

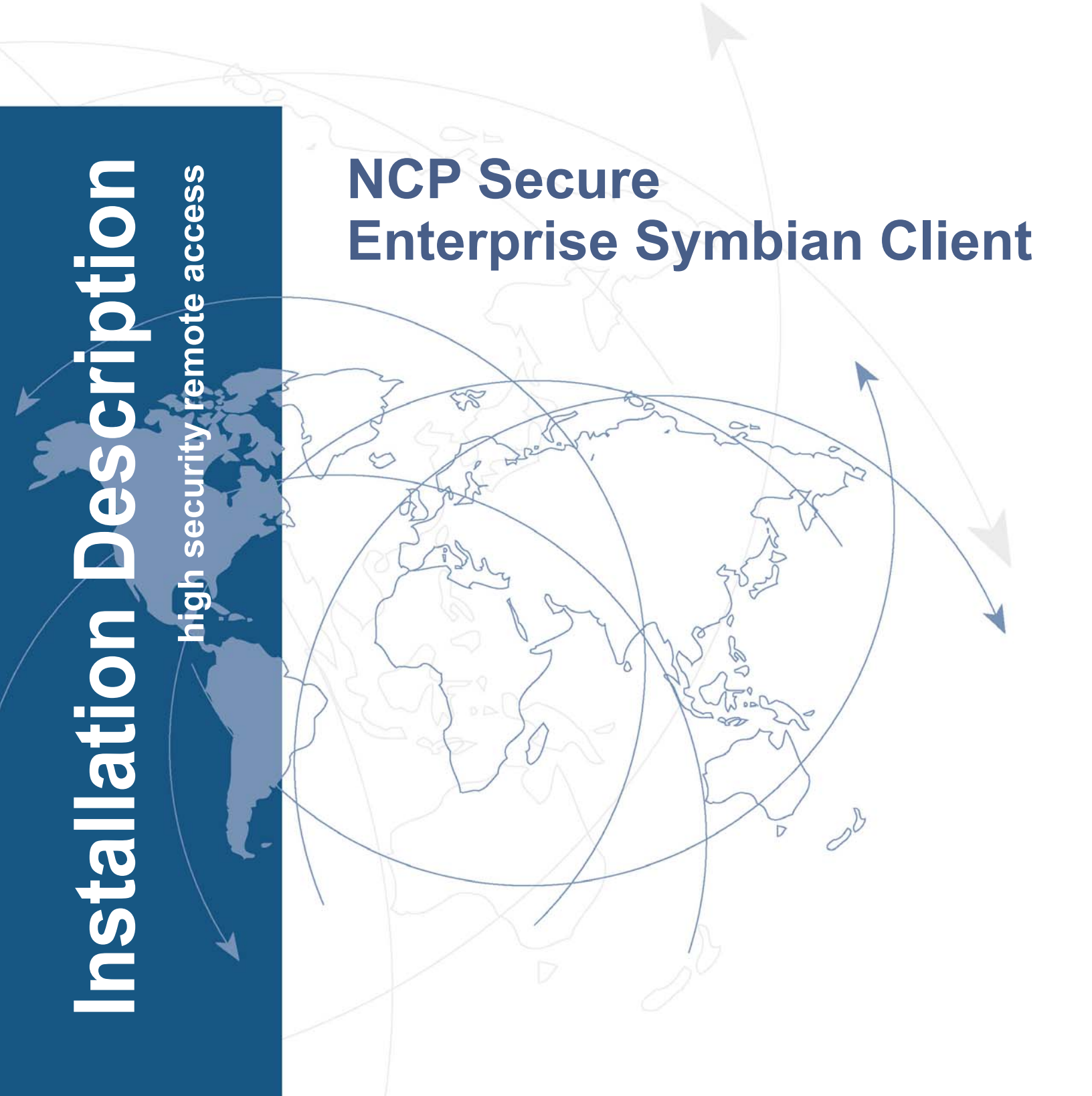


SECURE COMMUNICATIONS ■

# Installation Description

high security remote access

## NCP Secure Enterprise Symbian Client





# **Enterprise Symbian Client**

## **Installation Description and Quick User Guide**

(May 2008)



SECURE COMMUNICATIONS ■

Network  
Communications  
Products engineering GmbH

GERMANY

Headquarters:

Dombühler Straße 2

D-90449 Nürnberg

Tel.: +49-911-99680

Fax: +49 - 911 - 9968 299

Internet

<http://www.ncp-e.com/en>

E-mail: [info@ncp-e.com](mailto:info@ncp-e.com)

### Copyright

*Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.*

*NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose.*

*Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.*

*This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.*

*All trademarks or registered trademarks appearing in this manual belong to their respective owners.*

© 2008 NCP engineering GmbH.  
All rights reserved.

## Support

NCP offers support for all international users by means of Fax and Internet Mail.

