

Functional Description and Configuration

high security remote access

Enterprise Client Monitor





Secure Client Monitor

of the Enterprise 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.



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

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, April 2012

Secure Client Monitor	5
Secure Client Startup	5
Client Monitor Interface	6
View Menu of the Monitor	7
Show WLAN State	7
Always on Top	8
Autostart	8
Minimize when closing	8
Minimise when Connected	8
Language	8
Company and Project Logos integrated into Client Interface	9
Enterprise Client Parameter Locks	10
Configuring a Template with Parameter Locks	11
Group specific and user specific parameters	11
Authorisation	12
Profile Configuration (Destination Systems)	13
Locks	14
Profile Preview	15
Parameter Locks Depiction in the User Interface of the Enterprise Client	15
Unlock Parameter Locks	16
New Profile	18
Client-Side Profile Creation	18
Profile Groups	20
Group Display	21
Symbols of the Monitor	22
Status Displays / EAP Authentication / Chip Card Reader / PIN State	23
Firewall / Security Policy	24
Connection Setup Symbols / Symbols of the NAS Dial-in	25
Symbols of the VPN Dial-in	26
Profile Selection and Connection Establishment	27
Establishing a Connection with the Remote Station	27
Automatic Connection Mode	27
Manual Connection Mode	27
Variable Connection Mode	27
Passwords and User IDs	28
User ID for NAS Connections	28
User ID and Password for VPN Connections	28
Password for OTP Tokens	28
User ID and Password Dialog	28
Client Logon	28
Disconnection	29
Interruption and Error	29
Manual Disconnection	29
Automatic Disconnection	29
Information Windows of the Client	30
Connection Info	31
Available Communication Media	32
Log	32
Info	33
Client Info Center	33
Budget Manager History	33
EAP Options [Configuration]	34
EAP MP5	34
Logon Options	35
Logon [Logon Options]	35
Logoff [Logon Options]	35
External Applications [Logon Options]	36
Options [Logon Options]	36
Messaging Center (SMS)	37
Configuration Modes	38

Secure Client Monitor



The following documentation provides a description of the monitor interface design, as well as an evaluation and utilisation of available display options. To this end, menu points “Connection”, “Log”, and “Window” will be described. “Hotspot Logon” will be exempted here, since its functionality will be described under **Mobile Computing**.



Furthermore, this documentation will elaborate on Parameter Locks for the Enterprise Client.

Overview

- Generic User Interface
- Autostart Options
- Company and Project Logos integrated into the GUI
- Parameter Locks of the Enterprise Client
- Client-side Profile Creation
 - New Profile with the Assistant for Configuration
 - Configuration Modes
- Symbols and Messages in a graphic Display Field
- Client-side Info Windows
 - Connection Data
 - Connection Media
 - Log
 - Budget Manager Statistics
 - Info Window
 - Client Info Center
- EAP Options
- Logon Options
- Messaging Center (SMS)



The documentation **Enterprise Client Parameters** offers a detailed description of how to set up parameters for individual configuration windows.



The easiest way to access the desired information is via the **Enterprise Suite Navigation**. All available documents about your product are recorded in this pdf file.

Starting from navigator, you can jump directly into all relevant documents and download them from the NCP homepage in case they are not yet saved in your navigator directory.

Secure Client Startup



Once a standard software installation has been performed, and the first profile has been created (see **Enterprise Suite Installation**), the monitor can be activated via Start / Programs / NCP Secure Client / Secure Client Monitor. If a desktop icon was created during installation, you can start the client by double clicking on that icon. The monitor window opens (illustrations below).



Program Icon



Client Monitor after starting

Client Monitor Interface



The user interface is Windows conform. The interface operates via pulldown menus on the menu bar, via buttons on the button bar, or via the context menu (right click).



The user interface of the monitor can be altered in two ways: it can either be altered via the **View Menu** of the monitor or via configuration locks. The **Parameter Locks** alter the configuration interface in the profile settings and the configuration menu.

The Monitor consists of the following buttons and display fields (illustration to the left):

- title and software version notice
- main menu bar
- profile selection
- graphic display field for connection status, fire-wall, possible error messages, as well as a world map with time zones. (Depending on the time zone set on the computer, the respective section of the world map is displayed: Europe, America or Asia/Australia.)
- statistics field, displaying the most important settings and values for the selected profile (see **Information Windows of the Client**)
- a field for the display of the signal strength (only displayed for the connection types **GPRS / 3G and Wi-Fi**, see Mobile Computing),
- a field for soft certification selection (please also see description of soft certification selection in the documentation **Certificates at the Secure Client**),
- connection switch and logo



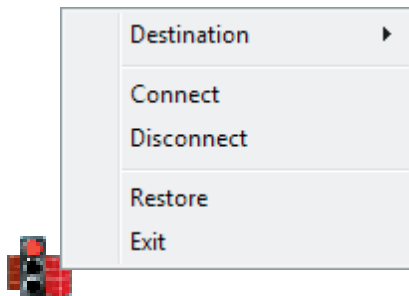
View Menu of the Monitor

Various information and statistic fields can be shown or hidden via the view menu (illustration on the left). With that the size of the monitor on the desktop can be enlarged with information fields, if needed, or it can be decreased in size to its smallest form by switching off all fields. Furthermore, the monitor can be always on top of the desktop or always be minimized as tray icon.

Via the view menu, the graphical user interface of the monitor can be varied and the language set. If all display and statistic fields are activated the monitor has its largest size, like it has after being started for the first time.



After switching off single operation elements the monitor is displayed in its smallest form (illustration on the left). In this size, the connection type cannot be read any more in the statistics field. To avoid this, the connection type can be added to the name of the profile and with that, it is displayed in the graphical status field (illustration on the left).



When minimising the monitor via the button [-], it will appear in the system tray as a 'traffic light' (illustration on the left), where depending on traffic light colour, connection status can be gleaned. Right clicking on the symbol, an available profile can be read, and a connection can be established or disconnected. Once a connection has been disconnected, the monitor can be exited.



As soon as the mouse pointer touches the tray icon a popup shows the state of the connection and the firewall configuration (illustration on the left). Please refer to the description **Personal Firewall**.

Show Wi-Fi State

Regardless of the connection medium of the currently selected link profile, the field for the graphic display of the Wi-Fi state can be opened or closed, if a Wi-Fi configuration was activated within the monitor menu "Configuration" under **Wi-Fi Settings**. Where a **Multifunction Card** was configured, the menu option "Show Wi-Fi State" will not be available.



Independent of the start of the Client Monitor or a



For Wi-Fi configuration and Wi-Fi state please refer to the PDF **Mobile Computing**.

Always on Top

If you have selected “Always on top”, the monitor will always be displayed in the foreground, regardless of which application is currently active.

Autostart

This menu option will configure the monitor to start after booting. The following options can be preset:

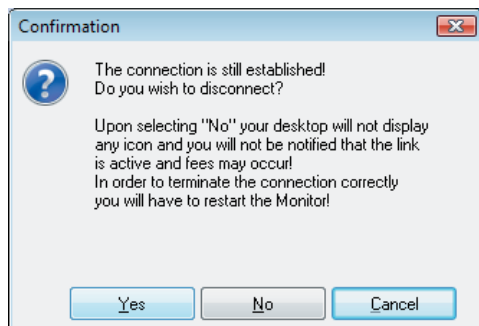
- No Autostart: don’t automatically start after booting
- Icon in System Tray: start up monitor after booting, and display icon in taskbar
- Monitor on Desktop: start up monitor after booting, and display in predefined window

If you frequently work with the Secure Client software, and require access to monitor information, then you should opt to have the monitor on the desktop after booting. In principle, communication with the remote client will not require monitor startup.

Minimize when closing



The monitor is usually exited via the “Close” button [x] on the right of the title bar, or via the system menu on the left of the title bar [Alt + F4], which exits the application. The monitor traffic light symbol will be removed both from the taskbar, and from the info area of the system.



VPN connection, the NCP Wi-Fi tool (illustration to the left) shows the Wi-Fi state as soon as the mouse pointer touches the tray icon.



If the monitor is exited this way during a current connection, a prompt will appear, informing you that the tray symbol will be removed, so that the connection status can no longer be controlled. The prompt will include three buttons:

Yes = Connection will be disconnected, before the monitor is exited.

No = The monitor is exited without disconnecting the current connection. The user will no longer be able to see on the desktop interface, if and how much of a connection fee will be accrued, or whether or not the connection has been disconnected. You have to restart the monitor to receive information about the connection status, and to be able to disconnect correctly.

Cancel = The prompt disappears, and you will be able to disconnect any current connections, before exiting the monitor. You can now also activate the window option **Minimise when Closing**.

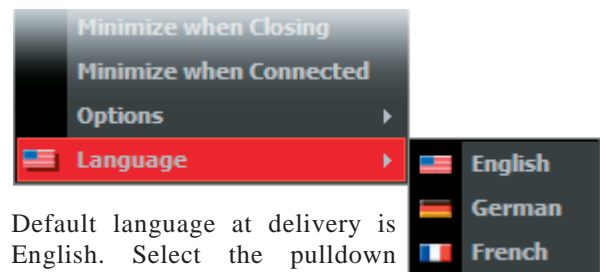


Once the option **Minimise when Closing** has been activated, the monitor will not close and exit, but will instead be minimised, and a tray icon will appear in the system info. Exiting the monitor will then only be possible via the main menu “Connection / Exit”, after which the above window will appear again, if a connection exists.

Minimise when Connected

If this function is activated, the monitor will appear as a tray symbol under system info only, once a connection has been established.

Language



Default language at delivery is English. Select the pulldown menu “Language” to select another language.

Company and Project Logos integrated into Client Interface

During the installation of the Client software, the file **Projectlogo.ini** is created in the installation directory. This file contains a description of how a company or project logo should be integrated into the Client's user interface, which will activate a mouse-over quick info display for the logo. A click on the logo will open a local HTML page via the preinstalled browser.

The file **Projectlogo.ini** can include the following entries:

```
[GENERAL]
Picture_96 = Logo
Picture_120 = Logo
ToolTip1 = Text Line
HtmlLocal = local HTML File
```



Logo

The logo will appear in a panel of the Client at the very bottom, across the entire width of the Monitor. A bitmap (96 or 120dpi) is required for the logo, 96dpi for a display with small fonts, or 120dpi for a display with large fonts. The size of the bitmap is predetermined at "min. 24 pixels in width" and "exactly 328 pixels in height" for small fonts, and "min. 29 pixels" and "exactly 404 pixels" for large fonts. The bitmap can be stored in any local directory. If it is stored in the installation directory, no path has to be specified in the INI file, otherwise the bitmap name will be specified with a path.

