

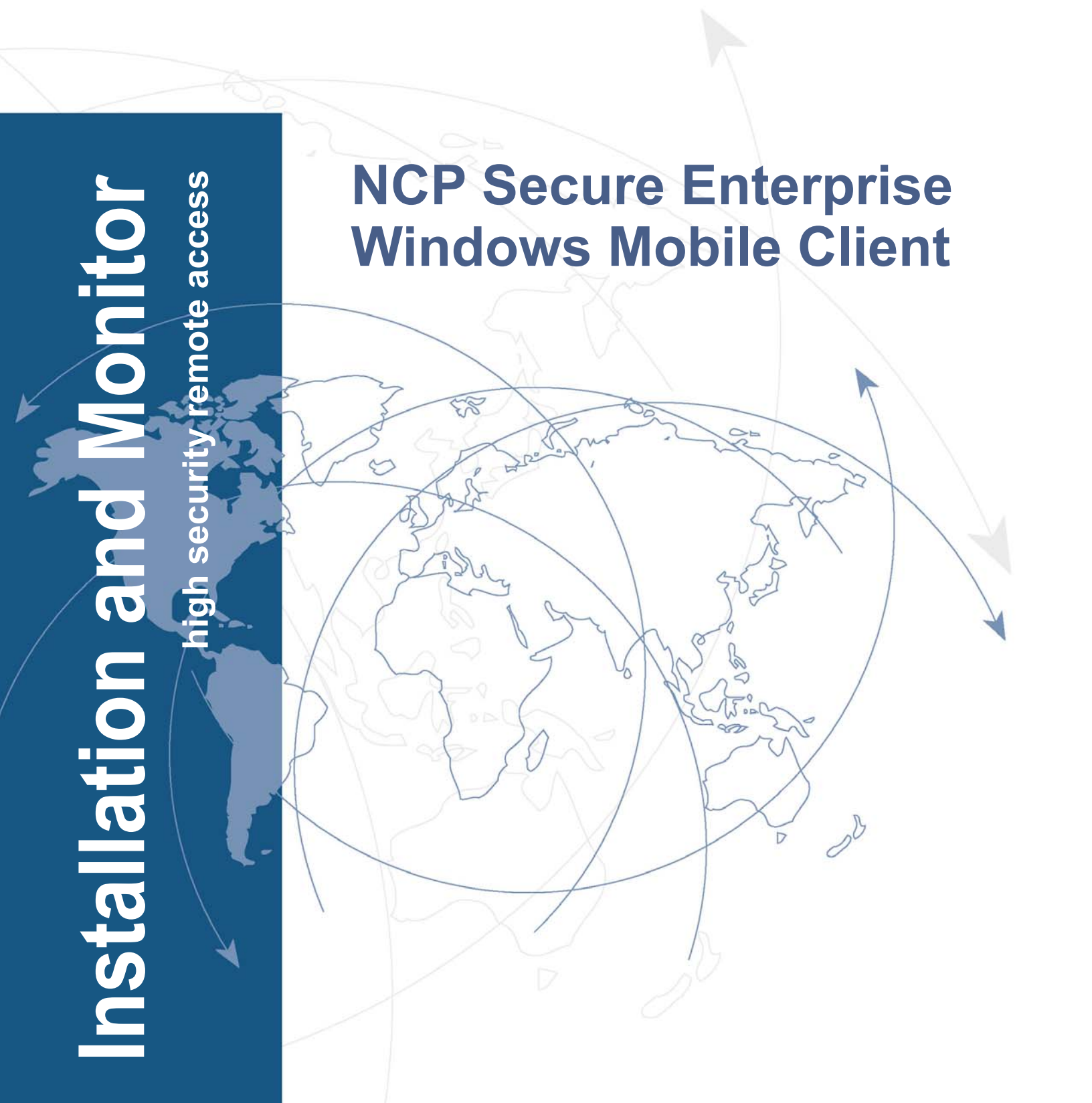
**NCP**

SECURE COMMUNICATIONS

# Installation and Monitor

high security remote access

## NCP Secure Enterprise Windows Mobile Client





# **Installation and Monitor**

## **of the Secure Enterprise Windows Mobile Client**

## 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

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)

NCP will do its best to respond as soon as possible, but we do not guarantee a fixed response period.



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>

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, Dombühler Str. 2, D - 90449 Nürnberg, Germany.*

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

© NCP engineering, January 2011

<b>Contents Overview</b>	<b>5</b>
<b>Product Description</b>	<b>6</b>
Performance Features	6
Performance Features for Mobile Operation	7
<b>Installation Requirements</b>	<b>8</b>
Operating Systems	8
Communication Interfaces	8
Requirements for Certificate Application	9
Supported Interfaces and Formats	9
CA Certificates	9
<b>Sequence from Installation until Commissioning</b>	<b>9</b>
<b>Installation of PC Component Configuration Manager</b>	<b>10</b>
<b>Client Installation on the Mobile Device</b>	<b>12</b>
Commissioning	12
<b>Configuration of a Profile with the Configuration Manager</b>	<b>13</b>
Connection to the corporate network via L2Sec	14
Connection to the corporate network via IPSec over L2Sec (only Enterprise)	14
Connection to the corporate network via IPSec	14
Establish connection with the Internet	14
<b>Data Synchronization between PC and Mobile Device</b>	<b>15</b>
Upload of Profile Settings	15
Download of Profile Settings	15
Refresh Modem Data	15
Upload PKCS#12 File	15
Upload CA Certificate	15
<b>Multi Certificate Configuration</b>	<b>16</b>
<b>Monitor Interface and Symbols</b>	<b>18</b>
Security Policy	18
PIN State	18
Firewall	18
Friendly Net Detection	19
EAP Status	19
<b>Connection Establishment and Symbols of the VPN Connection</b>	<b>20</b>
<b>Monitor Popup Menus</b>	<b>21</b>
Licensing	22
Auto-PowerOff	23
Minimize on Exit	23
Ping	23
Hotspot Logon	24
Requirements for Hotspot Logon	24
Hotspot Configuration	24
PocketPC Connection Manager	25
EAP	25
Certificates	26
<b>Extended Installation and Configuration</b>	<b>28</b>
Autostart of NCP Client Service	28
Command Line Options for ncpmon.exe	28
Cold Start Installation	28
<b>Disconnection</b>	<b>29</b>
Interruption and Error	29
Manual Disconnection	29
Automatic Disconnection	29
<b>Uninstalling</b>	<b>30</b>
Uninstalling the Client on the Mobile Device	30
Uninstalling the PC Component	30

# Installation and Monitor



This dokumentation describes the installing of the NCP Secure Enterprise CE Client.

Furthermore the synchronisation between PC and Mobile Device is described as well as the functions of the popup menus on the mobile device.

---

## Contents Overview

- **Product Description**
- **Performance Features**
- **Performance Features for Mobile Operation**
- **WLAN Handover and Roaming**
- **Automatic Re-establishment when Link is interrupted**
- **Network Login despite Standby Operation**
- **Installation Requirements**
- **Installation**
- **Commissioning**
- **Configuration of a Profile**
- **Data Synchronisation**
- **Multi Certificate Configuration**
- **Connection Establishment and VPN Symbols**
- **Monitor Popup Menus**
- **Licensing**
- **Hotspot Logon**
- **Extended Installation**
- **Disconnection**
- **Uninstalling**

## Product Description

NCP Secure Enterprise CE Client consists of two software components:

### NCP Enterprise Configuration Manager CE

This component is used to create the profiles, i.e. the configuration of the connection parameters which are necessary to establish a connection to the remote station. This component is also used to synchronise the data inventory on the mobile terminal. Operating systems: Windows XP / Vista / 7.

### NCP Secure CE Client

NCP Secure Enterprise Client is installed on the mobile terminal and is used to establish a connection to a VPN Gateway. Depending on requirements it is possible to select the relevant profile settings to establish a VPN connection to the remote station. The client monitor also displays the connection status to the VPN Gateway.

Operating systems: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2002), Windows CE.net 4.2 (Windows Mobile 2003 for Pocket PC), Windows CE 3.0 / 4.2/ 5.0 (Windows Mobile 5/ 6/ 6.1/ 6.5).\*

### Performance Features

NCP Secure CE Client is available in Enterprise and Entry versions. The difference between the products is that the Enterprise CE Client Software can be managed centrally with NCP Secure Enterprise Management (SEM) while the Entry version cannot.

