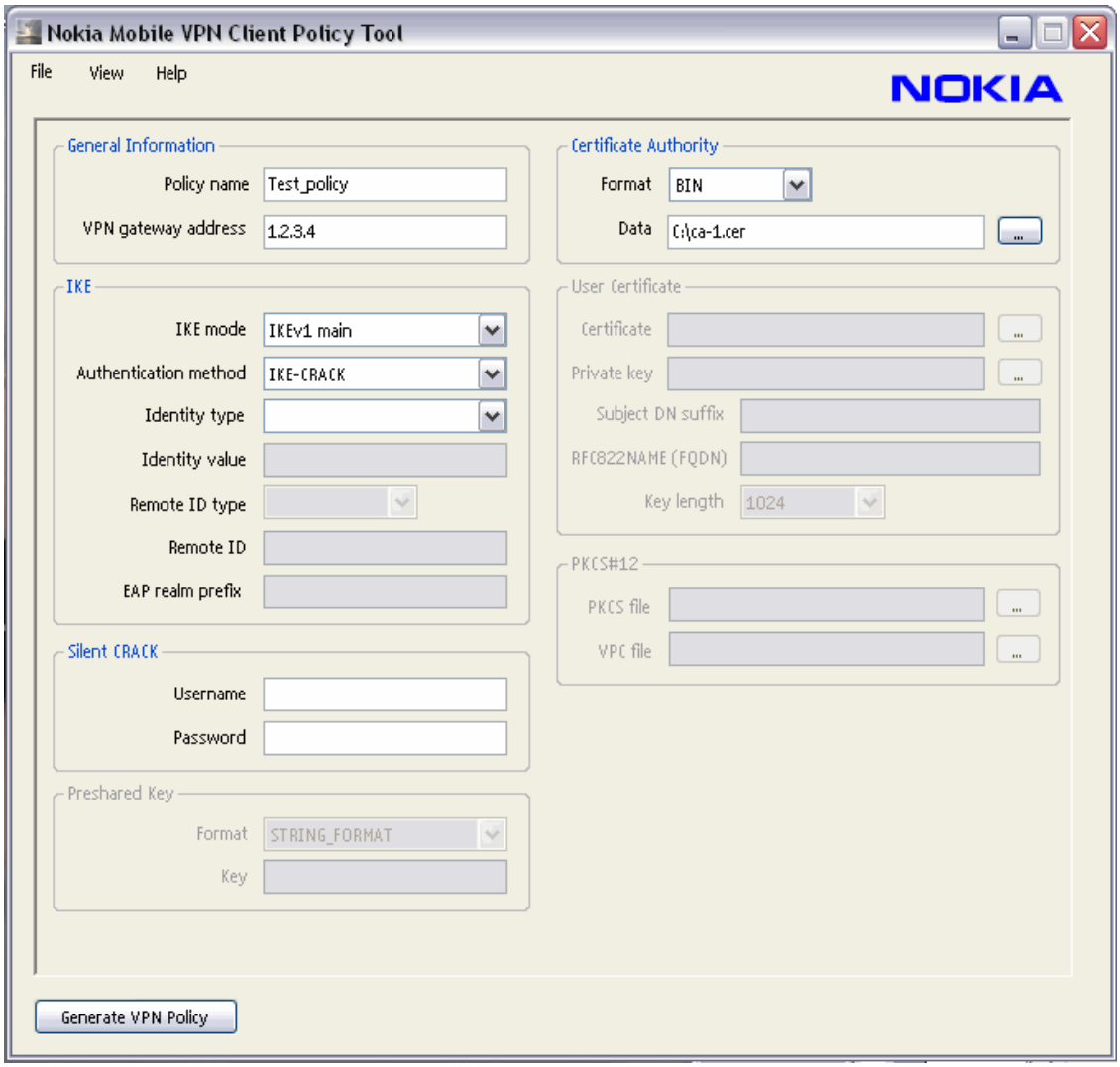
Usage

The tool has two views wizard and advanced. When the tool is launched, the wizard view is shown. For most of the parameters, the tool provides built-in help. Parameter specific tip box is displayed when user holds mouse over the parameter field.



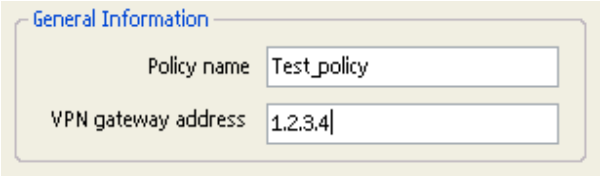
Wizard view

Wizard view contains all mandatory parameters for policy creation. The purpose is for the user to be able to create a working policy just by filling parameters shown in wizard view. It is not possible to generate a policy or move to advanced view unless all mandatory parameters are given. For every policy mandatory parameters are policy name and VPN gateway address. There are also other mandatory parameters depending on IKE authentication method.



General Information

General Information box has fields for policy name and VPN gateway's address.

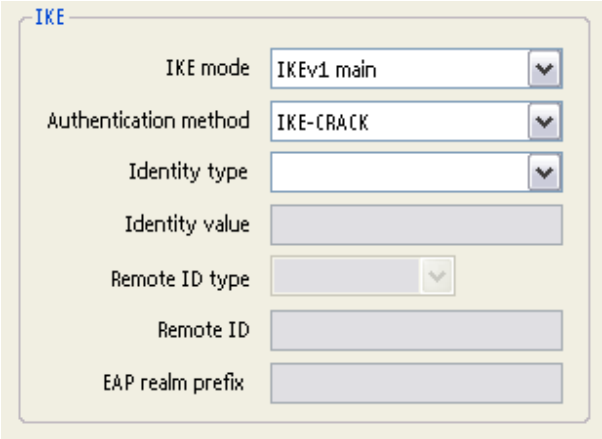


IKE

IKE box contains IKE parameters. Mandatory parameters are IKE mode and authentication method. Authentication method has an effect on other mandatory parameters:

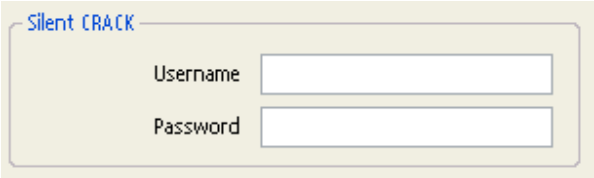
- If IKE-CRACK is selected as an authentication method, CA certificate information will become a mandatory parameter.
- If PRE-SHARED is selected as an authentication method, Preshared Key will become a mandatory parameter.
- If RSA_SIGNATURES is selected as an authentication method, CA and user certificate information will become mandatory parameters. These parameters can be replaced by giving path to a PKCS#12 file.
- If EAP_AKA or EAP_SIM are selected as an authentication method, EAP realm prefix and CA certificate information will become mandatory parameters.