Text Line

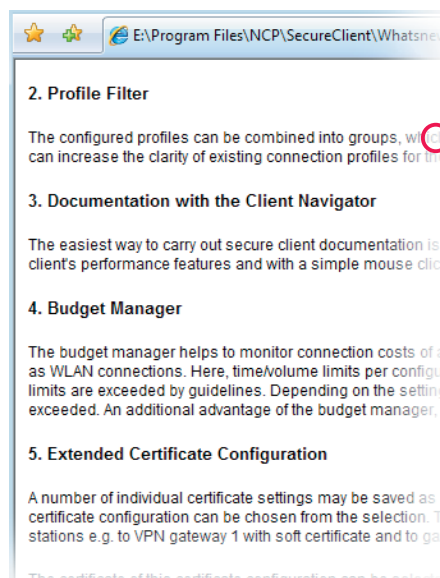
Text lines for Quick Info are listed with consecutive numbers per line, e.g.:

```
ToolTip[1] = Per mouse click you will get
ToolTip[2] = the new features of this client
```

Local HTML File

The HTML page to be displayed, once the project logo was clicked, must be stored in a local directory of the computer. Where no path is specified, the file will be called from the client's installation directory. Example: (illustration left):

```
HtmlLocal = Whatsnew.html
```



Enterprise Client Parameter Locks



The parameter locks of the client software have two important functions. On the one hand, the complexities of the configuration options will be reduced, which will give the software interface a more streamlined appearance. Any parameter fields for functions that are not required, are deactivated, and the user will only see setting options relevant for his environment. On the other hand, default settings can be defined, which cannot be changed by the user, which eliminates faulty configurations and unwanted connections. With default settings, the user only needs to enter his personal passwords after installation, in order to establish a connection.



The Secure Enterprise Client software can handle the administration, configuration, and deployment of many users in larger VPN environments via Secure Enterprise Management.

Terminology “Profile”



In older versions of the Enterprise Client (<9.1), the collection of individual configurations was called a “telephone book”. Starting with version 9.1 these are called **Profiles**. To edit a profile, select this configuration menu option, then a profile, and open the relevant **Profile Settings**. Completed profile configurations will then be stored as **Profiles** with a unique name in the configuration menu of the Client. For the purposes of better understanding, a **Profile** can also be called a **Link Profile**, as opposed to “Wi-Fi profile”, “certificate profile”, etc..



The following applies for Enterprise Client parameter locks:

- They are created centrally, and distributed automatically to the user’s remote PCs;
- Access rights for configurations within the Client Monitor menu are separate from
- Access rights for profile configuration (in the telephone book);
- both can be combined user specifically via separate profiles;
- Parameters can be hidden individually within the configuration fields of a profile, e.g. locks can be differentiated according to specific links;
- parameter locks can be removed by entering “User” and “Password” until the next configuration update, or until the next startup of the Monitor by entering a one-time password.



Enterprise Client parameter locks can only be created via Secure Enterprise management (SEM). Please read the Management System description (**SEM-Navigator**) for information on how to proceed for the creation of parameter locks. Here, only the required steps for the assignment of general user rights up to the customisation of the software are included.

The administrator uses templates for the creation of a software configuration with the Management System by means of a Client Configuration Plugin, which at first all users can use that are assigned to a specific group.

This template will be modified step by step for each user, resulting in individual profiles with profile specific locks, and also differentiations in regards to parameter locks.

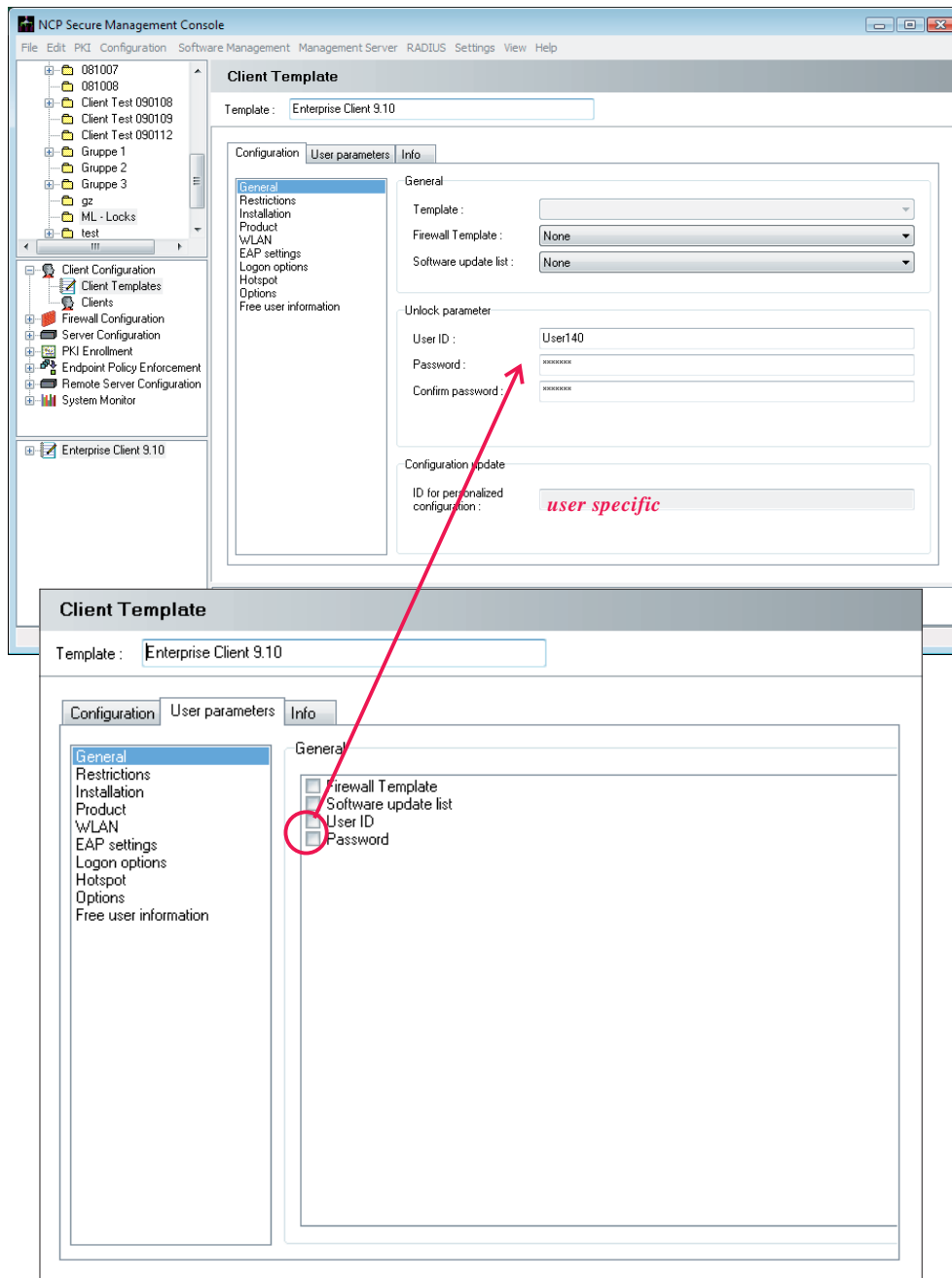
Furthermore, older profiles, which a user may have created earlier, can be deleted automatically during (configuration) updates.

The new profiles with their respective parameter locks will then be automatically distributed with their user specific Monitor menu interfaces (CNF file) by the Management System, providing a (configuration) update. Please also read the automatic update description (and the configuration update) for Secure Enterprise Management.

Configuring a Template with Parameter Locks

Group specific and user specific parameters

All values and entries of a template configuration are identical for all members of an organizational group, for which that template applies – with the exception of personal codes.



The template parameters, whose entry fields have been deactivated (illustration left), must be entered at the end of each client configuration..

The template parameters, to which this should apply, can be defined in the template field of the user parameters (see illustration bottom left).

Example: By default, the parameters “User ID” and “Password” can be configured, when the template is first opened in the configuration area, while the “ID for personal phonebook”, the user specific profiles, can not be modified.

That means that all user configurations, for which this template will be used, will have identical codes for “User ID” and “Password” in order to remove the parameter lock, but will have a unique ID for personal link profiles. This code will have to be entered at the end of the client configuration.



Please note that this configuration defines only, which parameters will be identical for all members of an organizational group, and which will only be entered at the end of the client configuration. These so-called “User Parameters” will have their check-box selected.



In regards to the parameter lock, this will only define whether all users will receive the same code to remove the parameter lock, or whether they will receive individual codes.

Authorisation

With “Authorisation” (see illustration below), the administrator can define group specific locks. He will define here, how the user interface of the Monitor should look, which configurations should be preset, and whether or not the user will be authorised to modify profiles (in the phonebook).

	Open dialog	Modify	Preconfigured
Call control manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Logon options	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
EAP settings	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Connection info	<input checked="" type="checkbox"/>		
IPSec configuration	<input type="checkbox"/>		
Profile settings backup	<input type="checkbox"/>		
Minimize when closing	<input type="checkbox"/>		<input type="checkbox"/>
Exit monitor	<input checked="" type="checkbox"/>		
Autostart	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Hotspot logon	<input checked="" type="checkbox"/>		
Hotspot configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Licensing	<input checked="" type="checkbox"/>		
Software update over LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Profile filter groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Client Monitor Menu (General)

Authorisations in this field refer to dialogs in the Client Monitor, located in the menu option “Configuration” and “Window”. The administrator can define authorisations, which will allow the user to ‘only’ open dialog boxes, and view default settings, or to modify the parameters displayed there.

Where a user is not authorised to open a dialog, it will be displayed as greyed out in the Monitor’s main menu. Where a user is not authorised to undertake modifications, no entry fields will be available. Furthermore, the administrator can set checkmarks regarding which parameters he wishes to include in the template by default, and which should not be available for modification by the user.

Where an administrator applies restrictive settings for all configuration options, and restricts the user from undertaking any editing at all, a new CNF file must be supplied for the client in case of failure - provided the client can still establish a connection - or the administrator will have to communicate directly with the user to provide him with the (one-time) password to remove

the parameter lock, and the user can then make the necessary changes himself.

Profiles (Phonebook)

Profiles

- ☐ Allow user to create new profiles
- ☐ Delete all profile entries

“User can create own entries” means that the user is authorised to create new profiles. Where this option was not check marked by the administrator, the user will only be able to establish a connection with the profiles defined by the administrator, and cannot add new entries.