Fax Hotline Number: +49 911 99 68 458

Internet Mail Address: [support@ncp-e.com](mailto:support@ncp-e.com)

When contacting NCP with your problems or queries please include the following information:

- exact product name
- serial number
- Version number
- Accurate description of your problem
- Any error message(s)

# Contents

<b>1. Installation</b>	<b>6</b>
<b>1.1 Installation der PC-Komponente Configuration Manager</b>	<b>8</b>
Installing from Hard Disc	8
Installing from NCP CD	8
<b>1.2 Installing the NCP Client Phone Component</b>	<b>10</b>
Starting the Secure Client	11
Uninstalling the NCP Secure Enterprise Symbian Client	11
<b>1.3 Configuring Destination Systems</b>	<b>12</b>
Configuration Assistant	12
- Name of the destination system	12
- Connection type (dial-up configuration)	12
- Access point	12
- VPN gateway parameters	12
- Access data for VPN gateway	13
- Static key (pre-shared key)	13
- Link firewall	13
Phonebook	14
Uploading and Downloading the Phonebook	15
Phonebook backup	15
Uploading	15
Downloading	15
<b>1.4 Licensing</b>	<b>16</b>
<b>1.5 Quick User Guide</b>	<b>17</b>
Main Monitor	17
Select another Profile	18
Establishing a Connection	18
Username and Password	18
Selecting an Access Point	18
Closing the Monitor	19
Terminating the VPN Tunnel	19
Statistics and Log Entries	19

## Installation Description



This document describes the installation of the NCP Secure Enterprise Symbian Client (consisting of PC and phone components), and the transfer of configuration data between these components.

PC component:

### **NCP Enterprise Configuration Manager Symbian**

This component is used to create phonebook entries (VPN profiles) and to synchronise the data file on the phone.

Phone component:

### **NCP Secure Enterprise Client**

NCP Secure Enterprise Client is installed on the mobile end device (phone) and is used to establish a connection to a VPN gateway. A destination system for the VPN connection can be selected from the integrated phonebook. The client monitor also shows the status of the connection to the VPN gateway.



**For more information on extensions and product versions, please go to the NCP website at <http://www.ncp-e.com>**

# 1. Installation

The software is easily installed using Setup. The procedure is the same for all versions of this software.



The following system requirements must be met to install and use the software:

## **PC component: NCP Enterprise Configuration Manager Symbian**

The current version of the Nokia PC Suite and one of the permitted operating systems must have been installed first. The mobile device with the Nokia PC Suite must be linked to the PC before the phone components are installed.

Operating systems: Windows 2000, Windows XP, Windows Vista;  
approx. 32 MB RAM and 15 MB free hard disc space.

## **Phone component: NCP Secure Enterprise Client**

The mobile device will need to be booted by switching it off and on after installation of the NCP Secure Client.

Operating systems: only Symbian OS v 9.1 or later as the basic system;  
only Nokia Series S60 3rd Edition and later\* as the interface;  
approx. 3 MB RAM and approx. 2 MB free data space

*\* For more information on extensions and product versions, please go to the NCP website at <http://www.ncp-e.com>*

The following condition must be met for data transfer between the components:

### **Nokia PC Suite**

The current version of Nokia PC Suite must be installed on the PC. This software is supplied with your Nokia mobile phone. If you accept the recommended standard installation of Nokia PC Suite, the software will install automatically using Auto-start. The connection between the PC and phone via the USB cable (or Bluetooth) will also be automatic.

### **Sequence from Installation to Starting**

Please follow the order below.

- Installation of current version of Nokia PC Suite
- Installation of “Configuration Manager” PC component
- Installation of “NCP Secure Client” phone component on the mobile device
- Restart mobile device by switching off and on
- Creation of phonebook with Configuration Manager
- Transfer of phonebook to mobile device
- Start using phone

## 1.1 Installation der PC-Komponente Configuration Manager

After the current version of Nokia PC Suite has been installed, the Configuration Manager for the NCP Secure Enterprise Symbian Client can be installed.

The Configuration Manager later configures the destination system (VPN profile), the composition of the phonebook, and its transfer to the phone (see “Configuring Destination System” section below).

### Installing from Hard Disc

If you prefer to install the software by downloading it from the NCP website, unzip the ZIP file in one of your directories. A “DISK1” subdirectory will be created automatically. In ”DISK1”, start the installation program

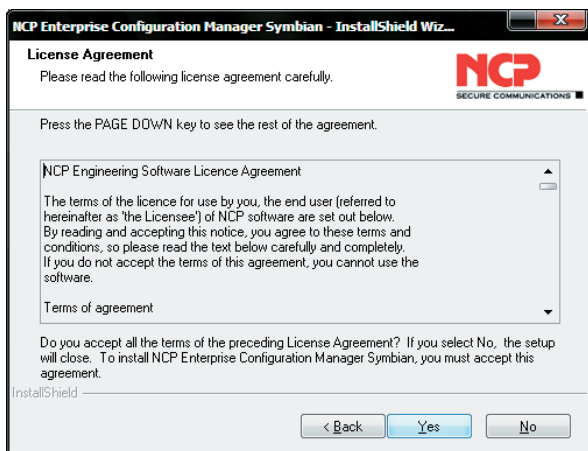
NCP\_EpCl\_Symbian\_xxx\_yyy.EXE\*.

The rest of the installation is the same as from the NCP CD.