Identity type and value are optional parameters with IKEv1. Identity type and value are optional parameters with IKEv2 when PRE-SHARED and RSA_SIGNATURES authentication method is used. Remote ID type and remote ID are optional parameters with IKEv2.



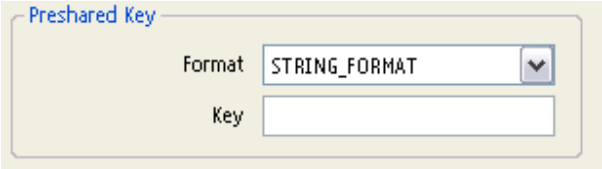
Silent CRACK

Silent CRACK box is enabled when IKE-CRACK is selected as an authentication method. Silent CRACK parameters are optional. If username and password are provided, they will be used in IKE authentication and user will not be asked to give username and password.



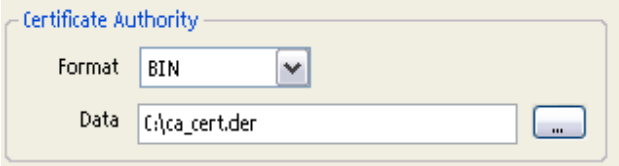
Preshared Key

Preshared Key box is enabled when PRE-SHARED is selected as an authentication method. Preshared Key parameters are mandatory when PRE-SHARED is selected as an authentication method.



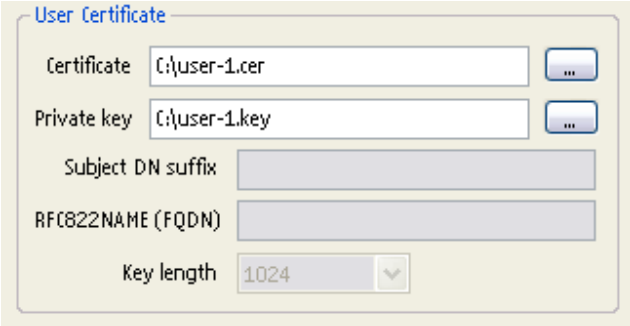
Certificate Authority

Certificate Authority box contains CA certificate information. Users can browse or drag&drop DER- or PEM-formatted certificates into the box. If needed, the tool will rename the certificate into Mobile VPN Client supported form. For this purpose the tool creates a temp directory which will be removed when the tool is closed. More CA certificates can be added from advanced view. Certificate file must be in DER- or PEM-encoded X509.3 ASN.1 format.

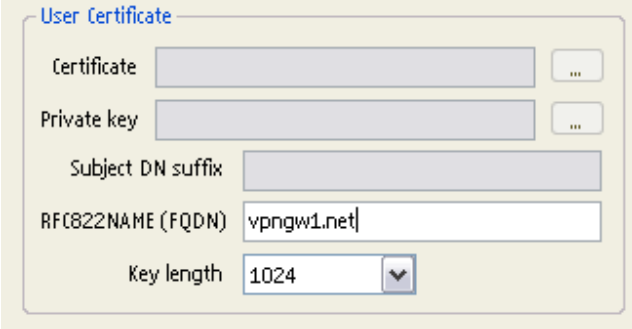


User Certificate

User Certificate box is enabled when RSA_SIGNATURES is selected as an authentication method. When user certificate is in binary format, paths to certificate and private key must be provided. User certificate box supports drag&drop functionality. When binary format is used, other fields are disabled. Certificate file must be in DER- or PEM-encoded X509.3 ASN.1 format.

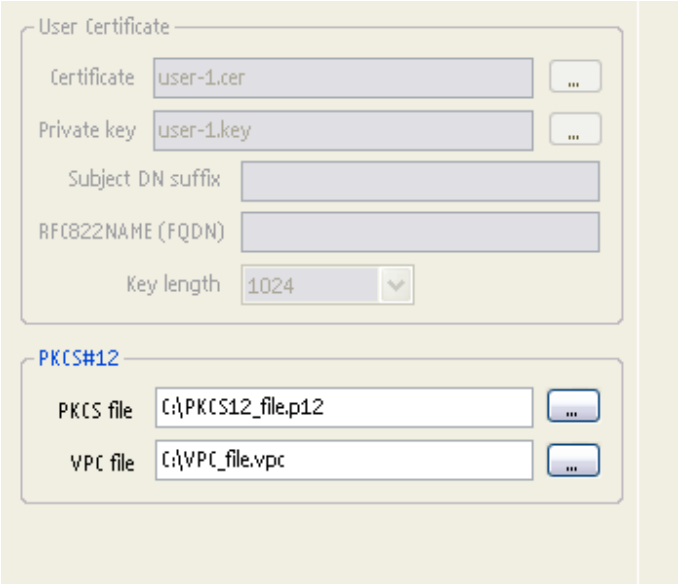


If the User Certificate is already installed to the end device, certificate information can be given in text format. When text format is used, Certificate and Private key fields are disabled.

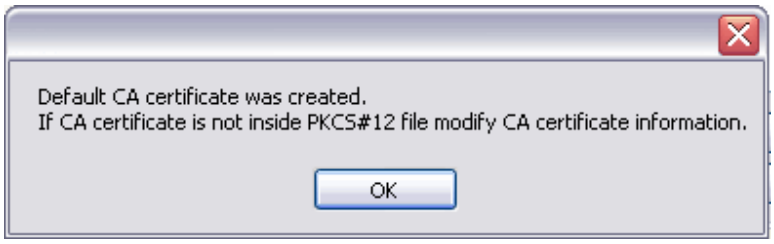


PKCS#12

PKCS#12 box is enabled when RSA_SIGNATURES is selected as an authentication method. It is assumed that PKCS#12 packet does contain user certificate and private key. In other words, when PKCS#12 file is provided, user certificate box is disabled with some default values. VPN configuration (VPC) file can be provided with PKCS#12 packet.