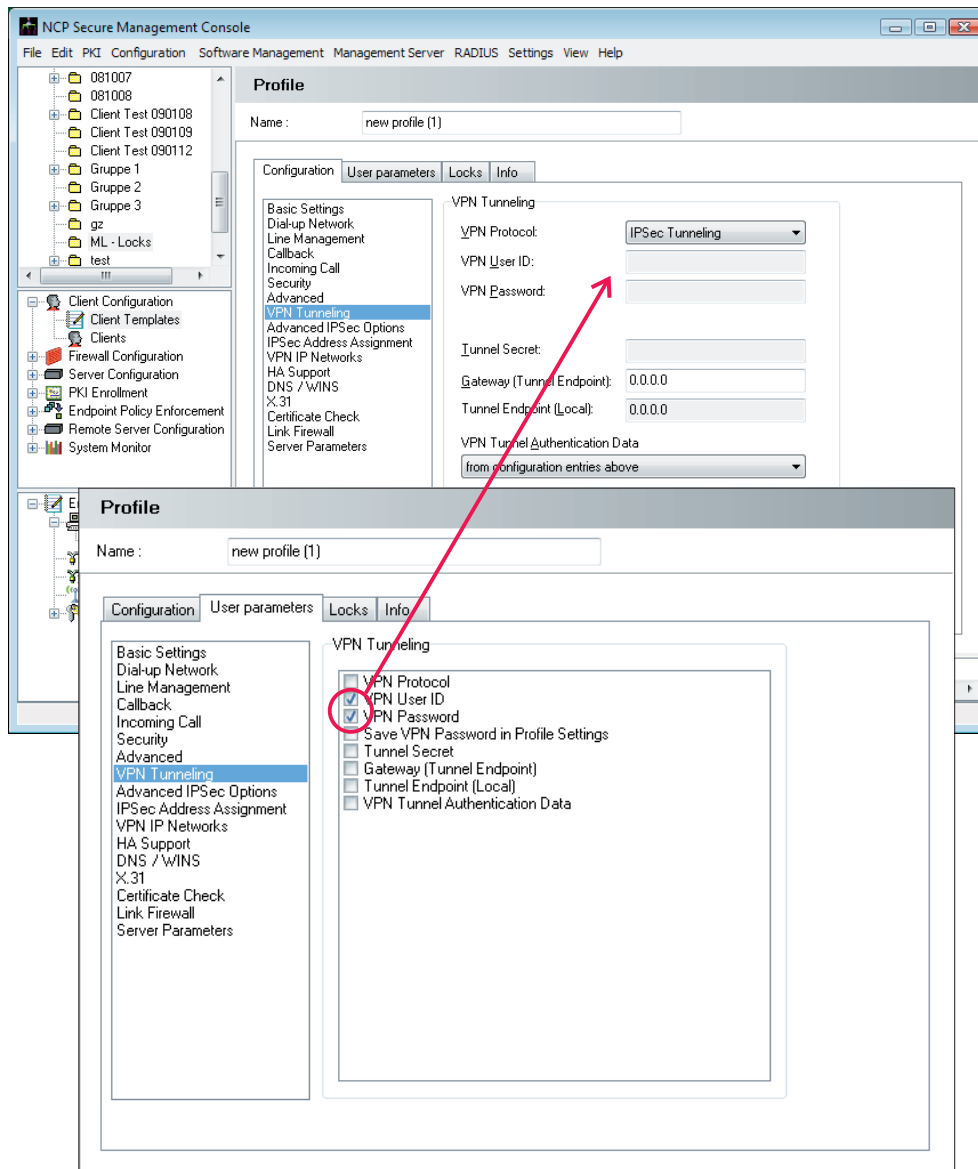
All profiles, including those defined by the user himself will be deleted via the option “Delete all Client entries” during a configuration update, e.g. once the client has received a new CNF file.

The administrator can lock storing the SIM PIN under **GPRS / 3G**. (See **Mobile Computing**.)

Profile Configuration (Destination Systems)

Profiles (destination systems) are part of the templates. Each user will later have one profile (or more) assigned via the template. (Should, for example, several users within one group have three destination systems assigned, and other users have five, then two separate templates will have to be defined: one for three profiles, and one for five. The same applies also, where various certification utilisations occur.)

Profiles are configured the same way via the management System console, as on the Enterprise Client; a differentiation occurs here in regards to which parameters apply equally for all clients, and which are to be user specific.



The template parameters, whose entry fields have been deactivated (see illustration left), must be entered at the end of each client configuration. The template parameters, to which this should apply, can be specified by setting a check mark for the template field of the user parameters (see illustration bottom left).

Example: By default, the required authorisation codes for the VPN gateway will not be editable when the template is first opened in the configuration area under "Tunnel Parameters".

That means that all users, who work with this profile, will have individual authorisation codes, which will be entered at the end of the client configuration process, or once the user establishes a connection.

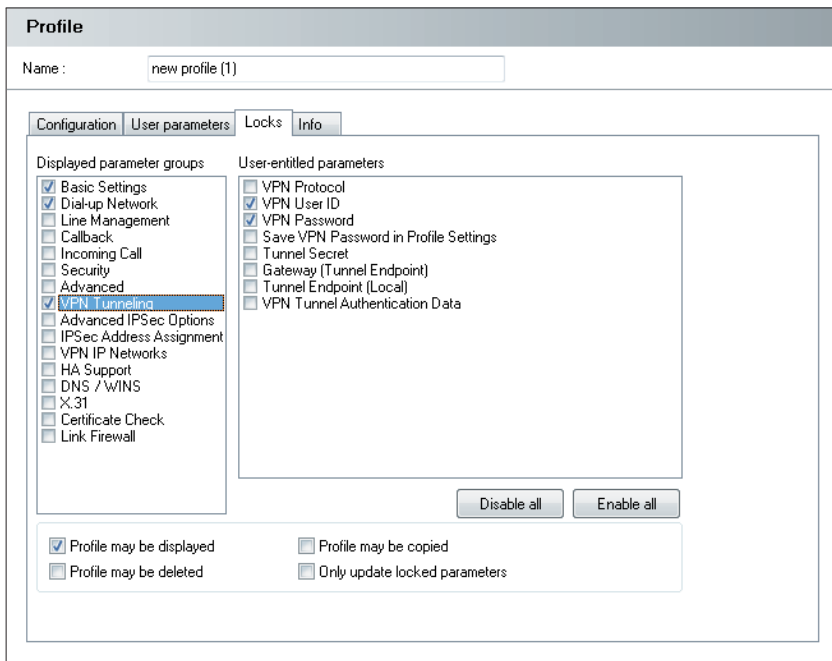
User Parameters



Parameters like **VPN User ID** and **VPN Password** are individual codes for each user, and will therefore need to be entered into the client configuration (where this data is not read from a certificate). See **Secure Client Parameters**.

That means generally that all parameters, which cannot be edited in a template for a certain profile, are personal and unique values, which can only be entered during client configuration in the SEM or directly at the client by the user.

Locks



Locks define the appearance of profile settings in the user interface of the Client software in such a way that the user will not be able to modify or even see certain parameters of the profile settings.

A lock-out is always associated with a profile or a parameter field in the profile settings of the Secure Client.

Visible Parameter Folders

The visible parameter folders list all the titles of all parameter folders from the profile settings of the client. Where titles of parameter folders are checked, those parameter folders will be visible to the user. Unchecked parameter folders will be completely hidden.

Unlocked Parameters

The list of all unlocked parameters will include all parameters within a checked parameter folder. If a parameter folder is visible to the user, a further definition of which parameters within this field should be locked for user entries, and which should be unlocked.

A parameter with a check mark next to it is available for user entries. Where there is no check mark visible, the parameter remains locked for editing.

Profile Modifications

For additional information, please read the section “Client-side Profile Creation” below.

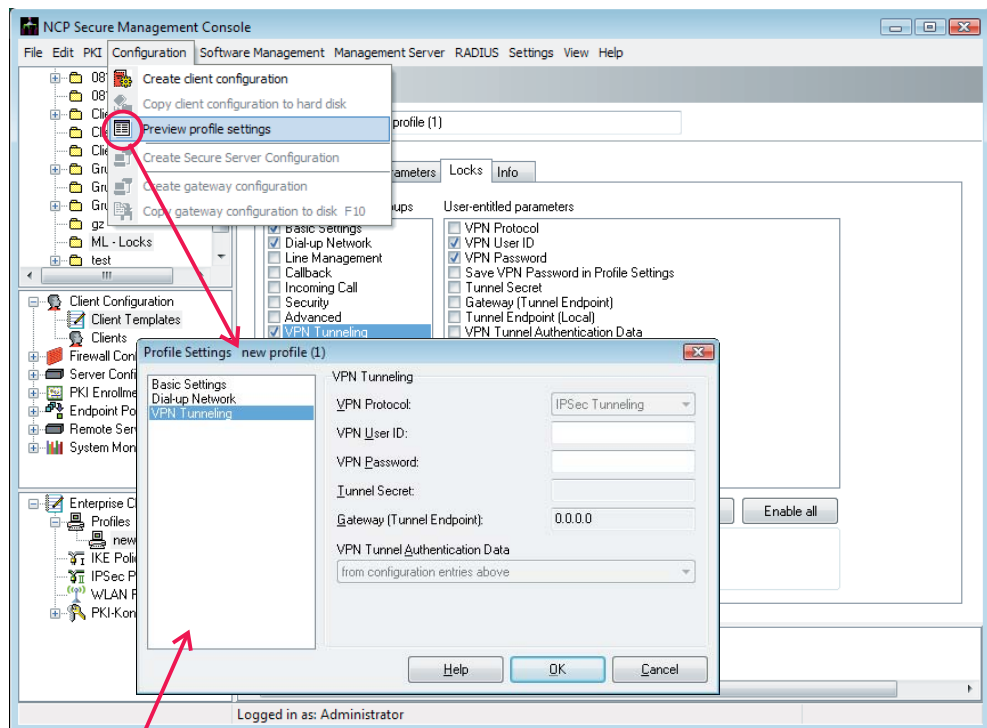
The functions “Show Profile”, “...delete”, and “...copy” will toggle all buttons in the profile directory of the Client Monitor (with the exception of “New Entry”) between active or inactive, allowing or disallowing the user to undertake modifications. The button “New Entry” is activated, where the user has the authorisation for “User can Create own Entries”. This authorisation affects all profiles and not only some, which is why this configuration option is located in the user interface of the template configuration (see section “Authorisation” above.)

The administrator can decide to “Show Profile” for this user by placing a check mark. Where no check mark has been set, the profile entry will not be displayed to the user, which means that also the button “Configure” will remain greyed out. The configuration options “Delete Profile” and “Copy Profile” affect the functionality of the buttons “Delete”, and “Copy” in a similar way.

“Only modify locked-out parameters” means that during a configuration update, only the settings of parameters that are locked out will be overwritten. This functionality helps to eliminate overwriting of parameters, which were modified by the user via the Client (e.g. modem settings) during a configuration update.

Profile Preview

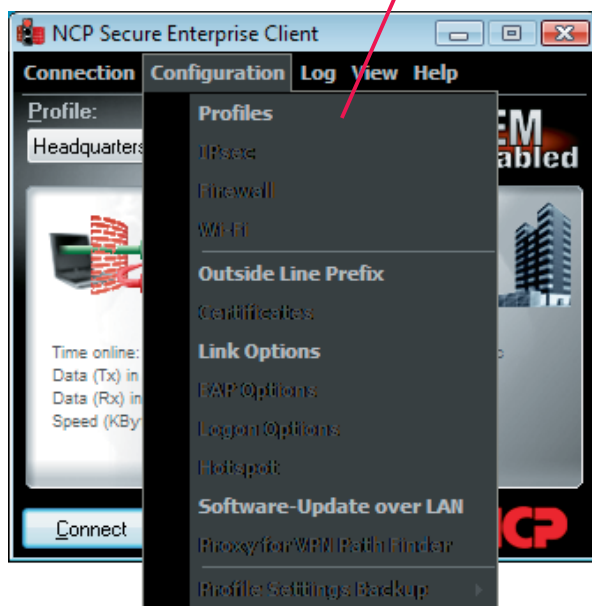
Once a profile configuration is complete, and lock-outs have been defined, profiles can be viewed as they will appear to the user on the client by simply clicking the button “Preview” in the taskbar, or selecting “Profile Preview” from the main menu under “Configuration”. (Illustration right).