The communication software supports **Virtual Private Networks (VPN)** as well as a **Public Key Infrastructure (PKI)** and is used for universal teleworking in user-defined remote access VPN environments. High security data connections can also be established to VPN Gateways of well-known providers on the basis of **IPsec standards**. The data transfer is carried out via any public mobile networks, the internet as well as wireless mobile networks such as wireless LANs business premises and at hotspots. Mobile teleworkers can access central data inventories and applications using their Pocket PC, handheld or tablet PC from anywhere. Another interesting application area is mobile data collection using an integrated barcode reader in the warehouse and then transferring the data via WLAN into the central inventory software.

Universal implementation possibilities require comprehensive security mechanisms. In addition to

**VPN tunneling** the most important integrated components are: **data encryption**, a **dynamic personal firewall**, support of **OTP (One-Time Password tokens)** and **certificates** in a PKI (Public Key Infrastructure). Policies for ports, IP addresses and segments can be defined via the Personal Firewall.

Provided that the algorithms of the Microsoft operating system has been validated as conformant to FIPS 140-2 (certificate #560), the VPN communication of the client is conformant to the **FIPS standard**.

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

The respective modules can be configured in the IPsec Settings .

An additional security criterion is “**Friendly Net Detection**” i.e. automatic detection of secure and non-secure networks. The appropriate firewall rules are activated or deactivated depending on whether a friendly net is detected. The NCP Dialer also offers protection against costintensive outside dialers.

“**Easy-to-use**” - simple installation and operation of the client software. Convenience is ensured by the integrated configuration wizard for the configuration PC and an intuitive graphic user interface on the mobile end device.

To the remote client a **private IP address can be assigned by the central Secure Enterprise Gateway**. This private IP address can be assigned either permanently or variably (dynamically) from an address pool, as required. If needed the client can retain a one-time assigned IP address, even in manual connection mode, in spite of physical connection clearing. This means that the logical connection between remote client and central resource remains intact. Even accessing networks in different local area networks poses no problem, in spite of changing IP addresses. The remote user can always be identified with the same name in the corporate network, wherever he/she is located. Integration in a DDNS (Dynamic Domain Name Service-Protocol ) structure is also possible. Optionally the connection to the central server and connection monitoring are automated unnoticed in the background of the user's activities. The NCP Secure Enterprise Client can be universally implemented in any remote access environment and supports the routable protocols TCP/IP.

\* Die Entry-Version unterstützt nur Windows Mobile 5/ 6/ 6.1

## Performance Features for Mobile Operation

### WLAN Handover and Roaming when Changing Mobile Network

Changing between access points in a WLAN or on different mobile networks (e.g. from WLAN to UMTS) during a data connection to the company network are carried out without the user noticing any interruption in the connection. There is no need to restart the mobile terminal. A tunnelled session to the gateway remains established. The allocation of dynamic IP addresses is controlled automatically within the connection management.

### Automatic Re-establishment when Link is interrupted

If data is transmitted from the central office to the mobile terminal in a VPN tunnel, e.g. in the event of an email push service and if the link is interrupted, for example, due to a dead spot, then the NCP client re-establishes a secure connection to the central office as soon as the link becomes available again.

### Network Login despite Standby Operation or switched off Mobile Device

PDAs, MDAs etc are, like all mobile terminals, operated with batteries. In order to save energy, these terminals switch automatically into standby mode if no data is transferred during network access. Or they are deliberately switched off by the user. In order to guarantee a continuous operation in these cases, the user remains logged into the company network (reservation of the IP address). He can continue to work at any time without having to login again.

### Simple Operation

The intuitive graphical user interface (monitor) shows all connection parameters (dial in, authentication, encryption, data compression) at the mobile terminal. The user can track the complete connection establishment and is informed about the connection status at all times. In the event of an error, it is possible to get the relevant information fast and precisely from the central support.

### High Security

A strong cryptography with an encryption length more than/equal to 128 bit symmetrically (3DES, Blowfish, AES) and 1024/2048 Bit asymmetrically (e.g. RSA), ensures highly secure data. Furthermore, a new encryption is generated for every connection.

## Technical Data



The technical data is listed on the data sheet for the NCP Secure Enterprise CE Client:

[http://www.ncp-e.com/fileadmin/pdf/datasheets/NCP\\_DS\\_Enterprise\\_Windows\\_Mobile\\_Client.pdf](http://www.ncp-e.com/fileadmin/pdf/datasheets/NCP_DS_Enterprise_Windows_Mobile_Client.pdf)



For further information visit the NCP website:  
<http://www.ncp-e.com>

## Installation Requirements

Software installation can be easily carried out via setup. The installation process is identical for all versions of this software. The following system requirements have to be met for the use and installation of this software:

### Operating Systems

#### NCP Enterprise Configuration Manager CE

Prior to installation, software for data synchronisation between PC and mobile terminal needs to be installed in addition to the admissible operating system. For Windows XP use ActiveSync as of version 4.x, for Windows Vista and Windows 7 use the Windows Mobile Device Center. The mobile terminal has to be linked with the PC via this software before the Secure Client is installed on the mobile terminal. This software also enables the exchange of configuration data (profile) between mobile terminal and PC.

The current version and future versions of the Secure Client are only checked for quality control on Windows XP, Windows Vista and Windows 7. The PC requires 32 MB working memory and 25 MB free hard disk space.

#### NCP Secure Client

One of the following operating systems has to be installed on the mobile terminal: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2002), Windows CE.net 4.2 (Windows Mobile 2003 for Pocket PC), Windows CE 5 (Windows Mobile 5/ 6/ 6.1/ 6.5). Furthermore:

- approx. 3 MB program storage devices
- approx. 2 MB free data storage
- ARM-Processor

### Communication Interfaces

The connection to the VPN Gateway is carried out via the mobile terminal. A PDA, MDA, tablet PC or Smart Phone is used as a terminal. All established PDA-Mobile combinations are supported since either the NCP-Dialer or the Microsoft RAS-Dialer may be used to establish a connection. Corresponding Windows CE compatible drivers are required.

#### Analogue Modems and Cellular Phones

The modem has to be correctly recognized by Windows CE in order to communicate via modem (or mobile phone).

Modem drivers which support the Hayes command set are integrated into Windows CE. Windows CE also supports most mobiles with an IR interface and/or Bluetooth integrated modem.



The modem data is downloaded from the mobile terminal at the start of the PC component or via the monitor interface of the PC component. Please ensure that a connection between PC and mobile terminal is established at this point.

#### LAN Adapter (LAN over IP)

A LAN-Adapter (Ethernet or Wireless LAN) has to be installed on the mobile terminal in order to operate the Client software with the connection type “LAN over IP” in a local area network.

## Requirements for Certificate Application

### Supported Interfaces and Formats

The secure client supports the following interfaces / formats:

- Smartcards: certgate, PKCS#11
- Soft certificates: PKCS#12 file

Drivers in the form of a PKCS#11 library are supplied with the software for the card reader or token. Instead of reading out the certificate of a Smart Card via a chip card reader, a soft certificate (PKCS#12 file) can also be used.



Please note: Before you undertake a certificate configuration with the PC component of the client, the information about available chip card readers must have been transferred from the mobile device to the PC. Because the NCP Client Service creates these, the NCP Client Service must have been started before starting the PC component. To transfer this data a connection between PC and mobile device is required.

### CA Certificates



The administrator of the corporate network specifies which certificate issuers can be trusted. This is done by copying the CA certificates of his choice into the installation directory under <CACERTS>. Currently only the binary format DER is supported for issuer certificates (extensions DER, CRT, CER).

Retrospectively, issuer certificates can be distributed automatically via the Secure Management Server (only to Enterprise Clients) or the user can save them himself in the relevant directory (Entry version).

If the secure client receives the certificate of a remote station, then the NCP client will determine the issuer by searching the issuer certificate initially on smartcard or USB token or in the PKCS#12 file and finally in the installation directory under <CACERTS>. If the issuer certificate cannot be found then the connection will not be successful. (If no issuer certificates are available, then no connection is allowed.)



If soft certificates are created with the PKI plug-in of the Management Server then the issuer certificate is saved in the PKCS#12 file.

## Certificate Configuration



Please ensure that: Path and name of the PKCS#12-file given with the configuration manager indicates the storage location of the file within the mobile terminal!

In order to transmit the PKCS#12-file, the menu item “Configuration / Upload PKCS#12 File” within the configuration manager can be used. If this function is used, then the certificate path is entered automatically in the certificate configuration as follows:

```
%INSTALLDIR%\CERTS\<PKCS#12-Filename>
```



Note the section **Multi Certificate Configuration** in this manual.