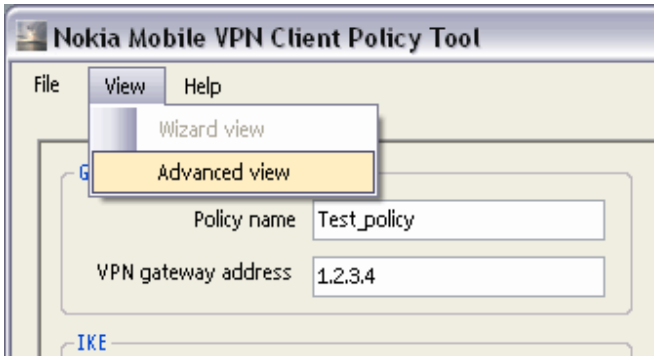


The tool will also assume that CA certificate is also provided inside PKCS#12 packet. This is why default CA certificate information is inserted automatically. If the PKCS#12 packet does not provide CA certificate, the user must edit CA certificate information manually.



Advanced view

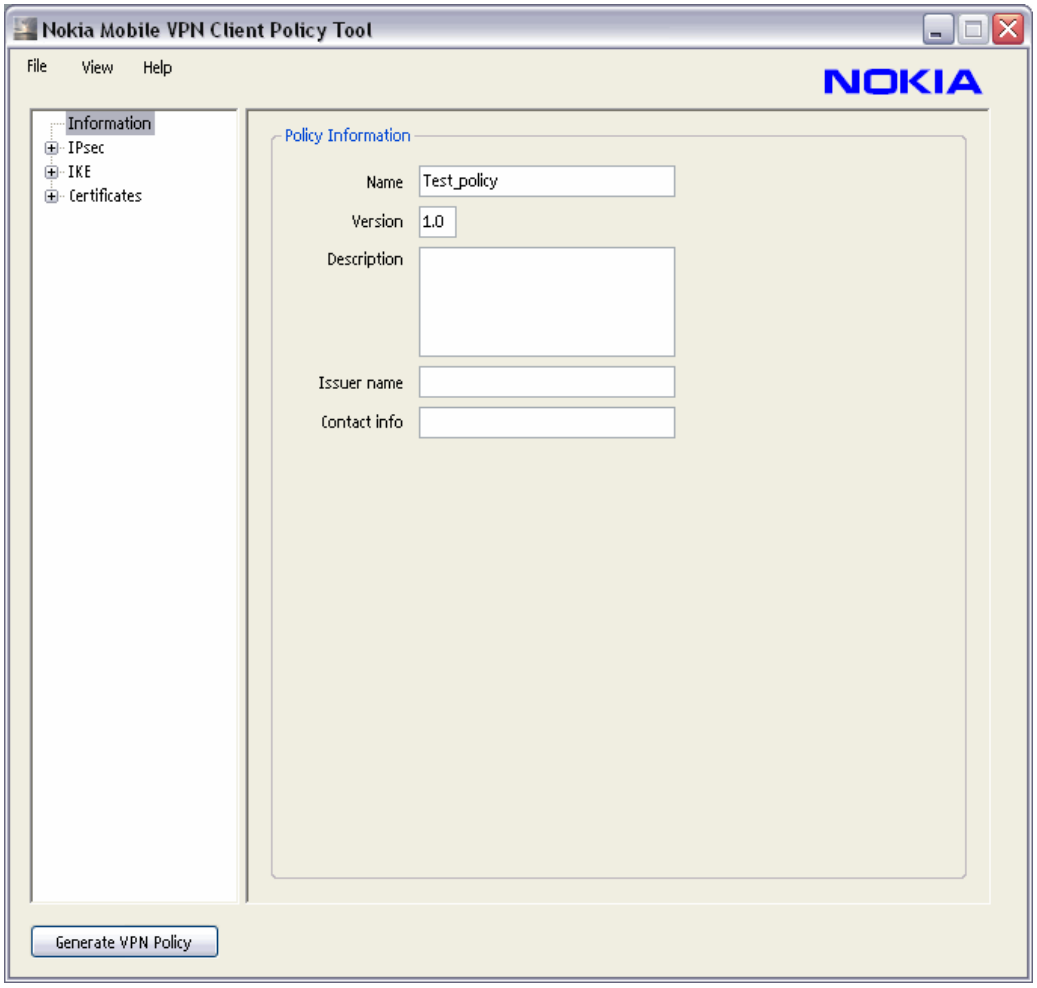
When all the mandatory parameters have been given, the user can generate VPN policy or switch to advanced view by click View -> Advanced view from the menu bar.



Advanced view lets the user modify all possible parameters. Some of the parameters are set by default. User can navigate through parameters by selecting nodes from the tree view. All the parameters provided by the tool are specified in [POLICY_SPEC].