Parameter Locks Depiction in the User Interface of the Enterprise Client

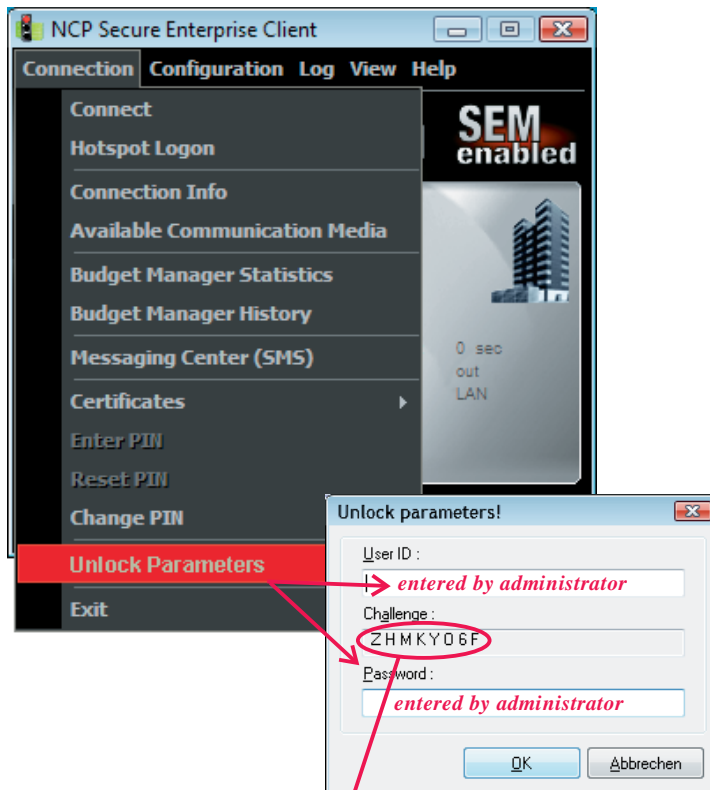
Following a roll-out or a configuration update, where a user Client receives the software with relevant lock-outs, the configuration menu of the Enterprise Client will be displayed as per the illustration you see here.

Individual configuration fields of a profile will be displayed as per preview on the SEM, provided they can be accessed (see illustration above).



Unlock Parameter Locks

Removing or modifying a lock-out should only be carried out as previously described in order to safeguard configuration security:



Centrally

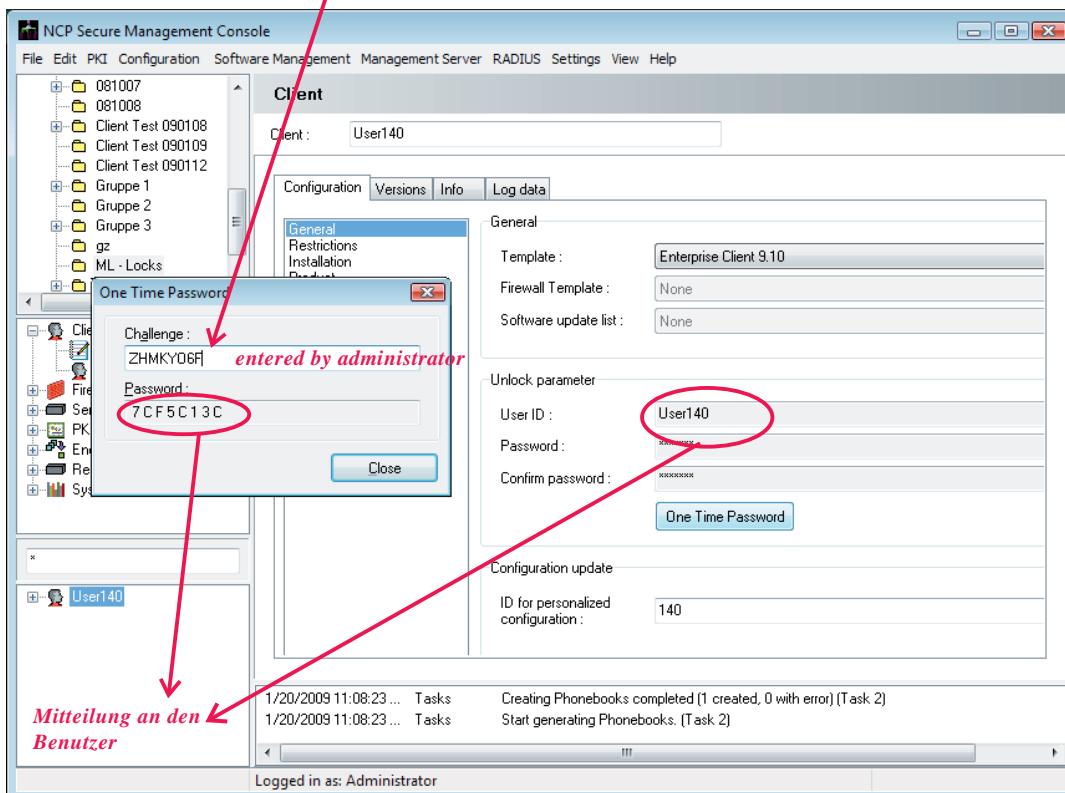
The administrator can create a new user configuration centrally via the SEM, and then provide a configuration update for the management server. Once the automatic update has been completed, modifications will have taken effect on the remote client. (For additional information, please read the description regarding configuration updates via SEM.)

Locally

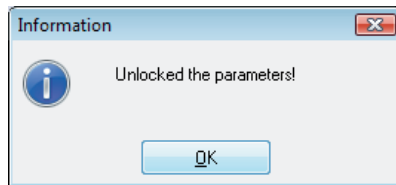
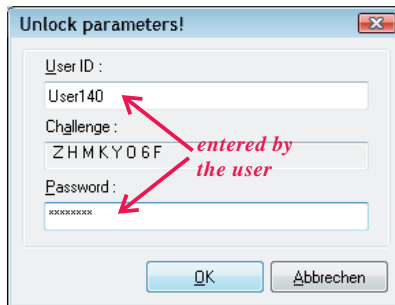
Should the remote client not be able to establish a connection with the Management System anymore, then the administrator can remove the parameter lock-out locally from the Enterprise Client. He selects the option “Remove Parameter Lock-Out” (illustration left) from the configuration menu of the Monitor, and then enters both the user name and the password as configured in the template under SEM (see above: “Group specific and user specific parameters”.) Once the modifications have been carried out, the administrator must not forget to reinstate all lock-outs (see below).

Remotely

The Administrator may decide to entrust the remote user with the removal of the parameter locks. For such a scenario, administrator and user must be in contact via telephone.



The user will disclose the challenge code to the administrator, which he receives after selecting the menu option “Remove Parameter Lock-Out” (above). He discloses the code to the administrator, who will enter it into the Management console. To this end, the administrator will click on “One-Time Password” for the general client configuration of the caller. He will receive the one-time password after entering the code (illustration above).



Once the user has entered the one-time password, all lock-outs will be removed (see illustration left).



The lock-outs will remain disabled until the user selects the menu option “Reinstate Parameter Lock-Out”, but latest until the Monitor is exited. Once the Monitor has been restarted, the lock-outs will once again be in place.

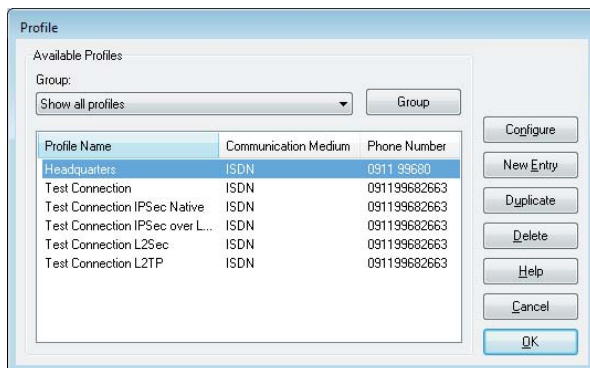
Client-Side Profile Creation

Provided the user is authorised to create personal profiles following a roll-out, or the user wishes to create new profiles following a standard installation, he should proceed as follows.

After a standard installation of the Secure Client software, there are no profiles available as yet. A wizard will appear on screen automatically (for more information, please read the installation manual for Enterprise Suite), which will assist you in the creation of profiles with test configurations. The process will provide you with initial profiles, the data of which can be modified as required. This process is carried out via “Profiles” in the configuration menu of the Monitor.



Once the menu option has been selected, existing profiles will be displayed in a three column list with the headers “Name”, “Communication Medium”, and “Phone Number”. (Illustration below)



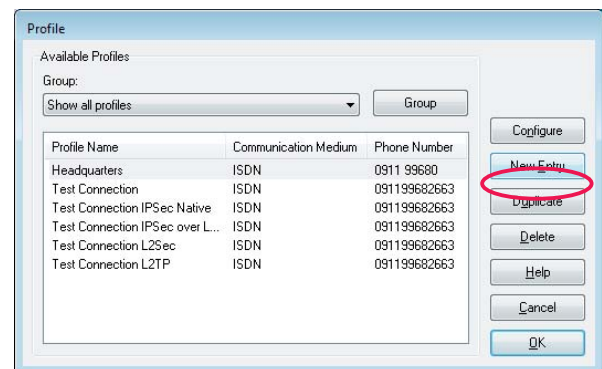
The buttons to the right of the profile settings menu are not available, if relevant lock-outs have been set.

For more information, please read **Profile Settings Modifications** (for the Enterprise Client) and note the different **Configuration Modes**.

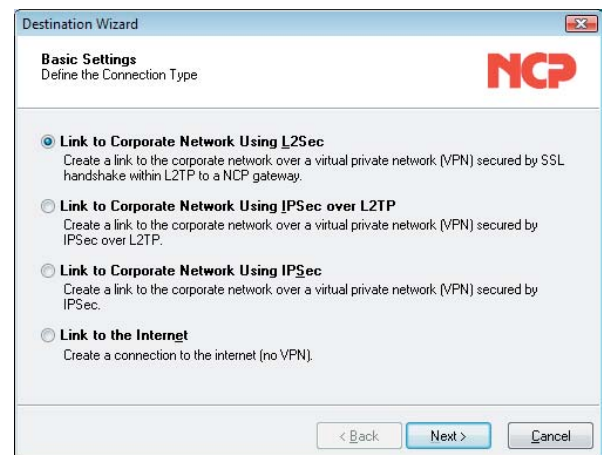
Where no limitations regarding profile settings were set, all buttons will be available, and clicking will initiate their respective functions.

New Profile with the Configuration Assistant

Click on “New Entry” to define a new profile.



The configuration wizard will now assist you in creating a new profile.



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 clicking on “Configure”.