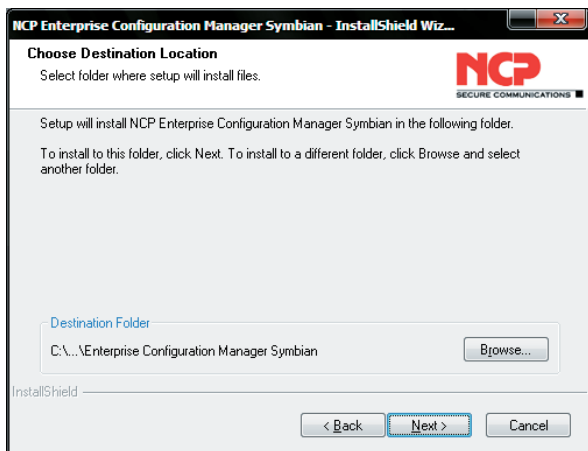
\*  $x = x = \text{version number}$ ,  $y = \text{build number}$

### Installing from NCP CD

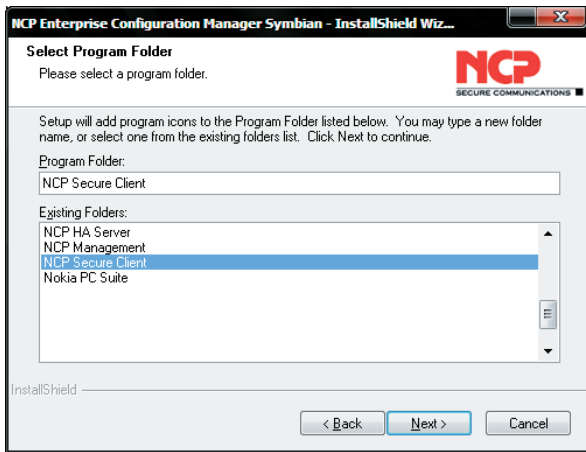
Insert the CD in the drive and wait a couple of seconds for the NCP welcome page to appear on your monitor. Select the product to be installed and click on “Install product”.



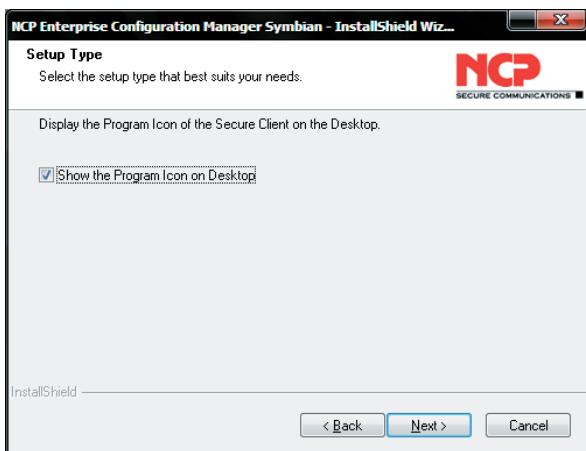
The NCP Secure Symbian Client is installed on your computer as soon as the Setup programme has prepared the Install Shield Assistant. First read the licence conditions carefully, then click on “Yes”. (See left)



Then choose the destination directory for the client software (normally Programme\NCP\Enterprise Symbian Configuration Manager), and click on “Next”. (See left)



Specify the programme file (normally “NCP Secure Client”) and click on “Next”.



In the next window, you can place a programme icon for starting the Configuration Manager on the desktop. Click on “Next”.



The Setup programme carries out the desired operations and installs the Configuration Manager on the hard disc.

Click on “Finish” to end installation. The computer does not need to be rebooted.

Leaving the setting “Start mobile device installation”, the installation of the phone component will be started after finishing automatically.

Removing this setting, the phone component can also be installed later. See the chapter “Installing NCP Client Phone Component”.

## 1.2 Installing the NCP Client Phone Component

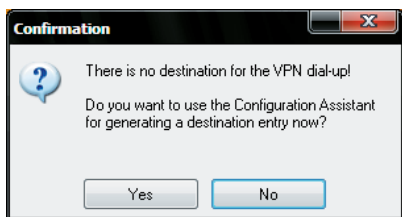
The phone component can be installed as soon as there is a connection to the mobile device via Nokia PC Suite. To connect:

### PC end

After the “NCP Secure Client” programme group has been installed, you will find the “Enterprise Symbian Configuration Manager” programme in the Windows Start menu.

Start the Configuration Manager from the Programme menu (or desktop icon).

If a confirmation window appears, you can click on “Yes” to create a destination system using an assistant (see “Destination system” below). However, this is not necessary for the installation.



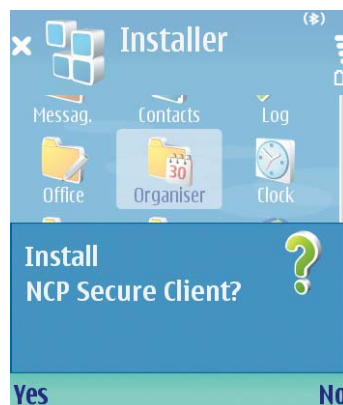
Click on “No” to continue installing the phone component.

Select “Install system / mobile device” in the Configuration Manager menu (see illustration below).

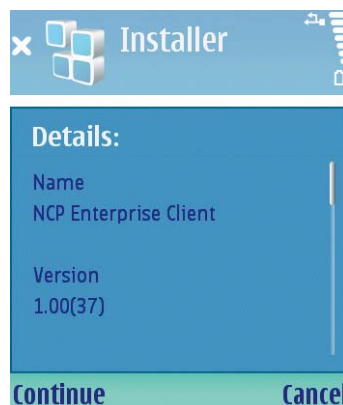


### Phone end

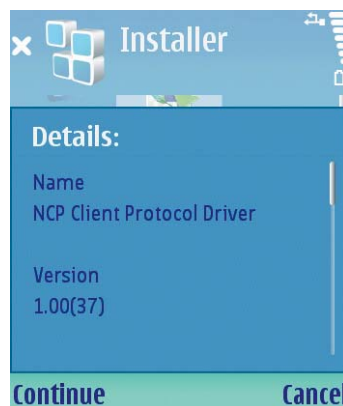
You install the phone components using the display on your mobile device. You will first require Nokia PC Suite to install the NCP Secure Enterprise Symbian Client on your mobile device.