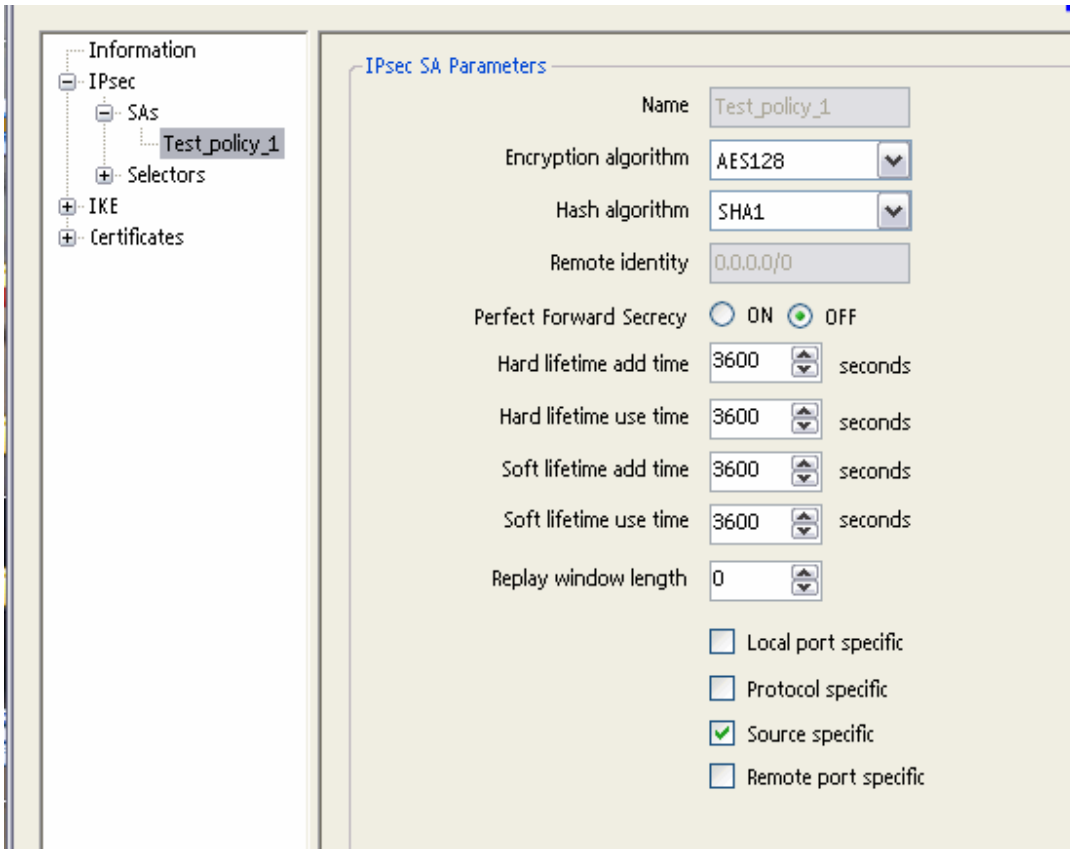
Information-node

Information node displays policy information.

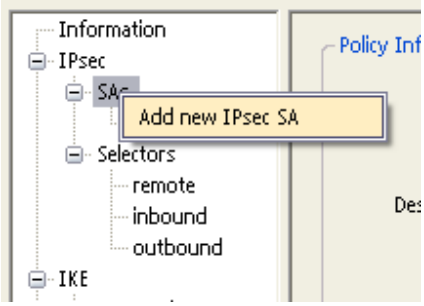


SAs-node

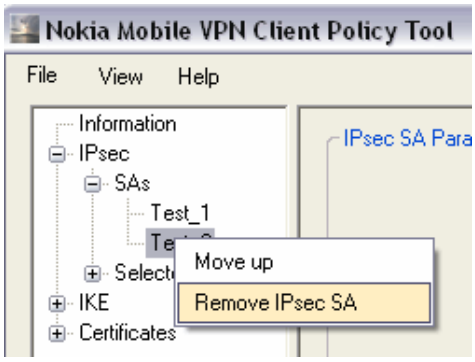
One IPsec SA is created by default.



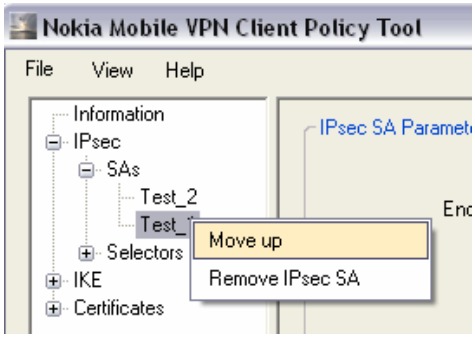
New IPsec SAs can be added by right-clicking SAs node.



IPsec SA can be removed by right-clicking IPsec SA node. One IPsec SA will always remain.

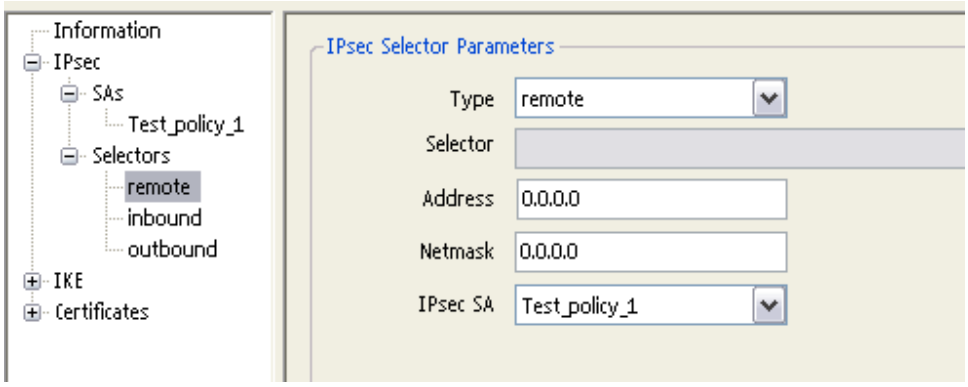


IPsec SAs can be rearranged by right-clicking IPsec SA node.

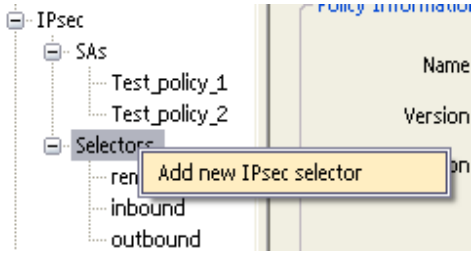


Selectors-node

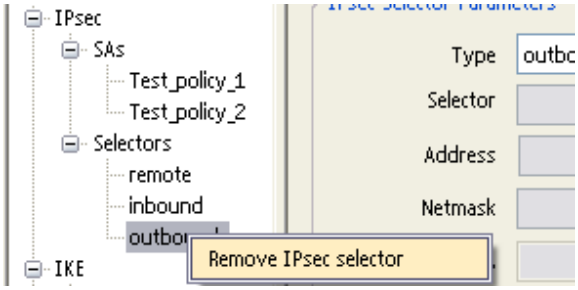
The tool creates bypass policy by default. This requires that remote, inbound and outbound selector. To create a “drop all” policy provide only remote selector.



New selectors can be added by right-clicking Selectors node.