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, Compression)
- 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

- Profile Name
- Communication Medium
- Access data for the Internet provider (User ID, Password, Phone Number)
- VPN Gateway parameters (VPN Gateway, Tunnelsecret, Compression)
- 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

Basic Settings

Dial-up Network
VPN Tunneling
Security
VPN Tunneling
Security
Link Firewall

Basic Settings

Dial-up Network
VPN Tunneling
Security
VPN Tunneling
Security
Link Firewall

Basic Settings

Dial-up Network
VPN Tunneling
Security
VPN Tunneling
Advanced IPSec Settings
IPSec Configuration*

Link Firewall

Basic Settings

Link Firewall



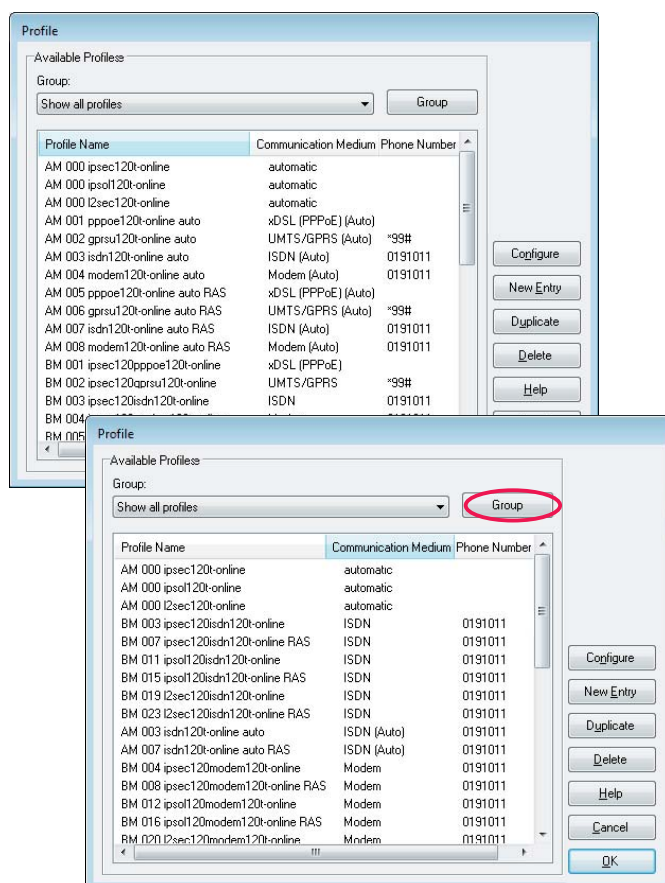
For additional information regarding parameter settings, please check [Secure Client Parameters](#). Click here to open this document.

In the top of the right-hand column, all configuration folders for profile settings are listed, where the requested data must be entered. Clicking on the individual terms will display their relevant descriptions.



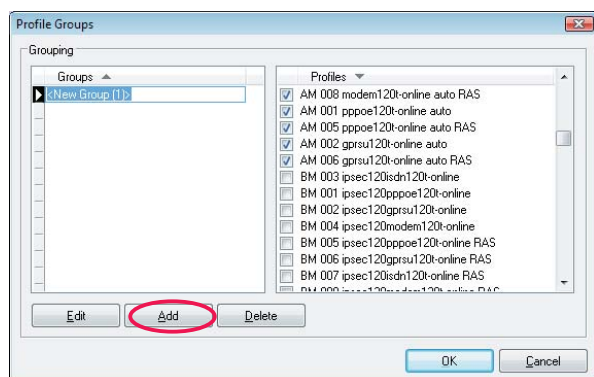
*** Click here for the [IPSec Configuration](#) of the Secure Client, which is divided up into several configuration fields.**

Profile Groups

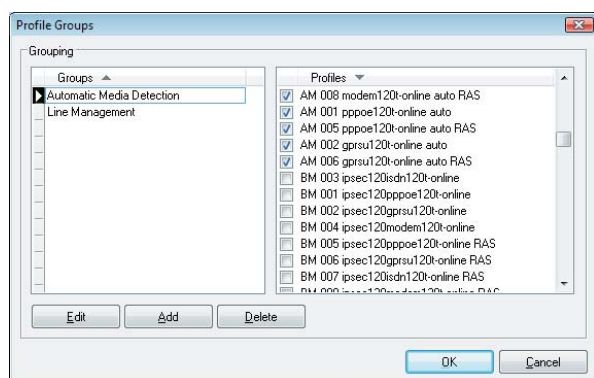


You can sort these profiles in the list of all profiles by name, by communication medium and (in case of a dial-up connection) by phone number. (Illustration left)

Should the list of profiles be too long for sorting, profiles can also be divided up in groups. Click on “Group” above the telephone no. display to open the group configuration (see illustration left below).



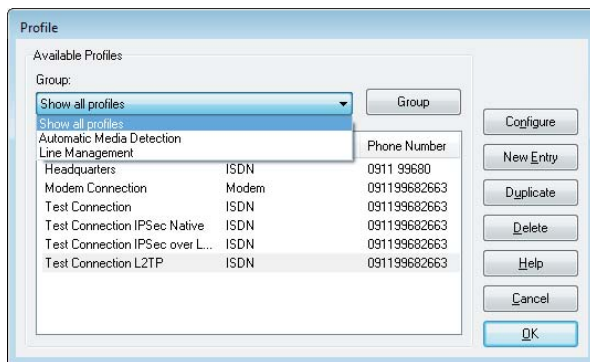
Clicking on “Add” will add a new group to the column on the left, which you can then name (e.g. group “Automatic Media Detection”) if you wish to group together profiles of that type. (Illustration left)



Select profiles from the right-hand column to add to the new group shown in the column on the left. You can associate profiles with multiple groups where required. (Illustration left)

Click on “Edit” to edit the name of the group. Click on “Delete” to remove the group currently displayed, and the relevant profile associations. The profiles themselves will however not be deleted.

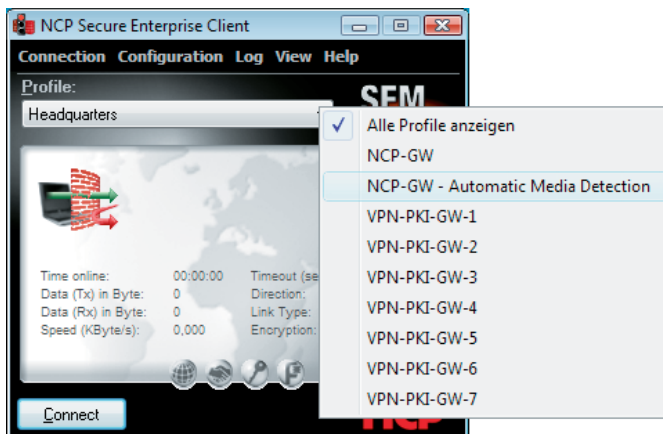
Group Display



You can now display all profiles, or alternatively only those profiles that have been associated with a selected profile group. (Illustration left)



An info text is displayed on the user interface of the Monitor in the profile selection area, ...



... where you can also choose to display all profiles, or just those associated with a particular group.

Symbols and Messages on the Graphic Display

Symbols of the Monitor

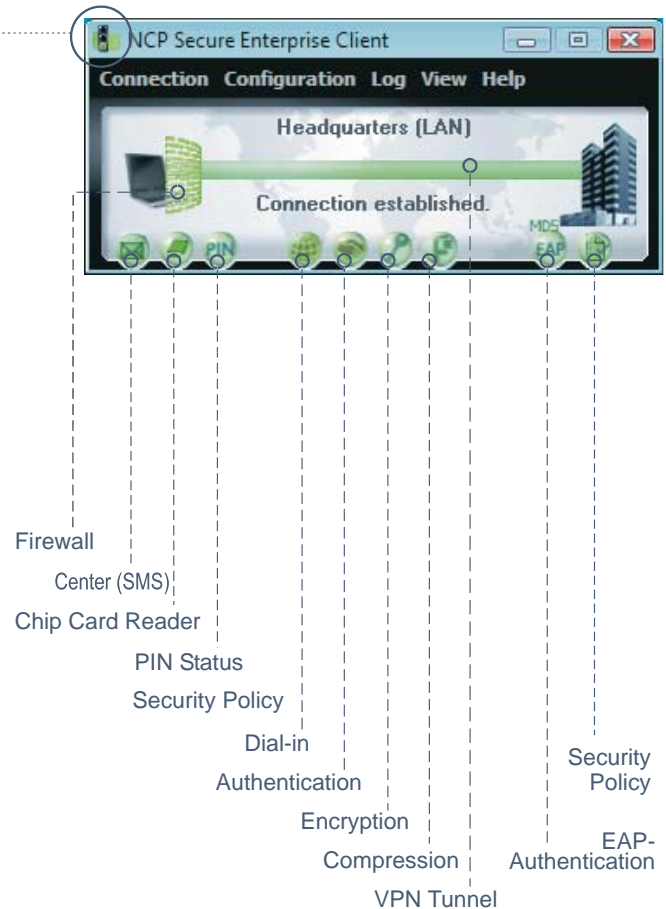
The Client's Monitor interface has been informatively designed with icons. They provide information about the current status of the connection or about specific configured features via appearance and color.

The traffic light icon is always visible when the Client starts. If you minimize (close) the Monitor, this icon will be displayed in the taskbar. Double click on this icon to re-open the Monitor. The traffic light icon only disappears when the Monitor is closed.



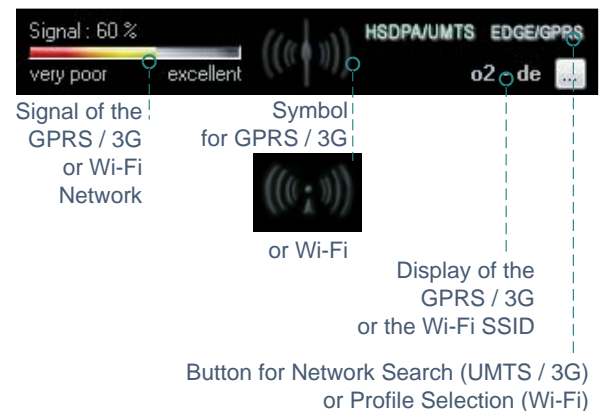
A red system tray light means "No Connection", a yellow one indicates that a connection is being established, and a green light, also in the taskbar - always symbolises an existing connection, for which charges may be accrued.

The other icons are described in details on the following pages.