## Sequence from Installation until Commissioning

- **Installation of PC Component**
- **Client Installation on Mobile Device**
- **Start of NCP Client Service on the Mobile Device for Certificate Application**
- **Configuration of a Profile with the Configuration Manager**
- **Transmitting the Profile Settings**  
(and the Certificate if applicable)
- **Client Commissioning on Mobile Device**



**Please adhere to this sequence!**

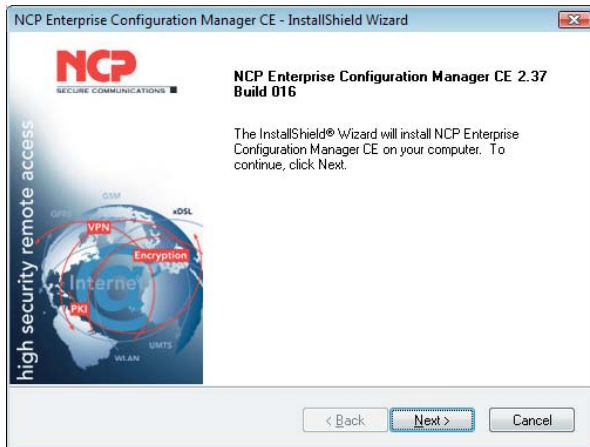
## Installation of PC Component Configuration Manager

Once the ActiveSync or Mobile Device Center is installed, the configurations manager for the CE Client may be installed.

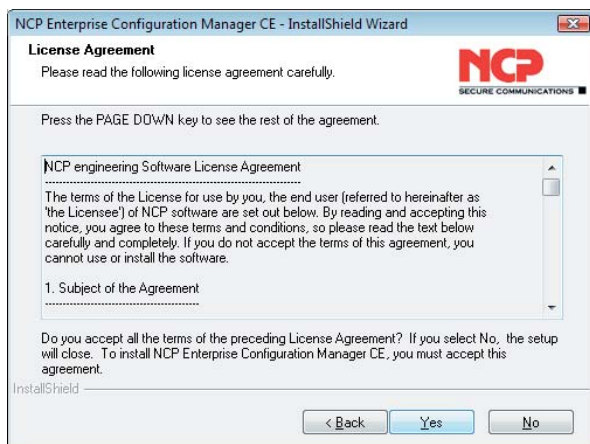
The configurations manager is used to configure the profiles later and to transfer the profiles to the mobile terminals.

### Install from Hard Disk

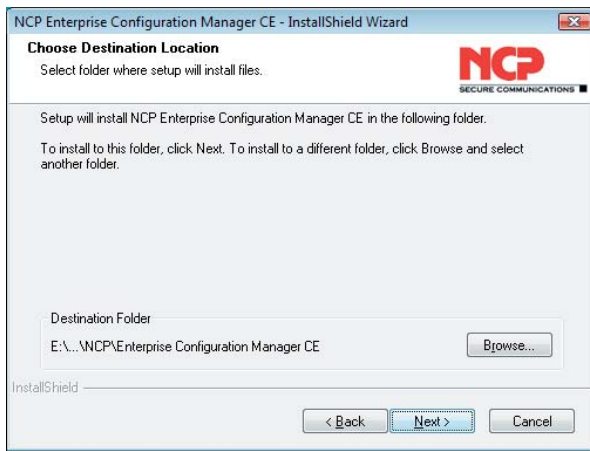
If you want to install the software after you downloaded it from the NCP website, then unzip the zip-file into the directory you created. If the sub-directory <DISK1> you created is created during unzipping, then start the installation program SETUP.EXE from this location.



Initially the configuration manager will be installed on your computer; once the setup program prepared the install-shield assistant. (Ill. on the left)



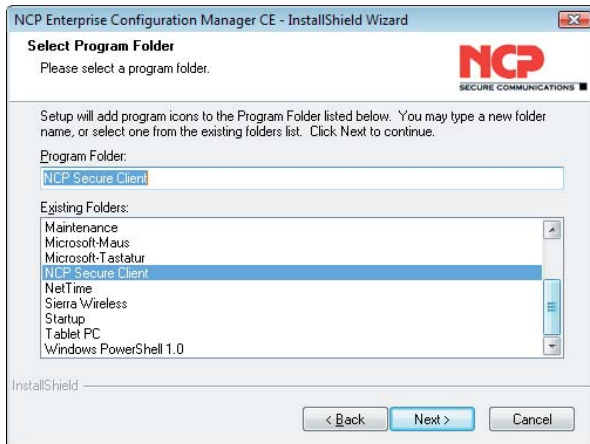
Read the license agreement carefully before you confirm with “Yes”. (Ill. on the left)



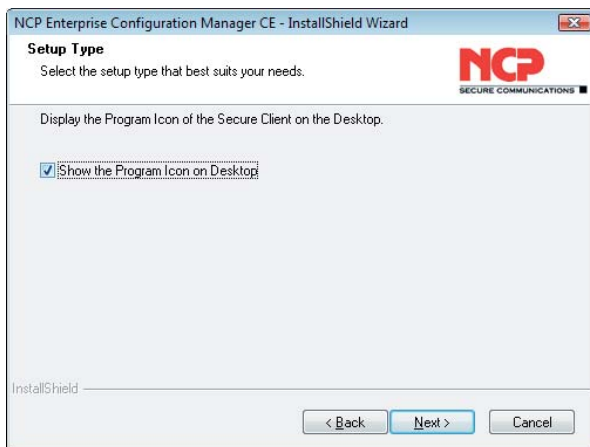
This is where you specify the destination directory for the client software. Standard is:

<Programs\NCP\Enterprise Configuration Manager CE>

... and click on “Next”. (Ill. left)



Continue by determining the program folder (standard is “NCP Secure Client”) (Ill. left) ...



.... and decide if you want to display the configuration manager program icon on your desktop. (Ill. left)

Then the files will be copied, the registry entries are created and the settings are executed.

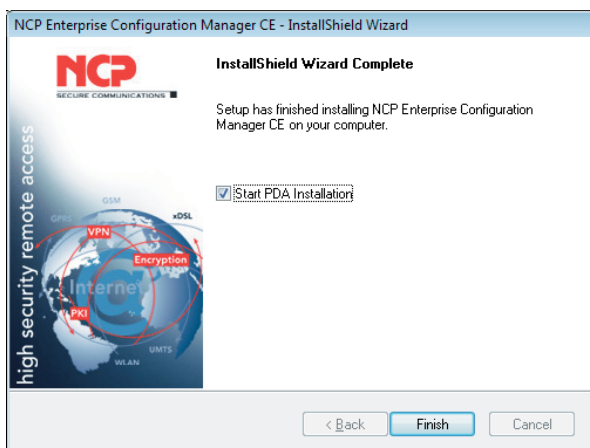
In the last installation window you can select if you want to continue immediately with the client installation on the mobile terminal or if you wish to do this at another time.

If you keep the displayed settings, then once the installation is completed and confirmed with “Finish”, the client installation is started for the mobile terminal.



Please note, that you require a connection to the mobile terminal via ActiveSync or Windows Mobile Device Center.

If you remove the setting of the automatic installation, then it is possible to install the client for the mobile terminal at a later date. If you click “Finish” the configuration manager installation is completed and the **configuration assistant** is started.



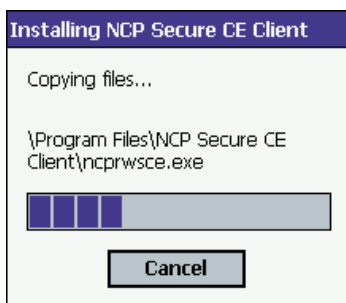
## Client Installation on the Mobile Device

If you did not proceed automatically with the client installation on the mobile terminal, then you need to start up the “Installation of mobile terminal” via the system menu of the configuration manager once you completed installing the PC component.

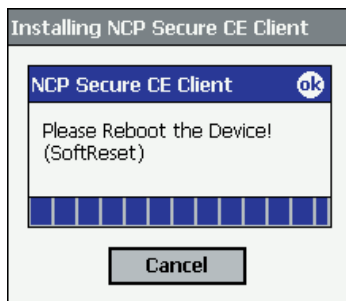


Please ensure that a connection between PC and mobile terminal is established at this point.

Initially the data for the NCP Secure CE Client is transferred. (Windows Mobile 5.0 will give you a notification that the software is not signed.)



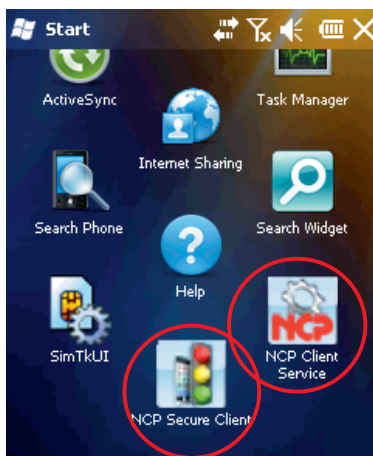
Once the data transfer is complete, check the monitor of your mobile terminal: The transferred data is unzipped on the mobile terminal.