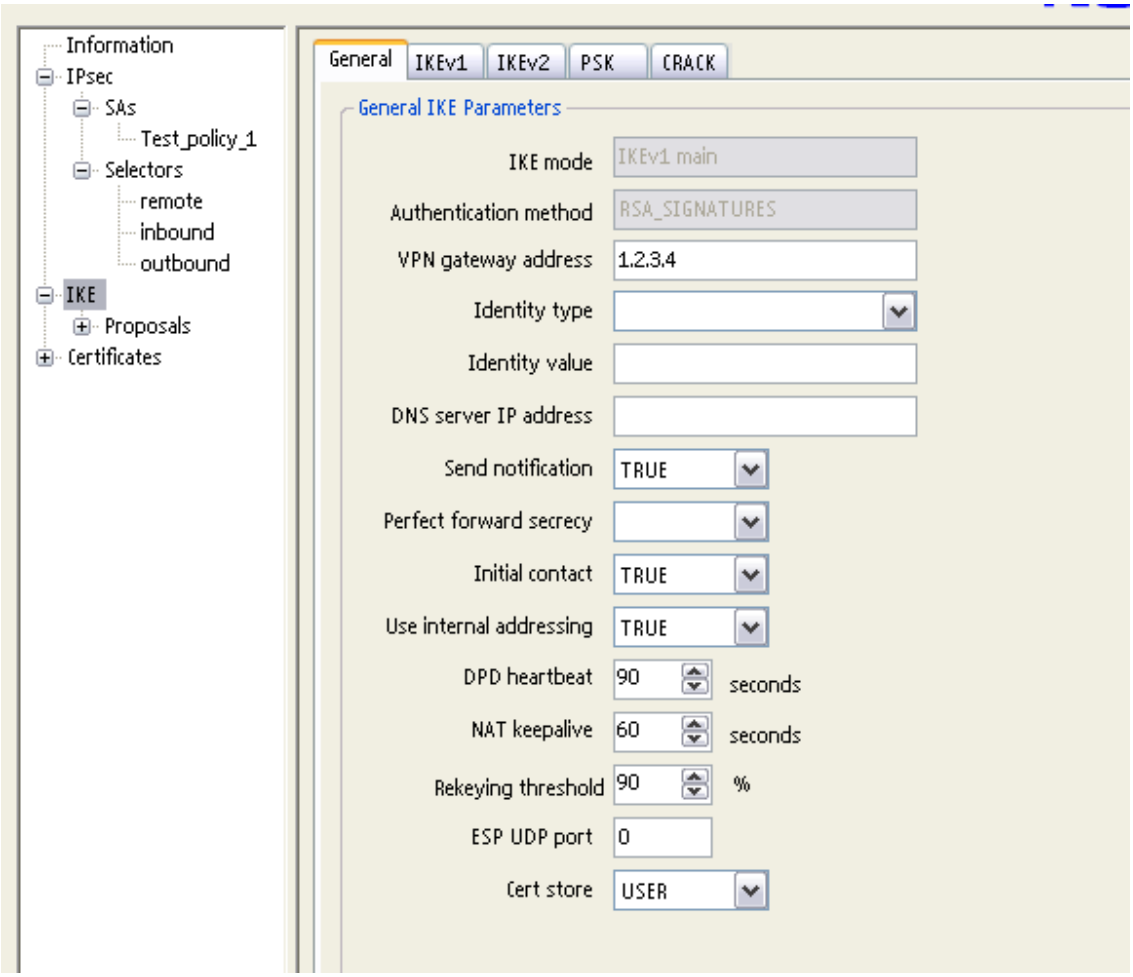


IPsec selector can be removed by right-clicking IPsec selector node. One IPsec selector will always remain.



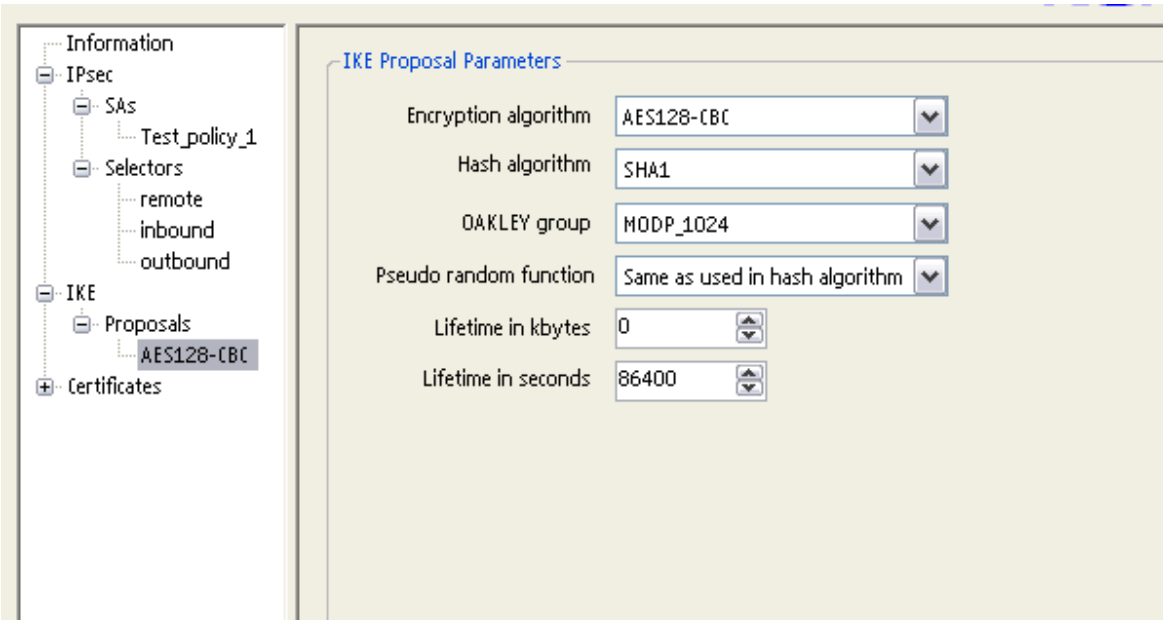
IKE-node

Some of the IKE parameters are set by default. IKE mode and authentication method cannot be changed from advanced view. General-tab contains common parameters from IKEv1 and IKEv2. IKE version specific parameters can be edited from their own tabs. If authentication method is Preshared Keys or silent CRACK, related parameters have their own tabs.