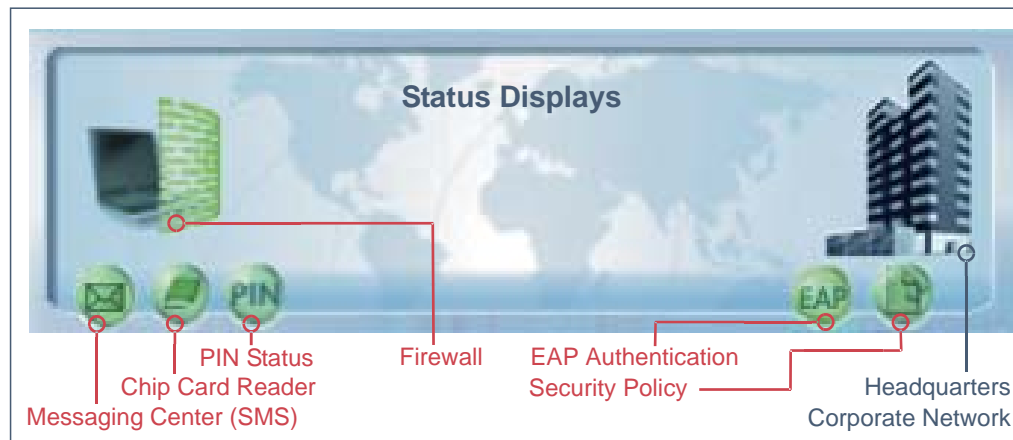
In addition either **Wi-Fi** panel or a **GPRS / 3G** panel will be displayed in the monitor depending on configuration and installation of a multifunction card.

In the GPRS / 3G panel you can select the desired data transmission process by clicking on the respective label. Then the icon will be displayed in green.



Status Displays

The graphic field of the Client Monitor displays different icons depending on the configuration; these icons can take on different status settings depending on the phases of the connection setup. Tool-tips provide brief comments relative to function when you move the cursor over one of the icons. The status displays are described below in the sequence in which they are shown in the illustration below, from left to right.



Messaging Center (SMS)



If the letter is colored in **red**, the **Messaging Center (SMS)** has been activated via the connection menu of the monitor but no suitable modem is available. If the letter is colored in **yellow**, the computer is searching for a GPRS or 3G network, the card is faulty, the SIM PIN is missing, etc. this, of course, will be accompanied with the respective message in the quick tip. If the letter is colored in **gray**, the text messages can be received. If the letter is colored in **green**, a text message has been received. The number of unread messages can be read in the quick tip.

EAP Authentication



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. Double click on the EAP icon to reset 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.

Chip Card Reader



If a smart card reader has been installed and configured (see the document **Secure Client Certificates**), then its icon will be displayed in **blue**.



If the smart card is inserted in the reader, this icon will be displayed in **green**.

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. Double click on this icon to open the dialog for entering the PIN. An incorrect PIN is acknowledged with an error message, and remaining number of possible PIN entry 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 Monitor menu “Reset PIN”) or the “PIN query function for each connection setup” must be activated under “Configuration / Certificate. In the latter case the dialog for PIN entry will not be displayed after double clicking on the grey icon, it will only be displayed after connection setup.



(See the document **Secure Client Certificates**)

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.

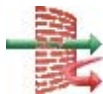


If the administrator has specified a Friendly Net (Friendly Net Detection), and if the Client is in a friendly net, then the firewall icon will be displayed in the color green. Friendly Net Detection specifications are made in the Monitor Configuration menu under “Settings / Friendly Nets”, either by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

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 Phonebook 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.

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.

All security-relevant parameters are defined in this plug-in. Compliance with the specified security policies is mandatory and checked prior to an access to the corporate network.

It cannot be bypassed or manipulated by the user. 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

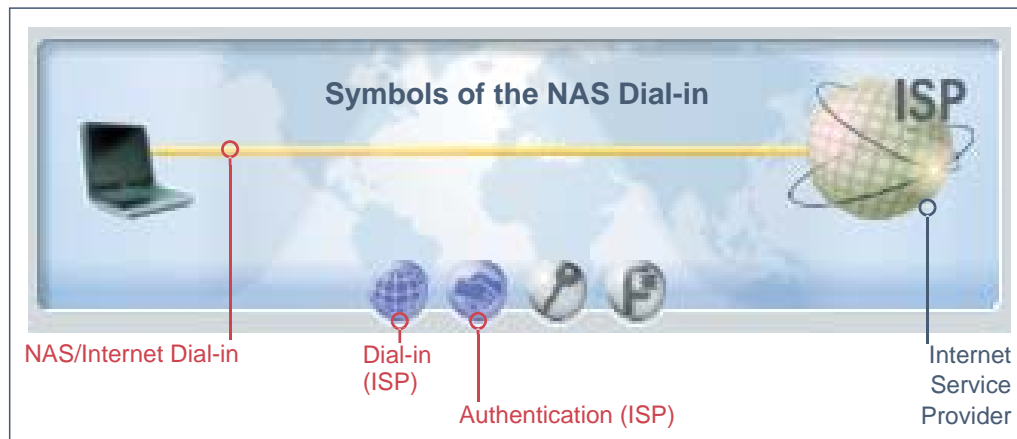
NCP VPN Path Finder Technology



If a connection is established using VPN Path Finder (i.e. using port 443), the monitor displays this via an icon in its state display (below and to the right of the HQ / gateway). The monitor interface displays the icon after VPN dial up. It is also displayed in the Windows Logon interface, via NCP GINA (XP) or NCP Credential Provider (Windows 7).

Connection Setup Symbols

In addition to the status displays the graphic field of the Client Monitor also includes connection set up icons.







Symbols of the NAS Dial-in

If a dial-in to the Network Access Server or Internet Service Provider (ISP) is taking place on the Internet then the dial-in connection will be indicated by a thin yellow line. The dial-in is concluded and the connection to the ISP is established when the thin connection line is displayed in green.



The colors of the NAS dial-in icons change color concurrently with the start of the connection setup.

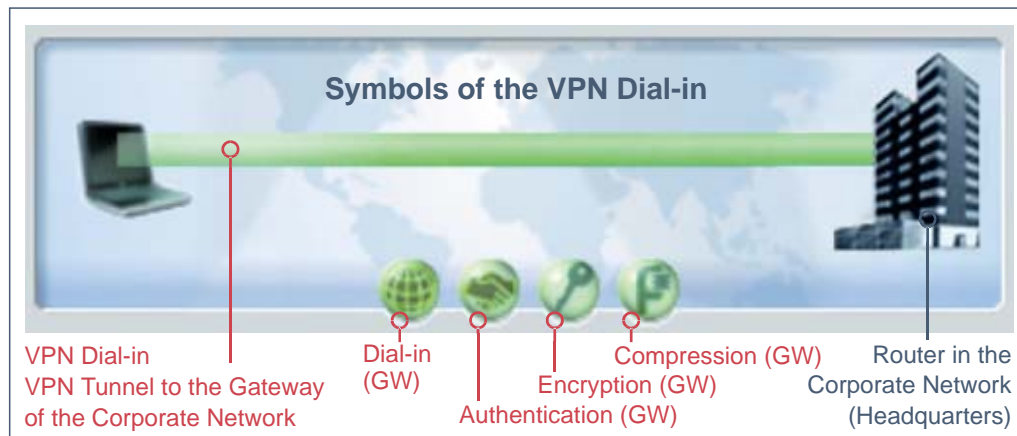


Dial-in to the ISP is displayed with a green globe; authentication at the ISP is indicated with a handshake. During the connection setup its color changes from gray   to blue  , then flashes green, and finally is displayed as constant green to indicate successful connection set up.

The parameters for NAS dial-in are located in the profile settings under “Network Dial-In”. If the profile will be used for “Automatic Media Detection”, then it is strictly required that you enter a user ID and a password under “Network Dial-In”.

Symbols of the VPN Dial-in

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 color concurrently with the start of the connection setup to the gateway. Dial-in and authentication on the VPN gateway are displayed in precisely the same manner as they are displayed for NAS dial-in. In addition there are icons for key negotiation (keys) and compression (pliers), if configuration of these icons is prescribed from the gateway side.

The colors of the icons change from gray to black, 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:

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”.

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 “Configuration / Certificates”, and the issuer certificate of the gateway that will be selected must agree with the user certificate.

Profile Selection and Connection Establishment

Once the software has been installed, and a profile has been configured correctly, a connection to a remote station can be established.

Select the required profile via the selection dialog in the main menu, or via right-click from the profile list displayed.

The Client Monitor does not need to be opened especially, or any dial-up to be carried out in order to establish a connection with a selected profile or a remote station. You will only need to start up the required application software. The connection will then be established automatically, according to the relevant profile settings. A connection can of course also be established manually, by clicking on “Connect” in the Monitor menu.



An existing VPN connection (see illustration above) is symbolised by a solid green bar between the client and the server, under which the message “Connection established” will be displayed.



At the same time, the tray icon will turn green. A green icon, also in the taskbar, will always symbolise a current connection, which may accrue charges. For more information regarding how to control connection charges, please read the Budget Manager description.

Establishing a Connection with the Remote Station

The type of connection to be used, can be configured under profile settings. You have the choice between three selection modes for establishing a connection: automatic, manual, and alternating.



Please note the section regarding connection control, and the automatic connection establishment, located in the parameter description.

Automatic Connection Mode

In contrast with Microsoft’s RAS technology, where the connection with the remote station must be established manually, the Client software functions on the basis of LAN simulation. You will only need to start up the required application software (email, Internet browser, terminal emulation, etc.). The connection will then be established and maintained automatically, according to the relevant parameters in the profile settings.

Manual Connection Mode

A manual connection is established via the Monitor menu “Connection / Connect”, or by clicking on “Connect”.

Variable Connection Mode

For the variable connection mode, a connection must initially be established manually. The connection mode will then alternate, depending on connection status:

- if the connection ends with a timeout, then it will be reestablished automatically at the time of the next request;
- if the connection is ended manually, a manual reconnection is required.

Connect

Provided the Monitor is displayed in the foreground, it will always display the connection status as described in “Connection Status Icons”, regardless of how the connection is established.

Passwords and User IDs

A password (see profile settings / network connection) is required for identifying the user for the Network Access Server (NAS). It can be up to 128 characters in length. Usually you will be assigned a password by the remote station, since you need to be recognised there as well. You receive the password by your Internet service provider, or your systems administrator.

When entering your password, all characters will be displayed as asterisks (*) to prevent others from recognising what you have entered. It is important that you enter the password exactly as given, taking special care to observe capitalisation.



You will have to establish the very first connection manually, and enter your password, regardless of whether or not you have selected the connection mode “Automatic”. The password will then be automatically entered for every subsequent connection, until the PC is either rebooted, or the destination system changes. Therefore the password will be entered autonomously for a number of automatic reconnections, once it was entered to establish a connection originally, even if the function “Save Password” (see Profile Settings / Network Selection) was not activated. Only a reboot will delete the password.



If you don't want the password to be deleted after a reboot, you need to activate the function “Save Password” (see “Profile Settings”/“Network Selection”). Please remember, however, that anyone can work with your Client software, once passwords have been saved.

User ID for NAS Connections

A **user ID** will always have to be entered under “Profile Settings” to establish a connection on the Internet. Without a user ID, no NAS connection can be established.

User ID and Password for VPN Connections

A **user ID** and password for the VPN connection to the gateway (see “Profile Settings / Tunnel Parameters or Identities at the Entry Client) can be entered for profile settings. Where this information has not been prepopulated, an entry prompt will appear at every attempt to connect to the VPN.

Password for OTP Tokens



A prompt for a one-time password and associated PIN will always be prompted, where an OTP token is used (see **Line Management**). The relevant dialog will be displayed, depending on whether or not the OTP token is used for a NAS, or a VPN connection.