A question will appear on the phone’s display, asking whether you want to install the client. Press “Yes”.

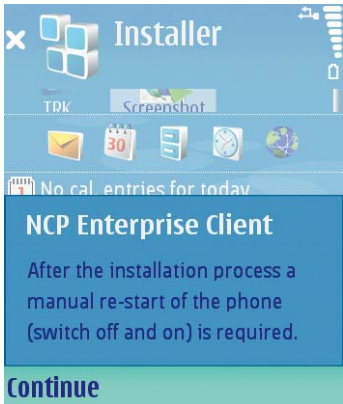


The product details and version will appear. Press “Continue”.



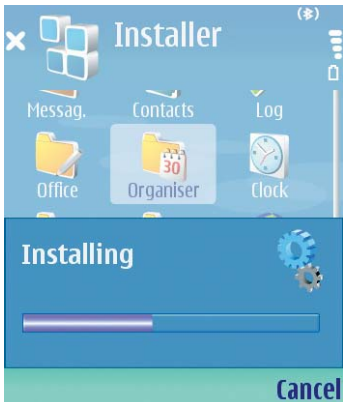
The following window informs about installing the protocol driver. Press “Continue”.

Press “Continue”.



You will be told you have to boot your mobile device after installation. Press “Continue”. (See illustration left)

Press “Continue”.



The installation process will display.

When it finishes, reboot your mobile device by switching if off and on.



The NCP Secure Client is inserted in the installation directory.



You press on the icon to start it.

## Starting the Secure Client

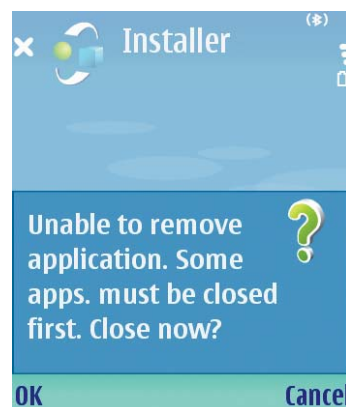
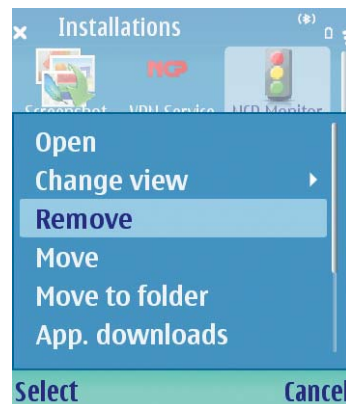
After installation of the NCP Secure Client on the Smartphone under “Installed programmes”, you need to restart the mobile device by switching it off and on.

Each time the phone is switched on, the VPN service from NCP is automatically loaded in the background, so a VPN connection to the configured destination system can be made immediately after the NCP Secure Client starts (see “Configuring Destination System” below).

## Uninstalling the NCP Secure Enterprise Symbian Client

The PC component of the Client is uninstalled using Windows System management / Software / Components.

The phone components are uninstalled using the system manager on the mobile device. The driver for the NCP Secure Client is deleted at the same time. The mobile must be switched off and on again to delete the driver from memory.



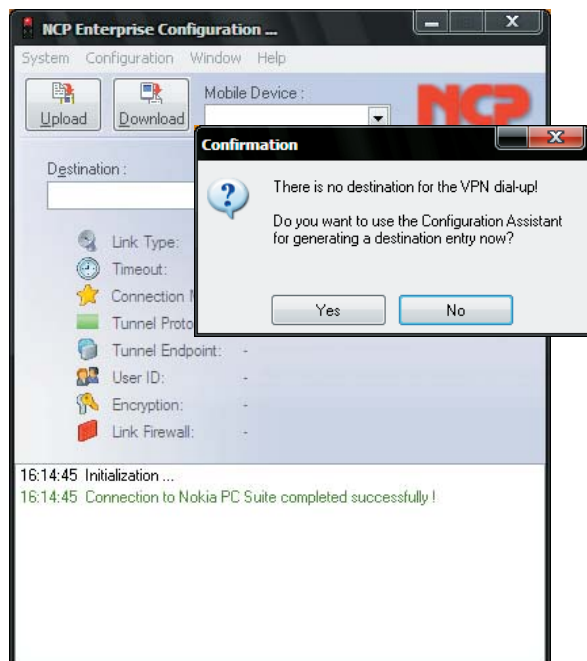
The VPN service running in the background must be terminated (closed). To do so, click on “OK”.

## 1.3 Configuring Destination Systems



A destination system is a phonebook entry in the Configuration Manager, where the most important parameters are defined: where and how a VPN connection from the NCP Secure Client is established on the mobile phone. A connection between the Smartphone and the destination system can not be established (see “Establishing a connection”) without configuring a destination system and transferring it to the mobile device (see “Phonebook / Uploading”).