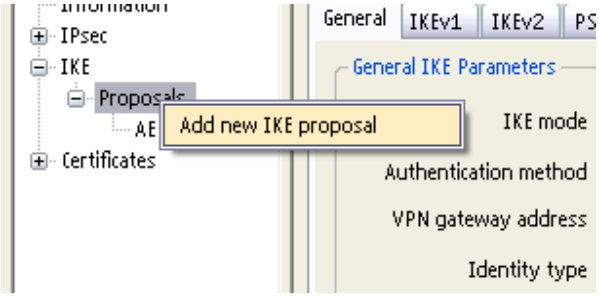


IKE proposals-node

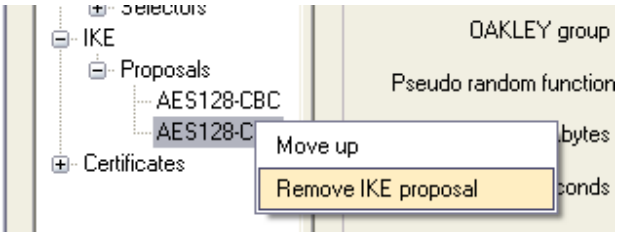
By default, one IKE proposal is added.



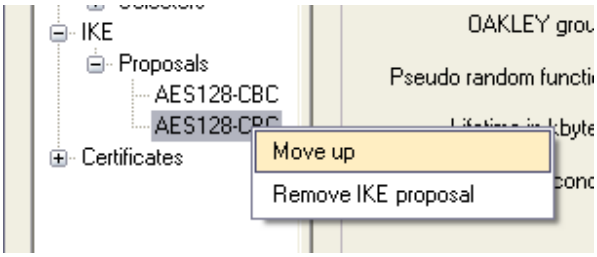
New IKE proposals can be added by right-clicking Proposals-node.



IKE proposal can be removed by right-clicking IKE proposal node. One IKE proposal will always remain.

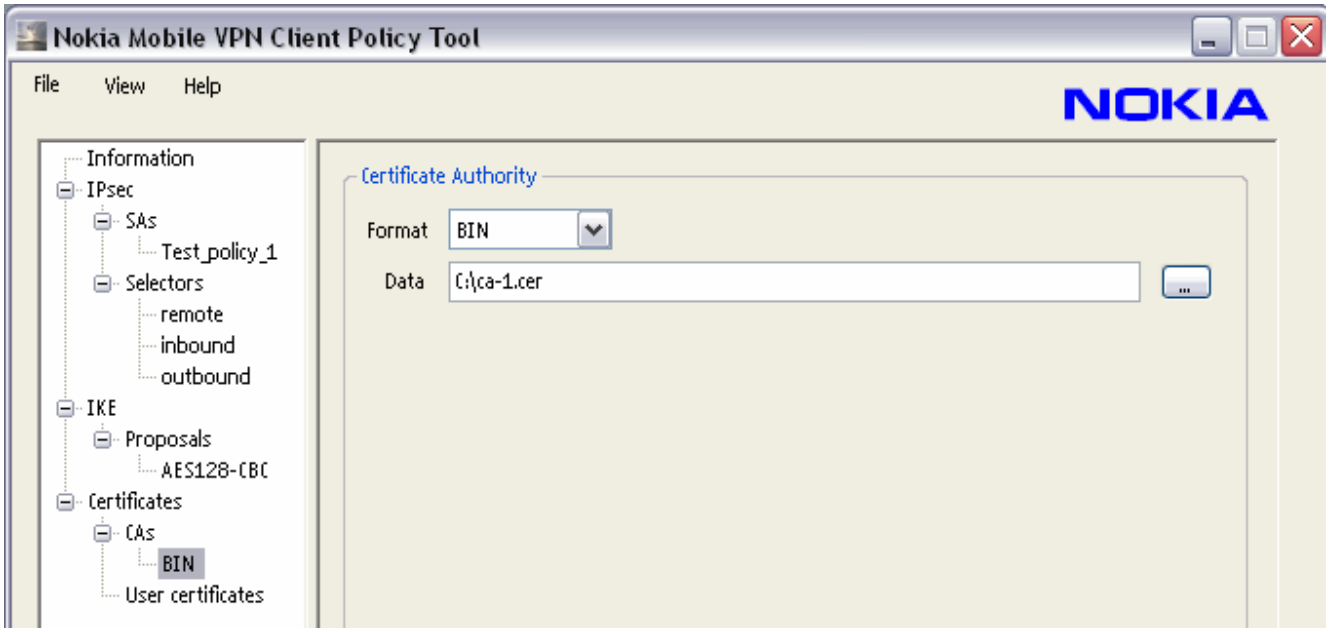


IKE proposals can be rearranged by right-clicking IKE proposal node.

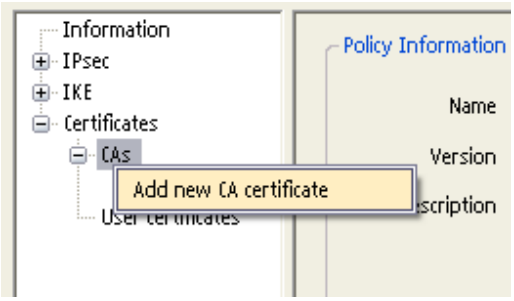


CAs-node

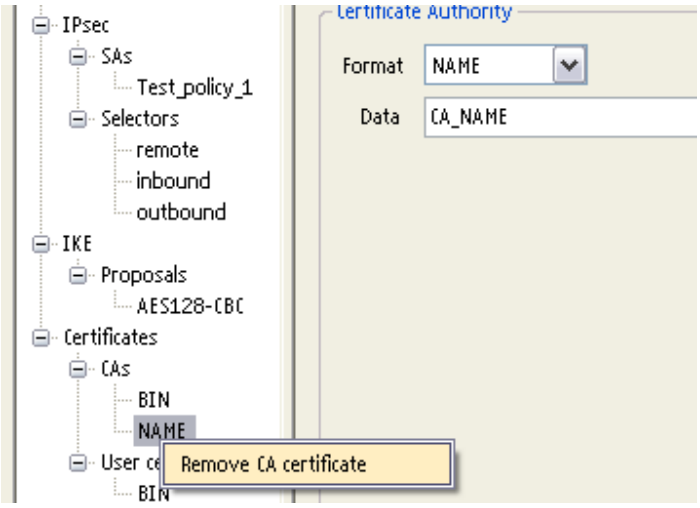
The first CA certificate under CAs-node is the one that is shown in wizard view. If needed, the tool will rename the certificate into Mobile VPN Client supported form. For this purpose the tool creates a temp directory which will be removed when the tool is closed. Certificate file must be in DER- or PEM-encoded X509.3 ASN.1 format.