Once the data is unzipped you are prompted to do a soft-reset. This completes the installation for the mobile component.

On completion of the soft-reset you will find in the program file the icons for

- NCP Client Monitor and
- NCP Client Service



## Commissioning

Please note: Before starting the monitor the service has to be started! When starting the monitor without the service a message box will call your attention to start the service with another click. The service can also be started automatically.

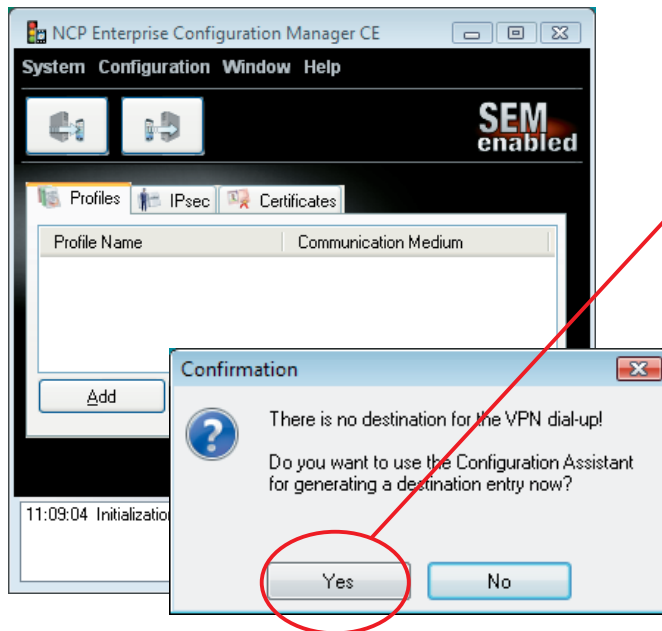


See **Autostart of the Service**.

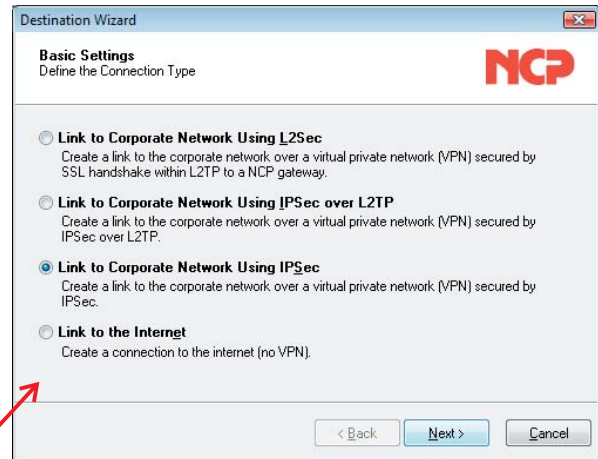
Before you can establish a connection, the **profile settings** created in the configuration manager and, if applicable, the certificate data have to be transferred to the mobile device using **data synchronization!**

## Configuration of a Profile with the Configuration Manager

If the configuration manager is started immediately after the installation, then the “configuration assistant” is started automatically – assuming that you have installed the secure client for the first time or you deleted the profile settings. They are located on the PC in the user directory (different between Windows XP and Vista) as ncpphone.cfg.



The assistant (Ill. above) gives you the option to create a VPN connection.



If you use this option, then the assistant will guide you through the configuration of the most important parameters and will create the relevant profile settings as per your input.

All required parameters will be displayed. Once you have completed your entries for these fields, the new profile is ready to use. All other parameter folders will be populated with default values, which you can modify at any time, once you have completed the profile creation by the configuration manager. (Ill. below)



After clicking on “Profiles” in the configuration menu the requested profil setting can be selected and the configuration can be modified accordingly.

A new profile can be created with the assistant at any time (see the following page).

The configuration assistant will always be started by clicking on “New Entry” in the profile settings. The wizard will offer various connection types for the new profile. Following user selection of the required connection type, and answering a few prompts, the new profile will be stored. Please note the following data, which will be required for the configuration:

### Connection to the corporate network via L2Sec

- Profile Name
- Communication Medium
- Access data for the Internet provider (User ID, Password, Phone Number)
- VPN Gateway parameters (VPN Gateway, Tunnelsecret)
- Certificate utilisation
- Access data for VPN Gateway (VPN User ID, VPN Password)
- Static Key (Preshared Key) where certificate is not used
- Firewall Settings

### Connection to the corporate network via IPsec over L2Sec (only Enterprise Client)

- Profile Name
- Communication Medium
- Access data for the Internet provider (User ID, Password, Phone Number)
- VPN Gateway parameters (VPN Gateway, Tunnelsecret)
- Certificate utilisation
- Access data for VPN Gateway (VPN User ID, VPN Password)
- Static Key (Preshared Key) where certificate is not used
- Firewall Settings

### Connection to the corporate network via IPsec\*

- Profile Name
- Communication Medium
- Access data for the Internet provider (User ID, Password, Phone Number)
- VPN Gateway parameters (VPN Gateway, Tunnelsecret)
- Certificate utilisation
- Access data for VPN Gateway (VPN User ID, VPN Password)
- Extended Authentication
- IPsec Configuration (Exch. Mode, PFS Group, Compression)
- Static Key (Preshared Key), without certificate (IKE ID Type, IKE ID)
- IP address configuration (Client IP Address, DNS/WINS Server)
- Firewall Settings

### Establish connection with the Internet

- Profil Name
- Communication Medium
- Access data for the Internet provider (User ID, Password, Phone Number)
- Firewall Settings

### Configuration Folders of the Profiles

#### Destination / Basic Settings

**Dial-up Network**  
**VPN Tunneling**

**Security**  
**Link Firewall**

#### Destination / Basic Settings

**Dial-up Network**  
**VPN Tunneling**

**Security**  
**Link Firewall**

#### Destination / Basic Settings

**Dial-up Network**  
**VPN Tunneling**

**IPsec Options**  
**IPsec Configuration\***

**IPsec Address Assignment / DNS/WINS**  
**Link Firewall**

#### Destination / Basic Settings

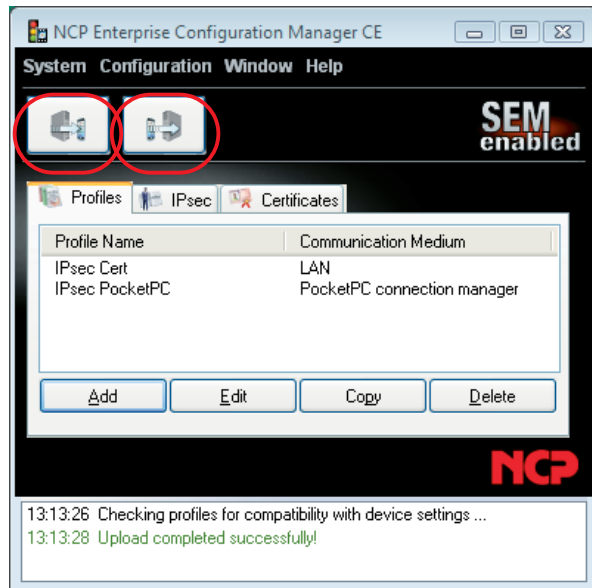
**Link Firewall**



**Descriptions of the functions and values for the individual parameters are available from the Configuration Manager online help system, listed in the same order as the corresponding configuration fields.**

## Data Synchronisation between PC and Mobile Device

A connection using ActiveSync or via Windows Mobile Device Center is always required for data synchronisation between PC and mobile device. This connection enables the transfer of profile settings, soft certificates, chip card reader data and modem data.



### Upload of Profile Settings

The profile settings are located on the PC in the user directory as ncphone.cfg.

When a profile has been created, this must next be transferred across to the mobile device, in order for it to be put into use.

To transfer profile settings click on the upload button in the configuration manager. NCP Client Service and Monitor on the mobile device do not have to be started up for an upload.



Please note however, that an existing VPN connection may be severed without warning during an upload. Profile settings which may already exist on the mobile device are overwritten without prior warning.