User ID and Password Dialog



The dialogs for user IDs and passwords (UID = User ID, PW = Password) can be combined by the administrator via Enterprise Management. Which of the information will be prompted in the two fields depends on the configuration of the lock-outs under NCP Secure Enterprise Management:

- No UID stored => UID field is empty and can be edited
- No PW stored => PW field is empty and can be edited
- Tunnel parameters blocked => UID field grayed out, UID not displayed, PW field empty / can be edited
- BPN UID blocked => UID field grayed out, UID not displayed,
- VPN UID open => UID field can be edited, UID displayed (if present)

Where no password was stored in the default settings for the Management console, the data last entered will be displayed in the Client after startup.

Client Logon

Where a domain server logon is required after Windows startup, and no network connection exists, then the NCP GINA must be utilised. These settings can be determined in the **Logon Options** of the configuration menu, provided they were activated at the time of installation (see **Enterprise Suite Installation**).



A connection is established via VPN during domain logon basically the same way as described under **Connection Status Icons**. Once a profile has been selected by clicking OK, the connection will be established. Where a (soft) certificate has been configured, a PIN entry must follow your user ID and password entry. The other steps of a connection establishment are carried out as described above.

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, and the colour of the system tray icon changes to red for the entire duration of the offline state.

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 above regarding window displays on the Monitor, and the section “Minimise when Closing” discussed above.

A connection is interrupted properly, by either selecting “Connection/Disconnect” from the Monitor menu, or by right clicking the disconnection function in the context menu.

If you wish to maintain the option of being able to disconnect 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

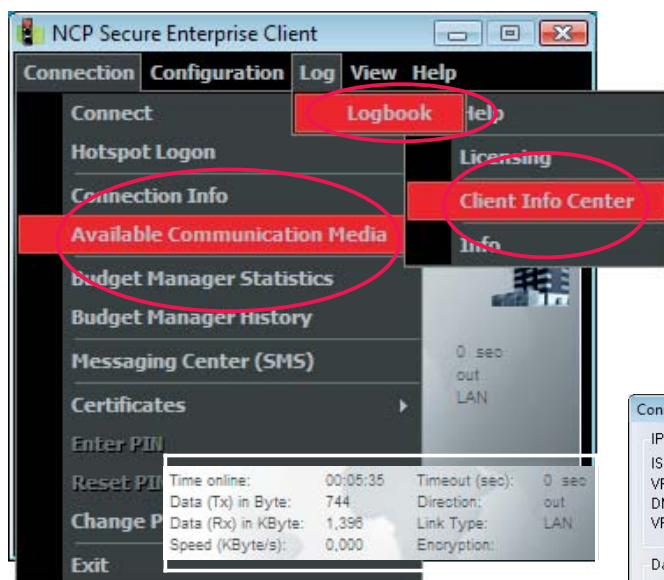
Where “Timeout” has been activated, the connection will be interrupted automatically. This parameter defines the time frame following the last data movement (received or sent) before a connection will be disconnected automatically. The value is input in seconds between 0 and 65535. Default value is “100”.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

Should your connection work with a call-charge impulse, then the Secure Client software will use the impulse interval for determining the best time for terminating a connection for the value you have entered. The timeout, which depends on the relevant call-charge interval, runs in the background and helps to reduce connection costs.

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

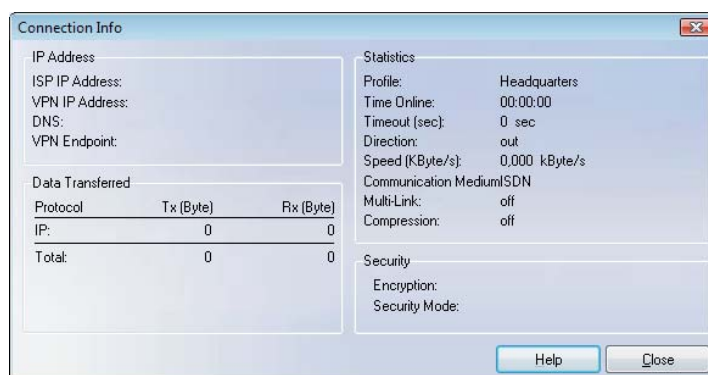
Information Windows of the Client

The Secure Client provides a number of information windows, which display statistical data for connection parameters, for connection phases, for encryption technologies used, and for online behaviour (e.g. transfer rate and duration).

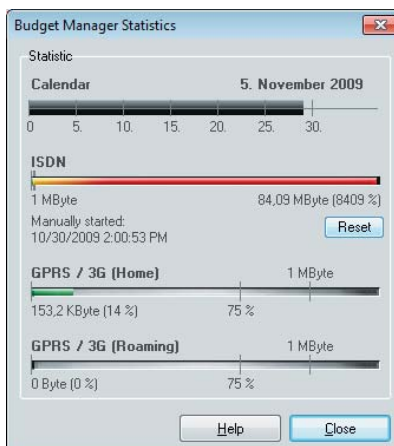
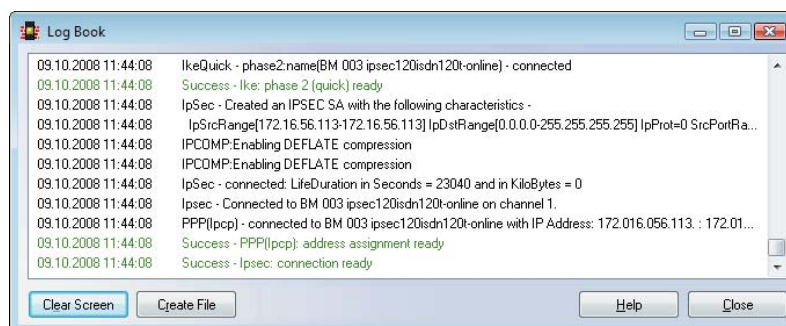
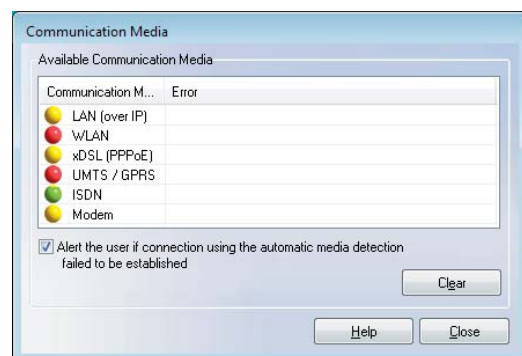


These information windows can be found in the Monitor menu under “Connection”, “Log”, and under “Help”.

Information windows under “Connection” and “Log” can be displayed simultaneously where required, while modifications are carried out in the Monitor menu, or for profile settings.



Connection information (illustration on the right above) can be set to “Hidden” by the administrator. Then the menu option will not be available, and IP addresses can not be displayed. Information regarding data transfer, connection medium, and security can alternatively be displayed via the statistics field of the Client (above).



The user obtains an overview of his (monthly) budget in the statistics regarding connection control. The statistic shows, with the current date, how much of the maximum exhausted budget in hours or bytes already have been used since the first of the current month or since the start of monitoring. Here you also can see limits that can be set in order to trigger certain actions. (Illustration above left)

For **Budget Manager Historie** click [here](#).

Connection Info

Connection Info displays statistical values, the security keys used, and which IP addresses are being exchanged during PPP negotiations between client and server.

Time Online

Time Online is a display of the entire time period, during which you are connected with a particular remote station, independently of any time-outs. The Time Online value will only be reset to (0), when you establish a new connection with a nother remote station, or the PC is rebooted.

Timeout

The time until the next timeout is displayed on the Monitor. Directly after the last data exchange (including handshake), the timeout timer is activated. The timeout value is preset in profile settings under Line Managment.

Direction

This section displays the direction of your communications as follws:

Out = an outgoing connection registered on this channel;

In = an inward connection registered on this channel.

Throughput

The rate displayed may vary depending on the current data throughput.

Communication Medium

The connection medium defined in the profile settings configured under Basic Settings is displayed.

Multilink

Where the connection consists of a number of ISDN B channels, this display will show "On".

Compression

Where compression is required, you need to activate the option in profile settings under Connection Control. Compression can only be utilised successfully, if the remote station supports compression as well. STAC compression with History is CISCO compatible. (IPSec compression is displayed as "On".)

Encryption

The relevant encryption algorithym is displayed. The following encryption types are supported: AES, Blowfish, Triple DES. The encryption type is predetermined by the central system, so that you only need to enter "assigned by remote station" in profile settings on the Client under "Security".

Key Exchange

A display of the type of session key exchange:

Static Key

The key must be identical for the client and for the central system. It is entered under "Profile Settings / Security / Static Key".

SSL

The session key to be transmitted is encrypted with a newly generated private key. Key negotiations are predetermined for the security mode L2Sec by the remote station.

SSL with Certificate

The private key for the certificate used encrypts the session key. These key negotiations are predetermined by the remote station in "Profile Settings" under "Security / Encryption (L2Sec)".

IKE (IPSec)

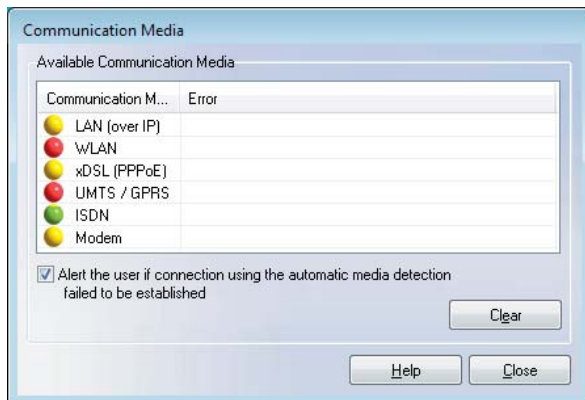
The encrypted control channel for phase 1 negotiations is used for transmitting the session key.

Rx and Tx Bytes

Rx and Tx Bytes displays the amount of data sent (out) and received (in). The total amount (Total) and data amounts differentiated by protocol, are displayed in bytes (1 byte = 1 character). Data transfer via SNA and NetBIOS protocols is only activated for the Client software of the Enterprise version.

Available Communication Media

Here, user data regarding available communication media, and the currently used medium are displayed. Where several communication media are utilised, the Client will recognise automatically, which media are currently available. They are displayed with a yellow signal icon, while the currently active connection medium selected by the Client is displayed with a green signal icon.



By activating the relevant checkbox, this window will automatically be displayed during media detection, when a connection has failed. This also applies where the Client Monitor has been minimised. The error will be displayed in red font behind the selected media type. Deleting will remove the text.



Please see the parameter descriptions for the profile settings **Basic Settings** for the client for configuring **automatic media detection**.