New CA certificates can be added by right-clicking CAs-node. When Preshared Key is used as an authentication method, CAs cannot be added.

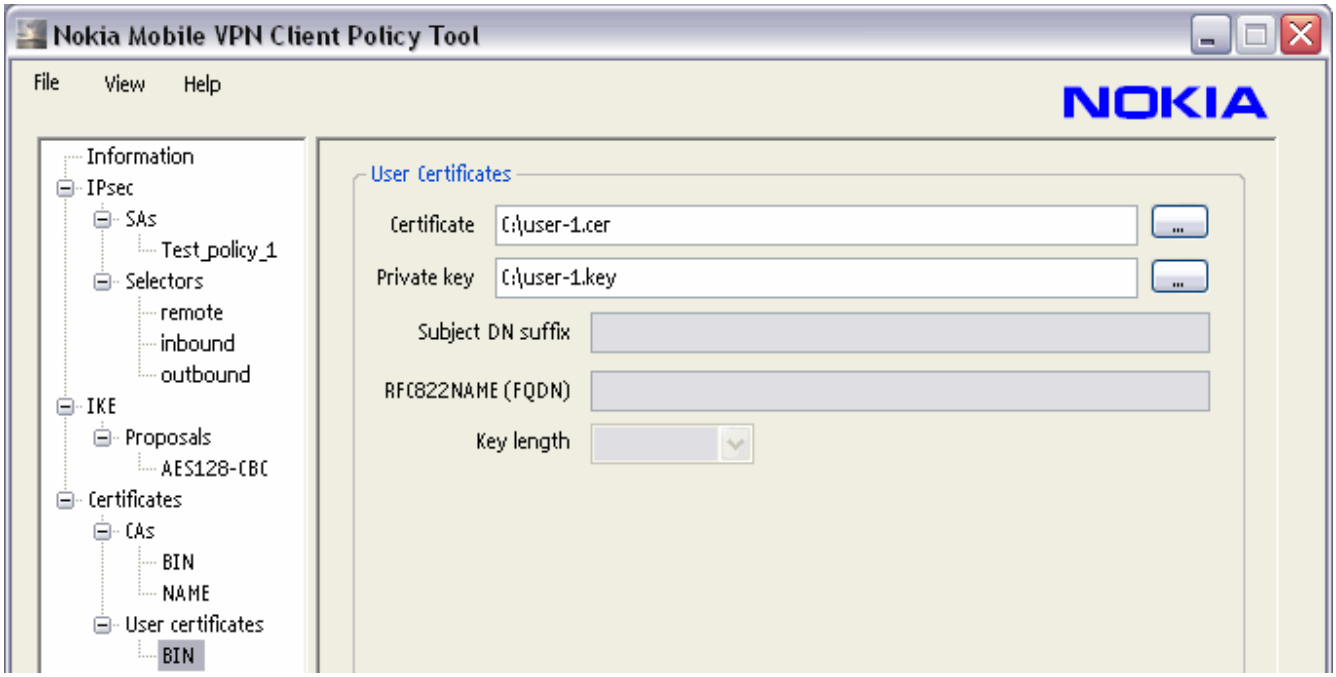


CA certificate can be removed by right clicking CA certificate node. One CA certificate will always remain.



User certificates-node

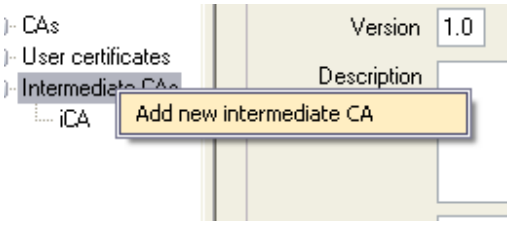
User certificate is added from wizard view based on IKE authentication method. User can only modify user certificate information from advanced view. Only one user certificate is supported. If needed, the tool will rename the certificate and the private key into Mobile VPN Client supported form. For this purpose the tool creates a temp directory which will be removed when the tool is closed. Certificate file must be in DER- or PEM-encoded X509.3 ASN.1 format.



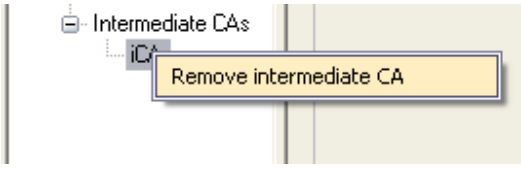
Intermediate CAs-node

Intermediate CA certificates are managed under this node. If needed, the tool will rename the certificate into Mobile VPN Client supported form (*-iCA-*.der/cer). For this purpose the tool creates a temp directory which will be removed when the tool is closed. Certificate file must be in DER- or PEM-encoded X509.3 ASN.1 format.

New intermediate certificate is added by right clicking the Intermediate CAs-node.

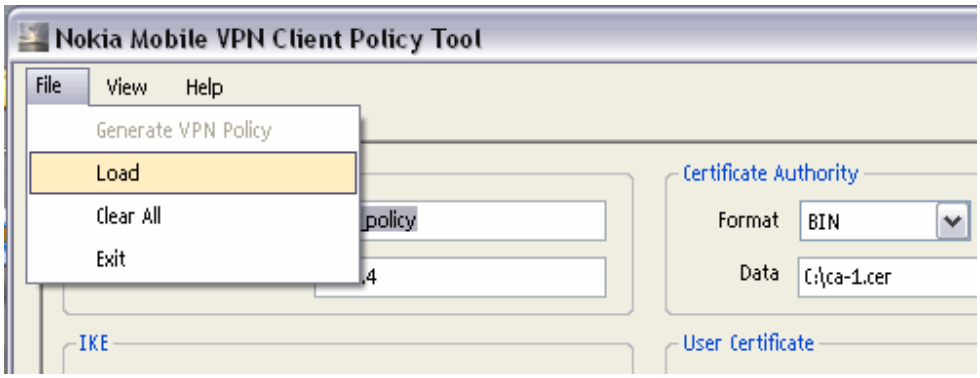


Intermediate CAs can be removed by right clicking the certificate node.