### Download of Profile Settings

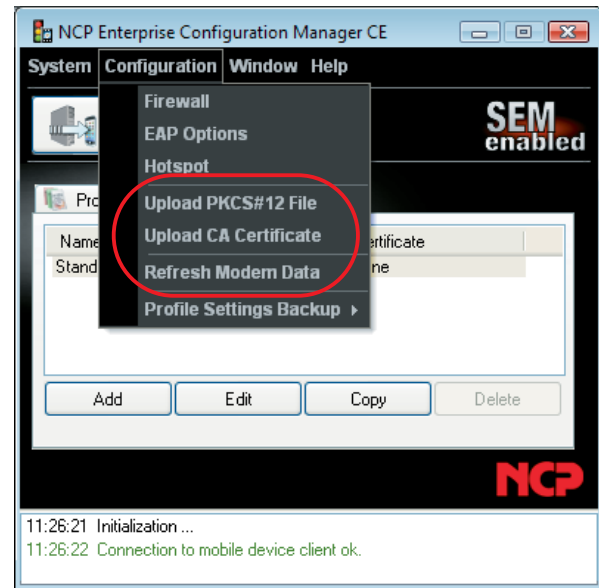
A download of profile settings on the PC is always necessary if changes have to be carried out to a profile configuration. Confirm by clicking the download button.



If you download the profile settings then the existing profile settings on the PC are overwritten.

### Refresh Modem Data

If you click this menu item, the modem data file (MODEM.INI) will be transferred from the mobile device to the PC.



When using the two menu points described below to transfer soft certificates, take note, also, of the description of Multi-Certificate Configuration on the next page.

### Upload PKCS#12 File

If you click this menu item, the PKCS#12-file can be transferred from the PC to the mobile device. Initially a selection screen appears and you have to select the required PKCS#12-file.

### Upload CA Certificate

If you click this menu item, the CA certificate can be transferred from the PC to the mobile device. Initially a selection screen appears and you have to select the required CA certificate.

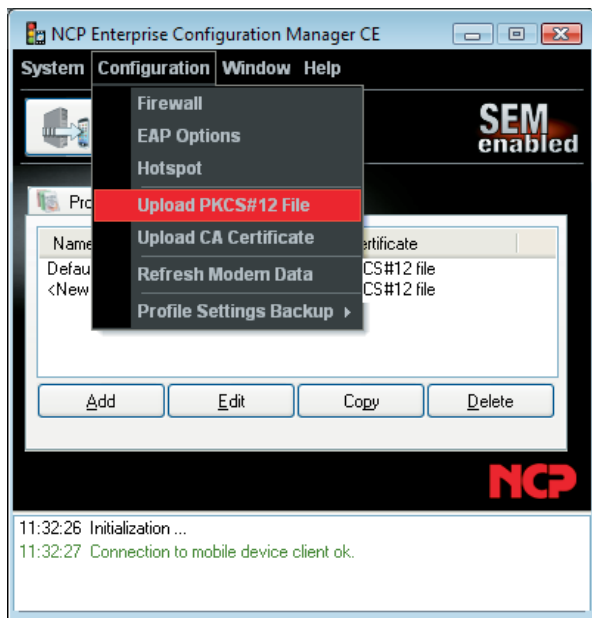
## Multi Certificate Configuration

For each Secure Client a large number of certificate configurations can be created with a separate name in each case.

The certificate configuration of a client older than version 2.37 will, in case of an update to this version, automatically be converted to the default certificate configuration. The default certificate configuration is set up after an initial installation of version 2.37.

For each profile you can select one of the stored certificate configurations. In this way, you get the option of various ways for authentication with different certificates against different VPN gateways. E.g. authentication with soft certificate against gateway 1 and authentication with certificate from token against gateway2.

In the configuration field “Security” a certificate which was initiated using the certificate configuration of the client monitor can be selected for the encryption and authentication in the security mode L2Sec or for the extended authentication in the security mode IPsec.



### Certificate Configuration

When using a soft certificate, the PKCS#12 file must next be transferred to the mobile device. (illustration above). The transfer of the user certificate and the CA certificate in its directory can be simplified by selecting **Upload PKCS#12 File** and **Upload CA Certificate** in the menu item.

The test certificates supplied by NCP, CA-certificate (ncpsupportca.der) and user certificate (client1.p12 up to client4.p12) are already located on the PC and the mobile device once installation is completed.

Please note, that the mobile device client is only able to read CA-certificates in DER-format (distinguished encoding rules) with the file extensions DER, CER or CRT! The PEM format is not supported.

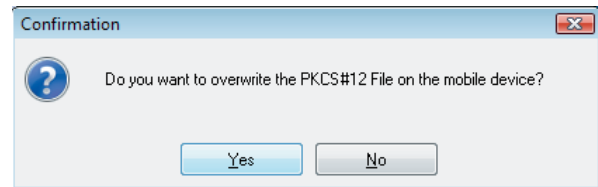
The destination directory on the mobile device for CA certificates is:

\Program\NCP Secure CE Client\CaCerts

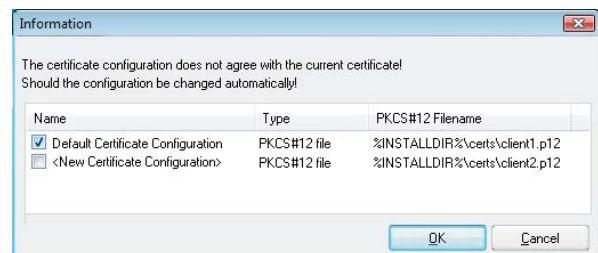
The destination directory on the mobile device for user certificates is:

\Program\NCP Secure CE Client\Certs

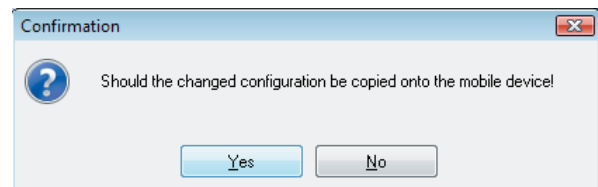
If there is already a PKCS#12 file with the same name present on the mobile device, a confirmation message is displayed (see illustration below).

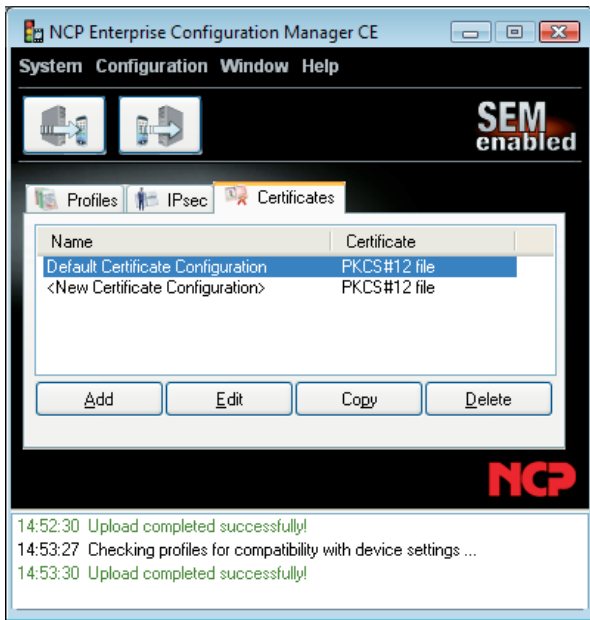


When a new certificate is used for an existing certificate configuration, the changes to the certificate configuration can be handled automatically by the Configuration Manager (see illustration below).



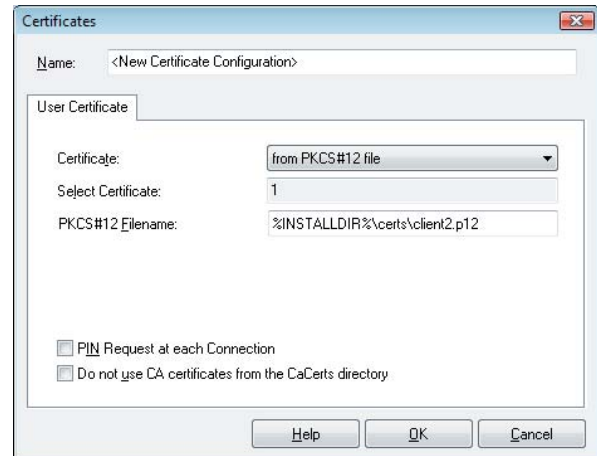
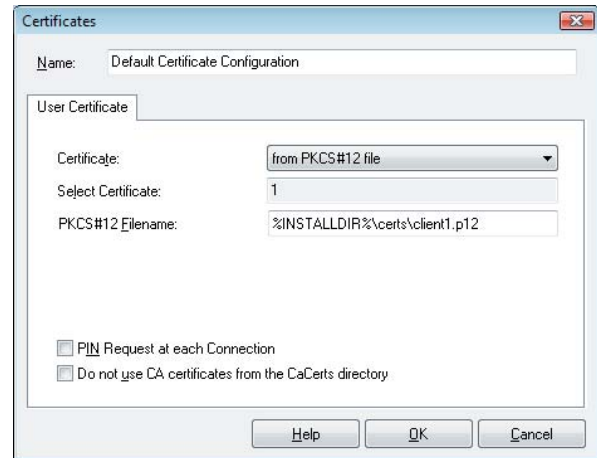
Finally the changed certificate configuration is copied to the mobile device (see illustration below).