After the PC component has been installed using the Configuration Manager (see above), start the Configuration Manager from the Programme menu (or desktop icon). The confirmation window (see illustration below) appears at the same time as the Configuration Manager interface. Press “Yes” in this window to start a configuration assistant automatically. The assistant is used to configure the first destination system or to create the first phonebook entry.



## Configuration Assistant



The Configuration assistant also starts when you want to add a new entry to the phonebook under “Configuration / Phonebook” in the menu (see “Phonebook” below).



IPSec connections to the company network can be established quickly using the Configuration assistant. It brings up the most vital parameters. Once you have accepted the entries in these fields, a new destination system is created. Standard values are entered for all other parameter fields in the phonebook; you can change these at a later time (see “Configuration Manager parameters” below). The destination system will be stored in the phonebook after a few configuration queries, depending on the basic setting chosen.

The sections below describe the parameters for configuring a connection to the company network via IPSec. The square brackets contain the parameter fields found in the Configuration Manager (also refer to the online help for the Configuration Manager and the description “Mobile client parameters”):

### - Name of the destination system

Enter a distinctive name for the destination system. It may include both alphanumeric and numeric characters except “+”, and be 39 characters long, including spaces [destination system].

### - Connection type (dial-up configuration)

You select the connection type to be established via the tunnel. The type can be specific to each destination system, provided you have the appropriate hardware connected and installed on your system (only “Symbian Internet access point” can be used with the current Symbian operating system [destination system]).

### - Access point

Different access points can be stored in the Smartphone (e.g. T-Mobile Internet or WLAN access point). These configured access points appear when setting up the connection for “Selection on mobile device” (see “Connection set-up” below) [destination system].

### - VPN gateway parameters

For which VPN gateway, i.e. which tunnel endpoint, should the IPSec connection be set up? Indicate here official IP address via which you can reach the VPN gateway. In the case of an IPSec con-

nection, you can also use extended authentication additionally to the authentication via a pre-shared key [tunnel parameters and IPSec options].

### - Access data for VPN gateway

Enter your code words, VPN user name and VPN password, for the tunnel connection here. (They also will be used for extended authentication, when activated; see above). If you do not want to save the password, it will be requested each time a connection is established [tunnel parameters].

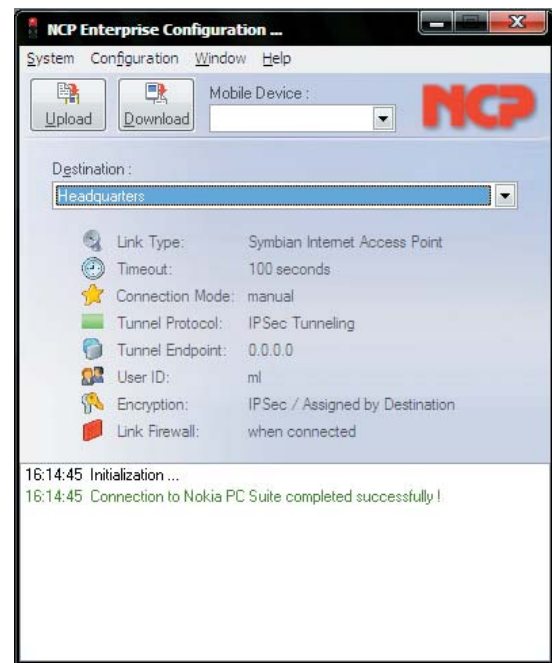
### - Static key (pre-shared key)

Common keys can be used for data encryption. Enter the key here (static key, pre-shared key) that must be stored on both sides - client and gateway. The associated string must be entered for the IKE ID, depending on selected IKE ID type [security].

### - Link firewall

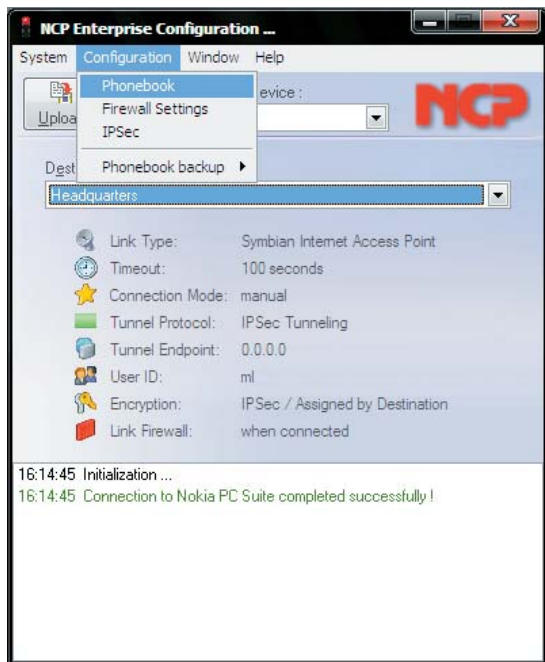
The settings for Link firewall apply only to the destination system configured here (the global firewall settings, on the other hand, are valid for all links). If you activate Stateful inspection, no data packets will be accepted from other hosts [Link firewall].

Once you click on “Finish”, the first phonebook entry is stored with the first destination system (see illustration below).