Using templates

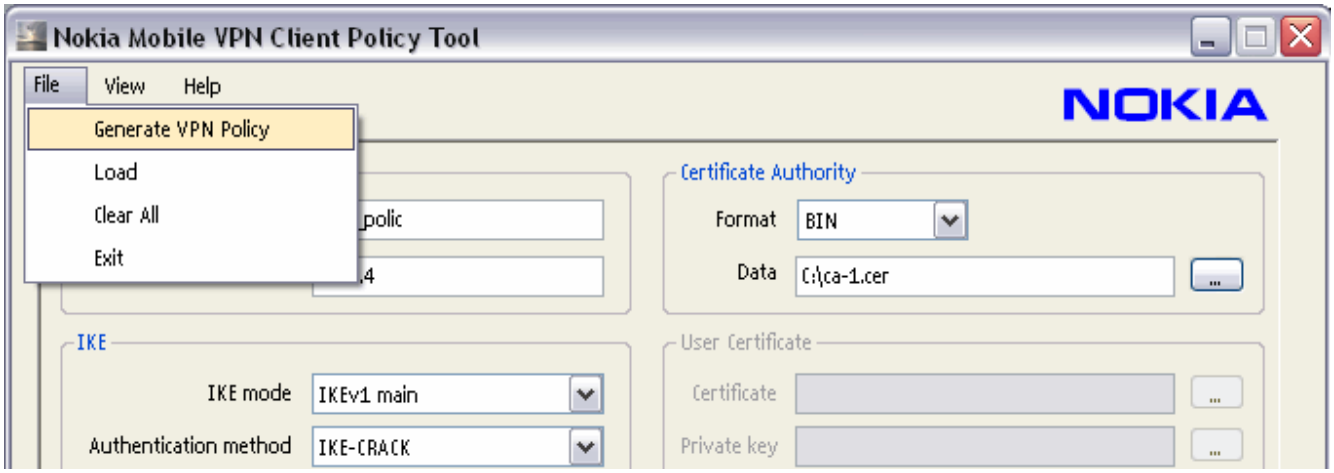
User can load policy- or vpn-files to the tool by clicking File -> Load or using drag&drop functionality. Loaded files are meant to ease the policy generation. Policy files provided by the tool contain all mandatory parameters and user has to fill only parameters that cannot be known beforehand. When policy is loaded, IKE mode and IKE authentication method cannot be changed. Loading is enabled when wizard view is active.



If vpn-file is loaded in, all certificates, private key, vpc- and PKCS#12 file inside the vpn-file are copied into the temp directory. The temp directory is removed when the tool is closed.

Generating VPN policy

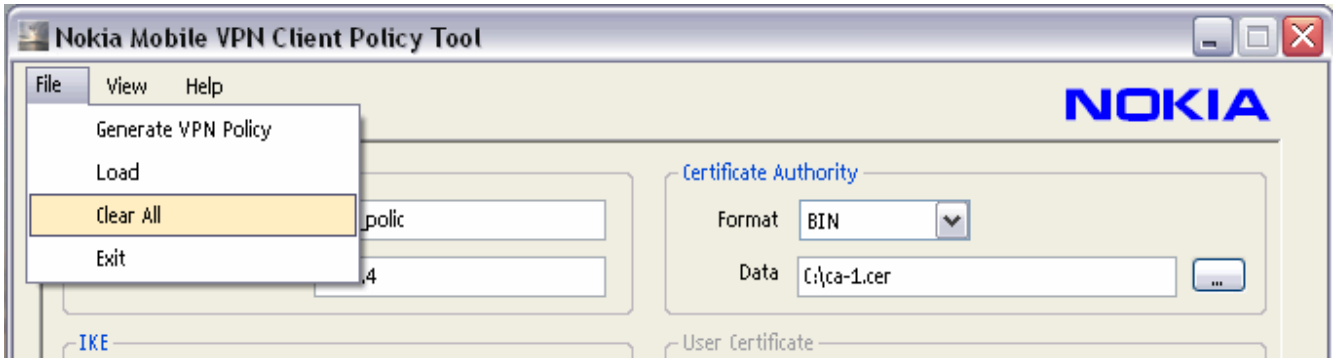
VPN policy can be created by clicking Generate VPN Policy button or File -> Generate VPN Policy from the menu bar.



The tool will create .vpn-file which can be transferred to the end device and installed by Mobile VPN client. See [MVPN_USER_GUIDE] for more details..

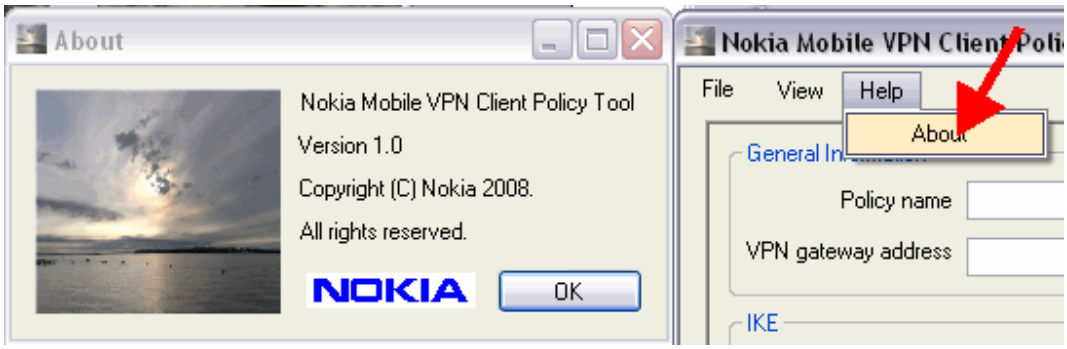
Clearing All

To erase all inserted data and start again from scratch, click File -> Clear All. This will also delete files from temp directory.



Policy Tool version

To see which Policy Tool version you have, click Help -> About from the menu bar.



Legal Notice

Copyright © Nokia 2008. All rights reserved. Reproduction, transfer, or distribution 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.

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. UNDER NO CIRCUMSTANCES SHALL NOKIA BE RESPONSIBLE FOR ANY LOSS OF DATA OR INCOME OR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES HOWSOEVER CAUSED. Nokia has a policy of continuous development and, thus, 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: europe@nokiaforbusiness.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