After the successful upload (illustration above), the certificate configuration in the Configuration Manager is updated.

The certificate path is added automatically in the certificate configuration and takes the form %INSTALLDIR%\CERTS\<PKCS#12-filename> (see illustration below).



## Monitor Interface and Symbols



The following status displays and symbols are, depending on the configuration of the current selected profile, displayed from left to right in the graphics field:

### Security Policy



If you wish to deploy endpoint security via the Enterprise Client, please ensure reading the descriptions provided with Secure Enterprise Management (SEM-EPS-Plug-in and the **SEM-Navigator**).

The policy icon is always visible if Endpoint Policy Enforcement is defined by the management system for this client. This means that the client has to fulfill the rules of the security policy to be granted access.



The policy symbol is displayed in **yellow** as soon as the connection to the gateway is established and the check of the policy is started.



The icon will be displayed **green** when the policies are fulfilled.



If the specifications are not fulfilled, then the icon will become **red**. The system will output different messages or execute various actions depended to the configuration. E.g. you can restrict network connection to an area that is defined to make an update.

Deviations from the destination specifications are logged and can trigger different messages or actions, such as:

- message display on the client
- outputting a message in the monitor log
- sending a message to the Management Server
- sending a message to a Syslog server
- VPN connection disconnect
- release of all firewall rules or of a certain firewall rule

### PIN State



A PIN icon in **gray** always means that the system is still waiting for the PIN to be entered for the respectively configured certificate. (With a tap-and-hold via the symbol, a popup menu opens with the PIN dialogue; see further down under “ Monitor Popup Menus”.) An incorrect PIN is acknowledged with an error message, and remaining number of possible PINentry attempts will be reduced.



After successfully entering the PIN the icon will be displayed in **green**. This color indicates that the entered PIN is valid, even if a connection has not been set up. If you want to ensure that unauthorized persons cannot establish a connection in your absence, then the PIN must be reset (see popup menu **Reset PIN**) or the “PIN query function for each connection setup” must be activated. In the latter case the dialog for PIN entry will not be displayed after a tap-and-hold via the symbol on the grey icon, it will only be displayed after connection setup.

### Firewall



The firewall icon is always visible if a firewall is activated. If the global firewall (Personal Firewall) with defined rules is active, and the link-specific firewall is not active, then the icon will be displayed in **red** without arrows.




If the administrator has specified a Friendly Net (Friendly Net Detection), and if the Client is in a friendly net, then the firewall icon will be displayed in the color **green**. Friendly Net Detection specifications are made in the Monitor Configuration menu under “Firewall / Friendly Networks”, either by specifying static network routes, or by activating automatic Friendly Net Detection. In this regard, see the description **Firewall and FND**.




If Link Firewall is activated, the icon will be displayed with arrows, regardless of whether the global firewall is active or inactive.



If the Link Firewall has been switched active in the monitor menu with “Activate Stateful Inspection / Always” and the system is configured so that communication is only allowed in the tunnel then the firewall icon will be displayed with two **red** arrows.

 If the option “Only allow communication in the tunnel” is switched off then the icon will be displayed with **one green arrow and one red arrow**.

If Stateful Inspection is only activated for an existing connection then arrow icons are only displayed after a connection setup.

 The **arrow symbols** appear **in front of a green firewall**, if in addition to Link Firewall options, a Friendly Net where the Client is currently located has been defined in the global firewall.

### Friendly Net Detection

If the administrator set a friendly net (e.g. company network) and the secure client accesses it, then the firewall symbol will change to green. Friendly net detection is set in the configuration menu of the configuration manager under “Configuration / Firewall / Friendly Networks” either by indicated static network routes or by activating the automatic recognition of known networks.

### EAP Status



If an extended authentication via the Extensible Authentication Protocol (EAP) has been activated in the “EAP options” then this will be displayed via the EAP icon. The color **yellow** indicates the EAP negotiation phase, **red** indicates unsuccessful authentication, **green** indicates successful authentication with EAP. A tap-and-hold on the EAP icon resets the EAP. Then a new EAP negotiation will be executed automatically.



If the Client is successfully authenticated relative to a network component, the opposite side will indicate which protocol was used; this information is always displayed with a green icon and the designation MD5 or TLS.

If an EAP icon is displayed in red and the connection has been set up nonetheless; this means that EAP has been configured in the Client, however the network component does not require EAP.

Extended authentication can be configured in the profile settings (for LAN or WLAN connections) under “authentication before VPN”. If EAP authentication is selected, then the EAP for LAN has to be activated in the “EAP options” of the configurations menu of the configuration manager as well as the user name and password needing to be entered. Only then is the EAP symbol is visible.

## Connection Establishment and VPN Symbols



The symbols for connection establishment appear in green if successful.

After NAS dial-in is concluded, the VPN dial-in to the corporate gateway can take place. In this process the dial-in connection will be symbolized with a thick yellow line. If the dial-in is concluded and the connection to the VPN Gateway is successfully established then the thin connection line will be displayed in green.

The colors of the VPN dial-in icons change from gray to blue, then flash green, and finally are displayed as constant green to indicate successful connection set up. In this regard the dial-in and authentication processes on the gateway must always be executed; encryption and compression are optional. From left to right the VPN dial-in icons are:

### Dial-in on the VPN Gateway



The destination address of the VPN gateway is specified in the profile settings under “IPSec Settings / Gateway”.

### Authentication on the VPN Gateway



The necessary parameters are in the profile settings under “Identity”. “Extended Authentication (XAUTH)” is always used. User ID and password are either read from the configuration under these parameters, or they are read from the certificate. A certificate that will be used is configured in the Monitor menu under “Certificates”, and the issuer certificate of the gateway that will be selected must agree with the user certificate.

### Encryption



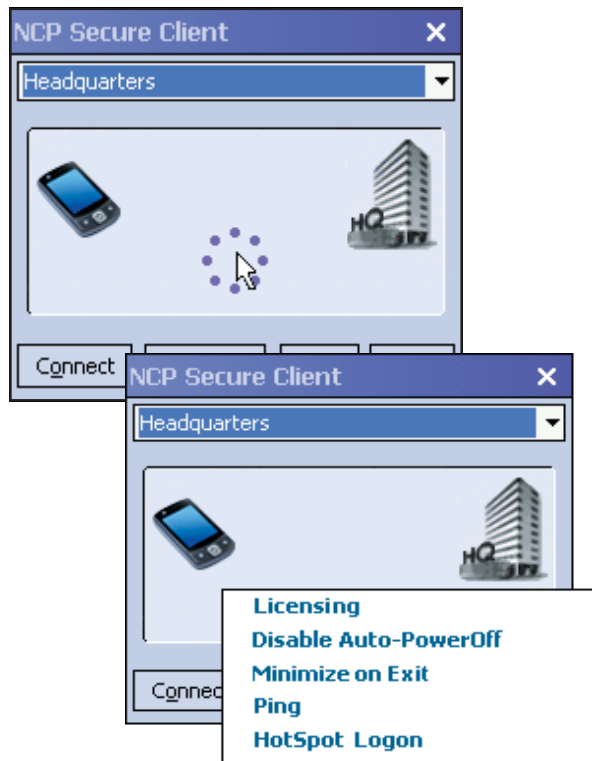
Either a pre-shared key or the private key from a certificate are used for encryption. Both alternatives are set in the profile settings under “Identity”. If the pre-shared key is used, then the “Shared Secret” must be entered here. If the “pre-shared key” is not used then the certificate will be used automatically. The gateway specifies which encryption will be used.

### Compression



Compression is only used if it is also supported by the gateway. You make the compression settings in the profile settings under “Use Extended IPSec Options / IP Compression”.

## Monitor Popup Menus



*The popup menu is activated by carrying out a tap-and-hold with the pen in the monitor's graphics field. (Ill. left)*

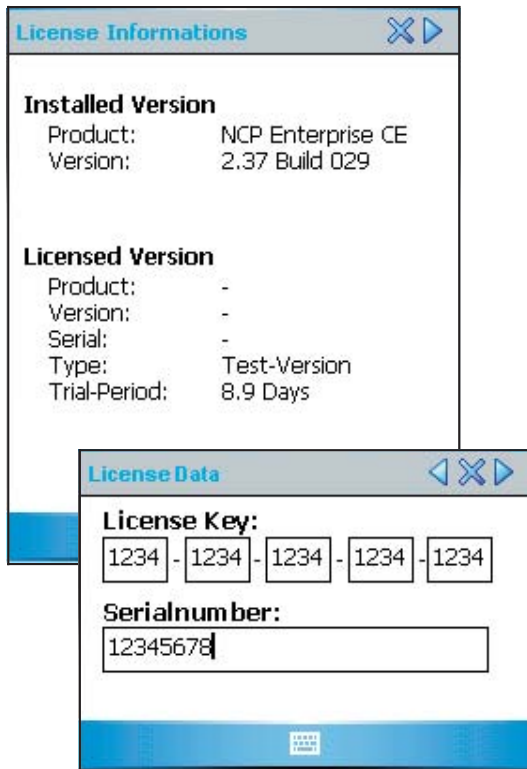
The adjoining menu items can also be selected during an established connection if necessary.