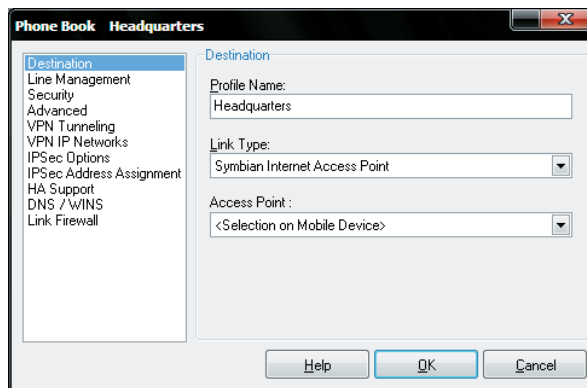


## Phonebook

The phonebook contains entries for alternate destination systems, i.e. different configuration profiles for establishing a connection to a VPN gateway. These configuration profiles can be regenerated or modified by selecting “Configuration/Phonebook” in the Configuration Manager menu.



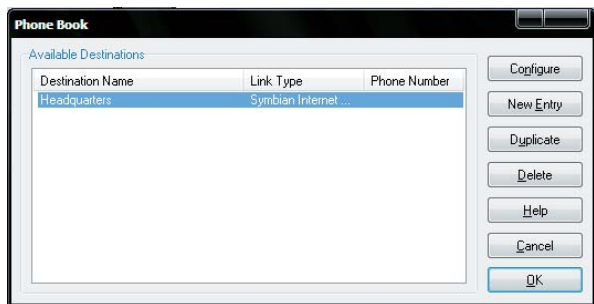
stant” above). The illustration below shows the “Destination system” parameter field for the phonebook entry “Headquarters”.



You can find a detailed description of creating destination systems and the meaning of the parameters in the description of the “Mobile client parameters” or in the Configuration Manager online help.

Because configuration profiles, i.e. the phonebook, cannot be created on the Smartphone, they must first be created in the Configuration Manager and then transferred to the Smartphone.

The phonebook displays a list of already available destination systems, with name, connection type (and call-up number, if applicable). Double-clicking on a destination system allows the configuration to be viewed and/or changed. The buttons on the right-hand side should be used as required. Pressing “Cancel” stores the phonebook without changes. Selecting “OK” accepts the changes before closing the phonebook.



If you want to modify the phonebook entry you have created with the assistant, click on “Configure” and select the parameter field where the assistant has put your entries (see “Configuration assi-

## Uploading and Downloading the Phonebook

### Phonebook backup



Please note that an existing phonebook on the mobile device will be always overwritten without asking if a new phonebook is uploaded. Similarly, a phonebook on the PC will always be overwritten when a phonebook is downloaded from the phone. If different phonebooks for different mobile devices, for example, are to be stored, this can only be done on the PC by renaming phonebook file `ncpphone.cfg` in the installation directory.



Phonebook backup via the Configuration Manager is only intended for recovering the last phonebook; the backup file `ncpphone.sav` is renamed again as `ncpphone.cfg`.

### Uploading

The phonebook with the configured destination systems is transferred to the Smartphone as follows:

Switch on the Smartphone and establish a connection between the PC and the Smartphone using PC Suite. Then press the “Upload” button in the Configuration Manager.



The transfer to the Smartphone fails and a corresponding error message appears on the PC, if the mobile device is not rebooted after installation of the client (i.e. if the VPN service is not running). In this case, start the Smartphone again by switching it off and on, then press the “Upload” button in the Configuration Manager once more.

If the NCP Secure Client has already started with an older phonebook, the older book will be overwritten and the NCP Secure Client will automatically load the new one.

If at the time of the upload there is a VPN connection from the NCP Secure Client to one of its destination systems, the existing connection will be cut by the upload without warning and the older phonebook overwritten.

### Downloading

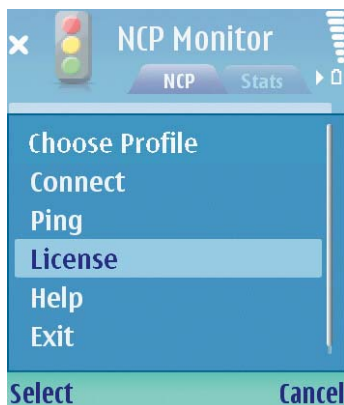
Press the “Download” button in the Configuration Manager to download a phonebook from the mobile device to the PC. (In this case too, the mobile device must be started and a connection established between the PC and the Smartphone using PC Suite.)

During downloading of the phonebook from the Smartphone to the PC, the book on the PC will be overwritten. If an existing phonebook on the PC is to be retained, it must have its own backup. It is located as file `ncpphone.cfg` in the installation directory (see above).

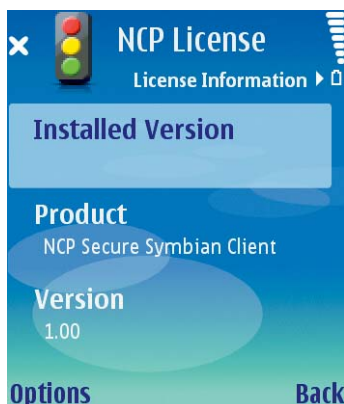


If a download fails, despite there being a connection between the PC and the Smartphone, the mobile device needs to be rebooted by switching it off and on again.