Please note however, that for configuration changes the settings on the mobile device and on the PC will differ. If the balance between the configurations needs to be recreated, then an upload or download of the profiles has to be carried out initially.

It also has to be pointed out that when saving configuration changes during an existing connection that the connection may be disconnected.

## Licensing



If you select the menu item "Licensing", then the adjoining window opens which displays installed and, if applicable, licensed software versions.

If the software is not yet a full version and if you want to license the test version, then you can open the entry window for the license codes using the button "Arrow to right".

Once you entered the license key and serial number tap on the button "Arrow to right". This will save the codes and the software is now the full version. If you tap on "Arrow to left" then the entered codes are deleted and you will be at the previous window.



Once you entered the codes correctly the licensing data will appear as in the adjoining image.

## Auto-PowerOff



The auto-poweroff function is deactivated as standard, as shown in the adjoining image, i.e. the mobile device does not switch automatically to energy save mode if a VPN connection is established.



(Using version 2.35 Build 58 or later the default setting is “Auto-PowerOff enabled”!)

## Minimize on Exit



The monitor is normally exited with the button [x], i.e. closed. If the function “minimize on exit” is activated, than the monitor is not closed by tapping the [x] button but only minimised and displayed as an icon in the task bar.

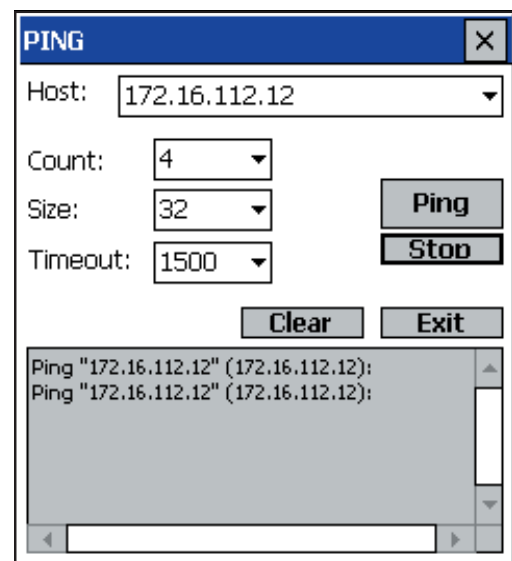


The monitor can then only be closed with the [x] button if the function “minimize on exit” was deactivated.



**Important:** An existing connection will not be interrupted or disconnected by closing or exiting the Client Monitor (by clicking on [x])!

## Ping



The CE Client has a program for sending ICMP echo\_requests (ping).

It is called via the Client’s popup menu (ill. above). The program “Ping.exe” is in the installation directory of the Client software and can also be used stand-alone.

## Hotspot Logon



Via the menu item the automatic hotspot logon will be done.



Please note in the description **Mobile Computing** the section **Automatic Hotspot Logon**.

After a tab onto this menu item, various connection messages may appear on the screen:

- If the user is already on the Internet, s/he is connected to their homepage. In the case of NCP, this is: <http://www.ncp-e.com>

A window appears with this message:

“No Hotspot Logon necessary - You are already in the Internet.”

The administrator can replace this text by specifying the address of a different HTML homepage in the form

`http://www.mycompany.de/hotspot_de.html`  
... and creating a page other than `hotspot_de.html` on the web server.

- If the user does not get to a website because the hotspot cannot be reached, the WLAN connection has fallen over or other connection problems have occurred, this Microsoft error message appears “... not found”.

- If the user has not yet logged in, the hotspot operator’s login page will appear, prompting the access details to be entered.

## Requirements for Hotspot Logon

The user must be in the receiving range of a hotspot, with an activated WLAN card. There must be a connection to the hotspot and the wireless adapter must have an assigned IP-address.

The clients firewall makes sure that only the IP-address assignment is being done by DHCP without any further possibilities of access to or from the WLAN. The firewall has intelligent automated processes for clearing the ports of one or more https so as to make logins and -outs to the hotspot available. During this process only data traffic to the hotspot server is possible. In this way a public WLAN can only be used for connecting VPN to the central data network, direct internet access is excluded. For opening the homepage of a hotspot in the browser a possible existing proxy-configuration must be deactivated.

At present the clients hotspot access works only with those hotspots, that redirect inquiries with the help of browsers to the homepage of the public WLAN provider (for example T-Mobile or Eurospot).

## Hotspot Configuration



Configuring for hotspot logon is done under “Hotspot” in the monitor’s configuration menu. (See also **Mobile Computing**.) The following settings may be made:

### Standard Browser

The basic setting is: Standard Browser for the Hotspot Logon. If the standard browser has a configured proxy server, this may sometimes need to be deactivated. If the checkbox is unchecked, a different browser can be entered.

### Alternative Browser

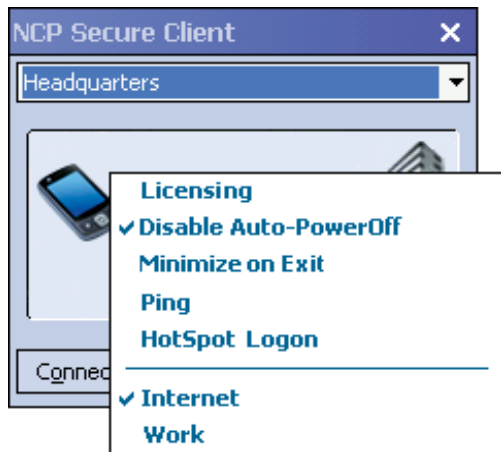
Using an alternative browser you enter the browser from the program directory.

The alternative browser is not part of the client software and must be installed and set up by the administrator or the user.

The alternative browser can be configured specifically for the Hotspot requirements.

The MD5 Hash value of the browser’s Exe file is also ascertained and entered in the “MD5 Hash” field. This ensures that a Hotspot connection can only be established using this browser.

## PocketPC Connection Manager



In the profile settings the connection medium “PocketPC Connection Manager” can be set for PocketPC platforms, in the “Basic settings” parameter folder.

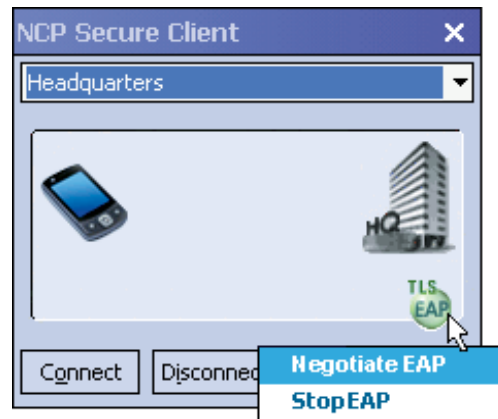
This connection medium is ideal for devices with integrated telephone (MDA). While a GPRS connection exists, you can telephone at the same time. The PocketPC Connection Manager automatically takes over the parking of GPRS connection. When configuring a profile for this application ensure that the selected timeout-period is large enough, or that timeout is deactivated, and Dead Peer Detection (DPD) is deactivated in the IPsec settings.

When using this connection medium, which is only practical for deactivated Loopback adapter, you can select the destination network: Internet or corporate network. This setting can also be changed retroactively on the PDA via the Popup menu.

When using this media type, the PocketPC Connection Manager is forced to set-up a connection (in the Internet or corporate network). This means that the Connection Manager will automatically select a RAS connection and set it up, or it will detect an existing LAN card and will not setup any other connection.

Under “Start / Settings / Connections”, the system can configure appropriate Internet and company connections with its own onboard resources. (If the network adapter of the NCP Client is active then more precise project-specific knowledge of the environment is required for the effective use of the Connection Manager.)