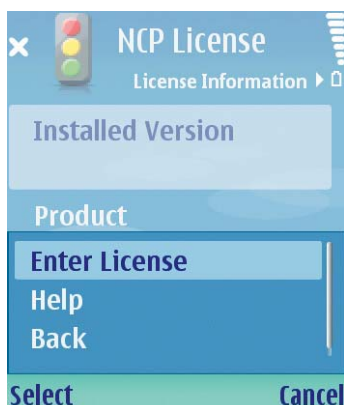
## 1.4 Licensing



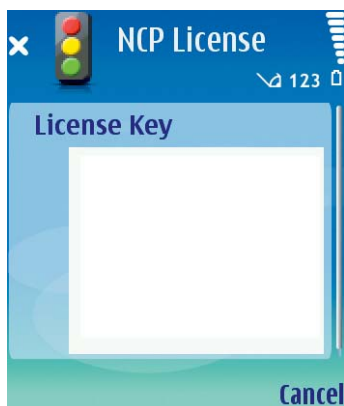
If you select menu item “License”, this window opens displaying the installed and, if applicable, licensed software version.



If the software is not yet a full version and if the test version is to be licensed, “Enter license” can be used to open the input window for the license code.



After entering the license code and serial number, use the right arrow button or “OK” to store the code and release the full version of the software. If you click on “Cancel”, the code will be rejected and you will be returned to the top window.



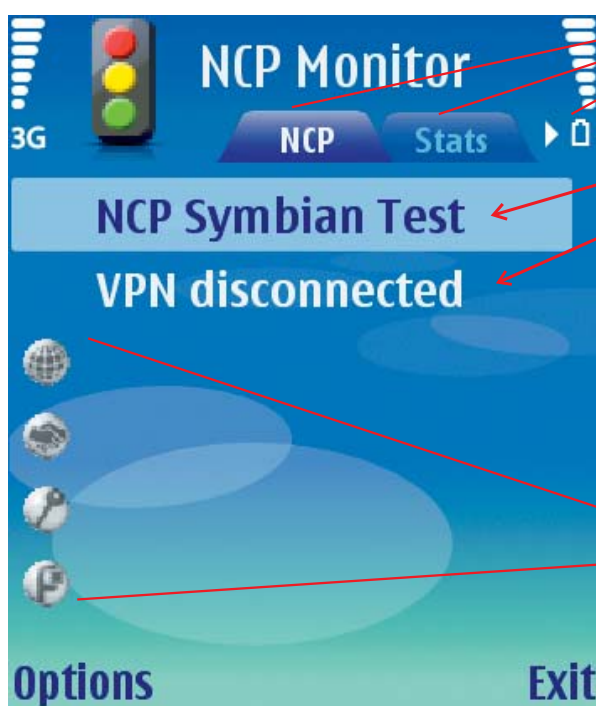
Once the code has been entered correctly, the license data will be displayed in this window.

## 1.5 Quick User Guide

Once you have transferred the phonebook with the configured destination systems to the smartphone, you can select a profile which was configured on the Enterprise Configuration Manager Symbian.

### Main Monitor

When you have started the client, the main monitor displays the destination system highlighted which was selected in the configuration manager in the phonebook. (See picture below)



#### Tabs:

There are three tabs: NCP, Stats and Log. The NCP tab displays: the **current profile** and the **VPN tunnel state**.

#### Stats:

Statistics and informations of the current connections

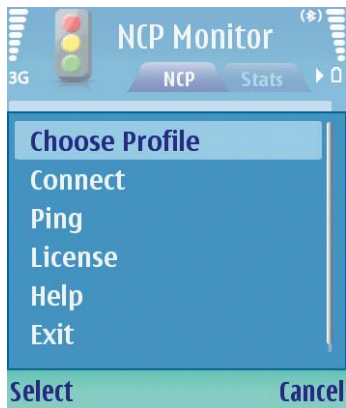
#### Log:

(In the picture of the left not displayed)  
Log entries for support purposes

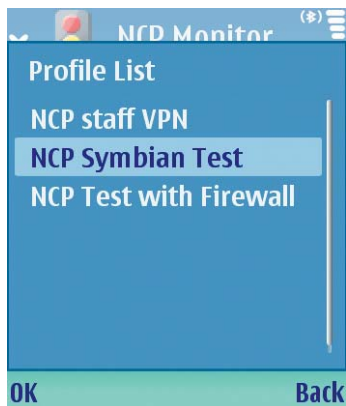
#### Status displays:

The client monitor displays different icons depending on the configuration; these icons can change the colors from grey to green depending on the phases of the connection setup.

**Select another Profile**

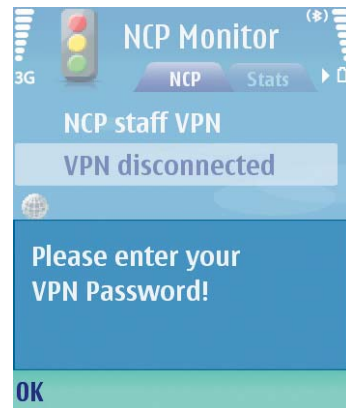


To select another destination system, press the action button or “Options” and afterwards “Choose Profile” (see picture on the left).

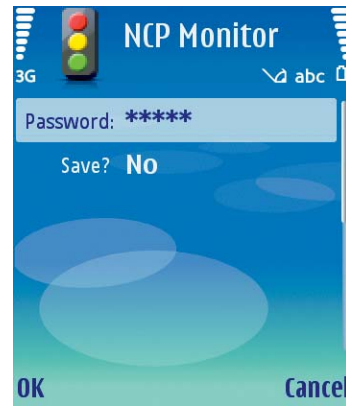


When selected the required destination system from the list, press “OK”.

**Username and Password**

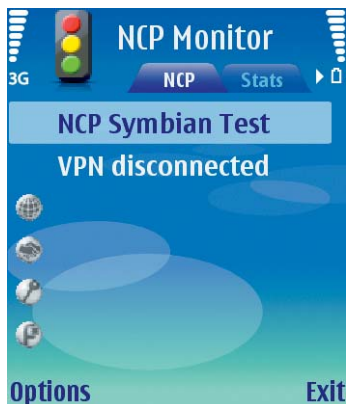


If username and/or password was not entered in the phonebook of the configuration manager it will be required when the connection is going to be established. Press “OK” and enter your password.

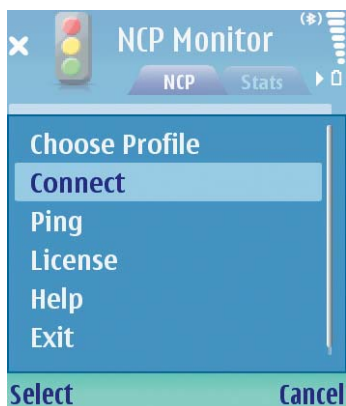


When you have entered username and/or password you can save the entry in the phonebook on the smartphone by pressing “save”. Then press “OK”.

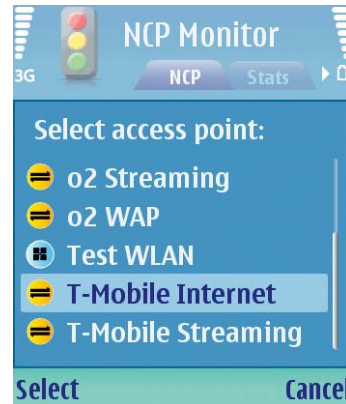
**Establishing a Connection**



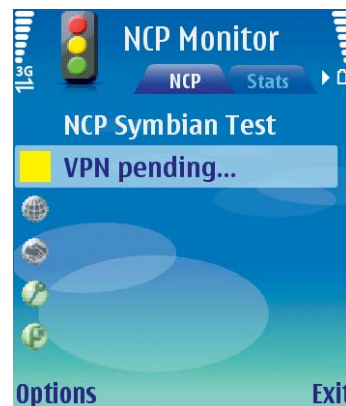
To establish the VPN tunnel to the destination system press the line with the tunnel state or “Options” and then select “Connect”.



**Selecting an Access Point**



After that select one of the preconfigured internet access points (IAP) and press “Select”.

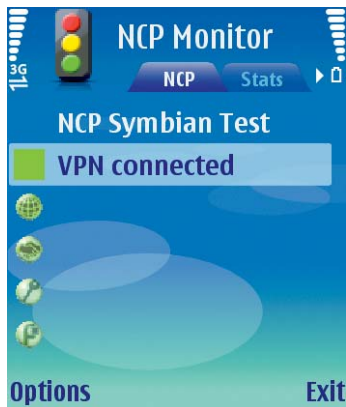


Now the connection will be established.

When starting an application (E-Mail, Web Browser) be sure that the IAP is the same as the one for the tunnel connection!

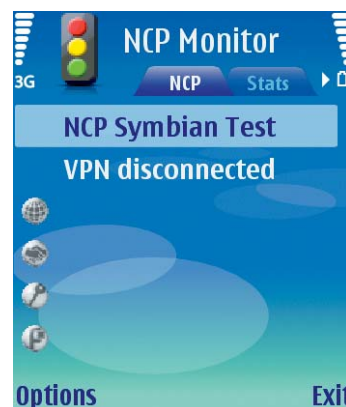


### Closing the Monitor



By pressing “Exit” the Monitor can be closed, but the connection will not be disconnected because the client will be active in the background.

### Statistics and Log Entries

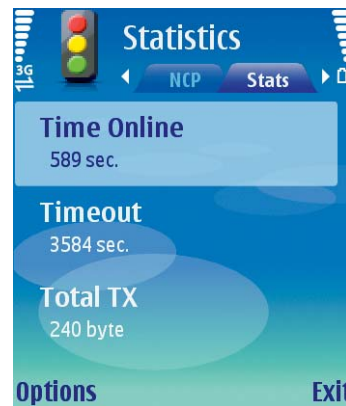


Selecting the tabs “Stats” and “Log” in the main monitor, you can read statistics and log entries of the current VPN tunnel connection.

### Terminating the VPN Tunnel



After finishing the application you can terminate the tunnel connection by pressing the menu “Options / Disconnect”...

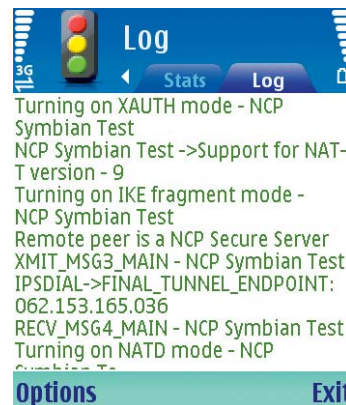


The statistic data display connection infos about: Time Online, Timeout, Total Tx/Rx Bytes; Encryption, Security Mode and views the own VPN IP address.



... or by highlighting the tunnel status and then press the action button.

When this question in the monitor (see picture on the left) is displayed, press “Yes” and the tunnel will be terminated.



The log windows shows informations to enable qualified system technicians to perform low level traces for fault finding and debugging purposes.