## EAP



Using tap-and-hold above the EAP symbol opens a small popup menu:

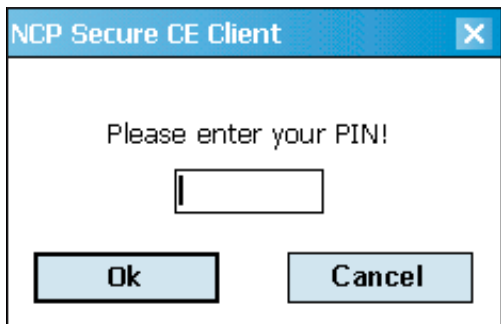
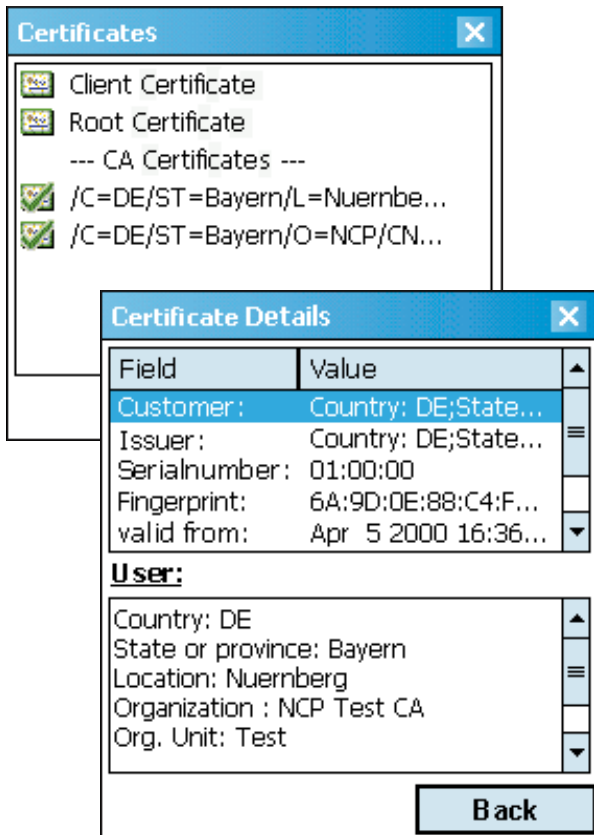
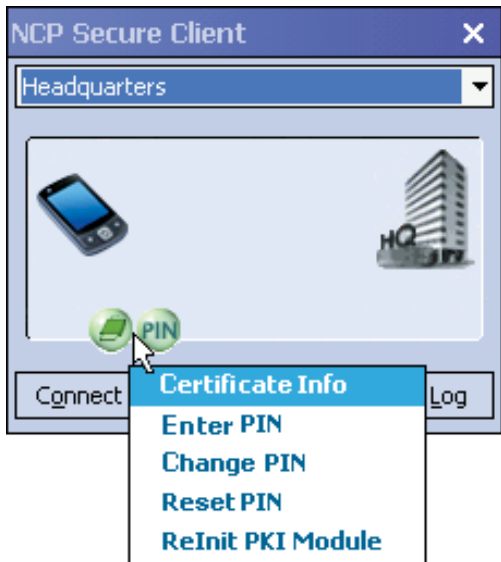
EAP can be reset with “negotiate EAP”. Immediately after, a new EAP negotiation is started automatically. If the authentication was successful to a network component, then the remote station replies with which protocol (MD5 or TLS) was used.

EAP is logged off with “close EAP”. To restart EAP negotiation, click “negotiate EAP” again.

*Extended authentication can be configured in the profile settings (for LAN or WLAN connections) under “authentication before VPN”.*

If EAP authentication is selected, then the EAP for LAN has to be activated in “Configuration / EAP options” of the configurations menu of the configuration manager, the user name and password need to be entered as well. Only then will the EAP symbol be visible.

## Certificates



Using tap-and-hold above the PIN or chipcard symbol opens the certificate information dialogue.

### Certificate Info

displays the used CA and user certificates.

### Certificate Details

A further tap on the required certificate displays its content (left).

### Change PIN

A smartcard PIN can only be changed in the menu item “change PIN” if the current PIN is entered first. Without entering the valid PIN you cannot activate this menu item. The PIN of a soft certificate cannot be changed.

### Enter PIN

The PIN entry can be done prior to establishing a connection. If the connection is then established later and requires a certificate then there is no need to re-enter the PIN unless the certificate configuration of the configuration manager was set to “PIN request at each connection”.

The PIN dialogue is always displayed if a connection is being established which requires a certificate and the relevant PIN has not yet been entered. If the connection is re-established manually then the PIN entry is not necessary.

If a soft certificate is used then the PIN has to be at least 4 digits, if it is a chip card then the PIN has to be at least 6 digits. Wrong entries are acknow-

ledged with an error report after 3 seconds. It is then not possible to establish a connection.

If the PIN was entered wrong three times in a row (this may be different depending on chip card) the chipcard is barred! (This does not apply to soft certificates.) In this case please get in touch with your administrator. If the chip card is removed during operation then the connection is stopped unless this has not been set differently in the certificate configuration.

### **Reset PIN**

This menu item can be selected to delete the PIN, i.e. to make the currently valid PIN unusable for a different user. This is useful if the mobile device is stored somewhere or if the user changes. Then a new valid PIN has to be entered in order to carry out authentication.

If the mobile device is on standby then the PIN is reset automatically for security reasons.

### **ReInit PKI-Module**

If the connection to the chipcard reader has an error again then this function will re-initiate initialisation.

## Extended Installation and Configuration

### Autostart of NCP Client Service

The NCP Client Service does not have to be restarted manually from the program folder after installation and a soft reset. The service is started automatically if the shortcut ncpwscstart was copied from the installation directory on the mobile device into the (to be created) autostart directory in Windows.

### Command Line Options for ncpmon.exe

The NCP monitor on the PDA understands, amongst others, the following command line options:

`-l license_key serialnumber`

Then the license codes can be entered. The license key with 20 digits is entered without the “-” separation between the group of four digits. The serial number has to be entered as 8-digits.

`-hide`

This allows you to hide the monitor interface. It does not, however, close the monitor, allowing continued PIN and password monitoring.

`-minimized`

It starts the monitor minimized, allowing continued PIN and password monitoring.

`-start`

This command starts the VPN service automatically (ncpmon start minimized.lnk is supplied) and if applicable also minimized with:

`-minimized -start`

### Cold Start Installation

A new installation including the directory can be carried out with a specific program (admin pack) without PC. The software is saved in the flash-ROM of the device or on the flashcard. It is then automatically installed after a cold start. The following three files are required to assume the profile settings and the licensing:

- the CAB file of the client software from the installation directory on the PC
- an installation program (admin pack) with manual
- a configuration program (script)

The installation program is started by the autostart mechanism of the system. The configuration program includes information on which software is used, if and where the directory is located as well as licensing information. It is also listed if additional settings before or after the installation have to be carried out in the registry. The admin pack is not part of the software and only available upon request from NCP.

## Disconnection

An active connection can be interrupted either an error, an automatism, or manually by the user.

Once a connection is interrupted, the coloured connection image on the Monitor disappears.

### Interruption and Error

Should an error occur during connection, then the connection will not be established and the cause will be displayed on the Monitor. An error message is generated, just as it would for a physical interruption. For additional information, please read the remarks regarding error messages on the Monitor and in the Client Info Center below.

### Manual Disconnection



**Important:** An existing connection will not be interrupted or disconnected by closing or exiting the Client Monitor (by clicking on [x]). Please also read the descriptions about the popup menu "Minimize when Closing" discussed above.

A connection is interrupted properly only by pushing the "Disconnect" button in the monitor.

If you wish to disconnect the connection manually at any time, select the option "Manual" for establishing a connection, and deselect automatic timeout, by setting the timeout option to "0". Timeout configuration is carried out via "Profile Settings" in "Connection Control".

### Automatic Disconnection

Where "Timeout" has been activated, the connection will be interrupted automatically. This parameter defines the time frame following the last data movement (received or sent) before a connection will be disconnected automatically. The value is input in seconds between 0 and 65535. Default value is "100". Where the value "0" was entered, no automatic disconnect will be carried out.

The timer for the selected interval will only activate, once data movement and handshakes have ceased on the line.

## Uninstalling

### Uninstalling the Client on the Mobile Device

To remove the component on the mobile device go to: “Settings / System / Remove Programs” and select “NCP Secure CE Client” from the list.

The system will ask you to confirm with “Yes”.

The client will be stopped and then you will be requested to execute a soft reset. Click OK here, execute a soft reset

The profile settings will be automatically deleted. If certificates are still present on the mobile device then these must be manually removed.

### Uninstalling the PC Component

To remove the PC component, go to: “Start / Settings / Control panel” and click on “Add / Remove Programs”.

If you uninstalled the client, then you have the option to keep the configuration and profile settings in the client directory. If at a later date, a newer client version is installed in the same directory, then all personal data can be used again. If you want to delete the personal data in the client then you will have to confirm this specifically. In such a case all data and directories of the client are removed irretrievably.