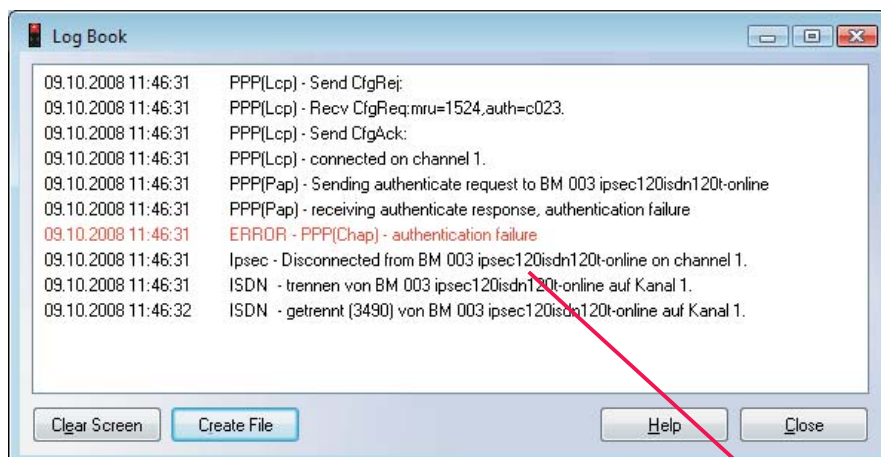
Log

The log function establishes a log of all communication events for the Secure Client software. Selecting the log function will display the window “Logging”. Data displayed here, will remain cached until the next reboot. Clicking on “Delete” will delete the contents of the window.

When you open a file, a second window is displayed, where you can enter the name and path of a file, where the contents of the window can be saved (default: ncptrace.log). All transactions, including selection and reception, including addresses, are logged automatically, and saved in this file until you close the file. If you create a file, you will be able to check transactions for an extended period of time. The closed log file can be used for analysing transactions under Secure Client, or for troubleshooting purposes.

When you close the log window, the window “Logging” will close as well, and you will be returned to the Monitor.

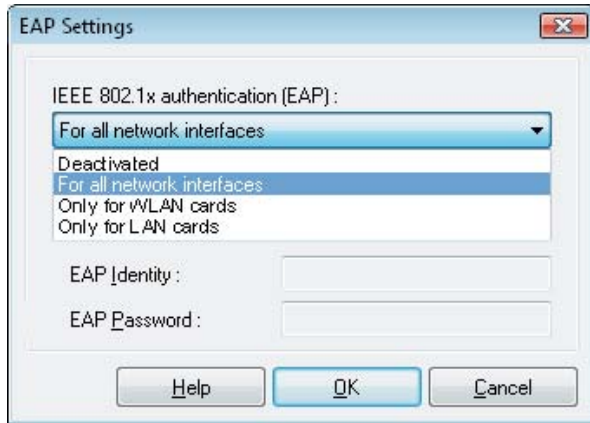
An additional log file logs all Client actions during the past seven days. Log outputs older than seven days will be deleted automatically. The file is located in the installation directory under LOG, with the name NCPyymmdd.LOG. It will be written (with a date in the format yymmdd) each time the Monitor is exited. The file can be opened and edited with any text editor.



Errors will be displayed with red letters in the logbook. These errors are also displayed in the graphic display field of the monitor (see right).



EAP Options [Configuration]



You can specify whether EAP authentication will only be executed via WLAN cards, LAN cards, or via all network cards, in the “EAP Options” of the Monitor menu. The setting made here applies globally for all phonebook entries. In an activation box the EAP authentication can be set as follows:

- Deactivated
- For all network cards
- Only for WLAN cards
- Only for LAN cards

EAP MP5

This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication Mode for the access to the wireless LAN. You can prevent unauthorized users from getting into the LAN via the hardware interface with the Extended Authentication Protocol (EAP MP5).



You can use either “VPN User ID” with “VPN Password” (from the configuration field **Tunnel Parameters**) or your own “EAP User ID” with an “EAP Password”.

Certificate content can be automatically transferred if in the profile settings under Tunnel Parameters VPN User ID and VPN Password are transferred from the certificate, and if “Use VPN User ID and VPN Password” is activated in the EAP options.



For **EAP-TLS** (with certificate) now the EAP user name can be directly referenced from the certificate configuration. The following content of the configured certificate can be used by entering the appropriate placeholders in the EAP configuration:

```
Commonname : %CERT_CN%
E-mail : %CERT_EMAIL%
```

After configuration of the certificate these placeholders are entered in the monitor menu under: Configuration / EAP Options / User ID and Password. Double click on the **EAP icon** to reset the EAP. Subsequently a new EAP negotiation will be executed automatically.

Logon Options

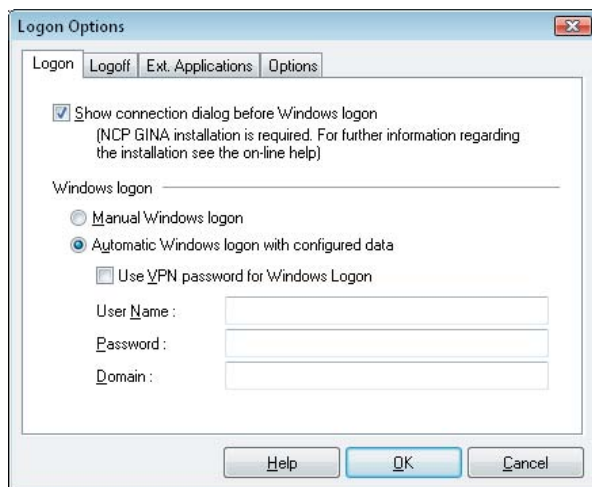
Please note that the client logon option (Gina / Credential) must have been installed in order to use this menu option. Normally this occurs when the client software has been installed, however, it can also be installed retroactively with the program `rwscmd.exe`. The logon options are only effective when the computer has booted.

Logon [Logon Options]

Because the connection set up to the gateway occurs prior to the Windows logon, the logon to the remote domain is already encrypted and the firewall is activated.

Display connection dialog before Windows logon

The dialogs of the logon option (GINA / Credential) can be hidden via the monitor menu without deinstalling the logon option. Thus concatenations of the logon option that may possibly be necessary for the respective work environment remain intact.



If you want to display the dialog, then note that the logon option must be installed in any case. This can be done in three ways:



- During **software installation**, the system asks the user if he wants to use the Windows logon via the logon option (GINA / Credential). If yes, it will be installed.
- Retroactive installation is possible via the command line interface `rwscmd.exe`, likewise retroactive de-installation is also possible.
- The logon option is also installed if an appropriate profile is provided via Secure Enterprise Management.

If the logon dialog does not appear, the connection to the domain server cannot be set up via the logon option. In other words you must have the “Display connection dialog before Windows logon” so that in the boot phase the connection to the VPN gateway can already be set up. For this connection set up you must enter access data for the network dial-in, or PIN and SIM PIN must be entered before the Windows logon.

Windows Logon

The following Windows logon can be executed automatically or manually depending on configuration. “Execute manually” means that the user must enter his logon data manually in the Windows logon screen. Automatically means that the client software will transfer the data entered here to the Microsoft logon interface (GINA / Credential) without user intervention.

The VPN password from the profiles under “VPN parameters” which in turn can be read from the certificate can also be used for the Windows logon.

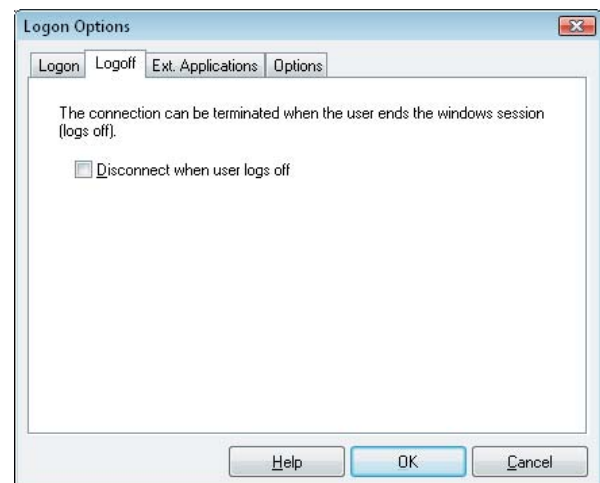
If you use the logon option with callback then “Negotiate PPP callback” must be activated (see: parameter field “Callback” in the profile setting).

To select the destination with the logon option please see the section “Set up a connection - Client logon” and the appendix for Mobile Computing.

Logoff [Logon Options]

The client connection to the VPN gateway or ISP can be maintained when a Windows logon is executed.

This permits a change of Windows users on the computer, without having to disconnect the VPN connection.

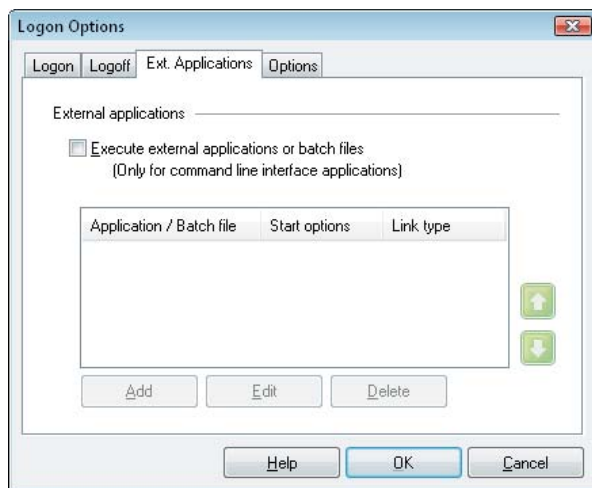


External Applications [Logon Options]

Use this configuration field to start applications or batch files, depending on the Client Monitor (no Windows programs!).

The external applications are added as described on the next page. The call sequence from top to bottom can be changed with the green arrow keys. After you have selected the function “Start external applications or batch file” you can select an application or batch file from the computer, this application of batch file is then loaded, depending on the start option:

- execute before a connection has been established (precon)
- execute after a connection has been established (postcon)
- execute after client Logon (always)



The latter start option permits you to start applications after the EAP negotiation via the logon option (GINA / Credential) and subsequent “Local logon” without VPN connection.

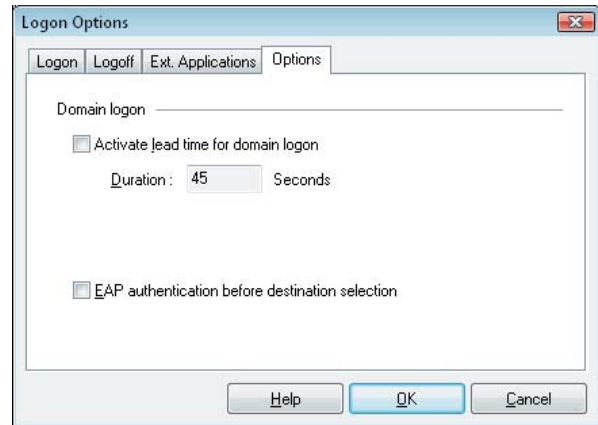
In addition, the application can be started depending on the connection type of the destination system that is selected in the logon dialog. The application always starts if the connection type “All” has been selected.

“Wait for domain logon to complet (postdom)” means that after the initialization period, the application is started immediately.

The wait function “Wait until the application is finished” can then be relevant if a series of batch files is to be executed one after the other.

Options [Logon Options]

Windows requires a certain initialization time between network logon and domain logon. This preparation time for the domain logon can be activated and set here. The Windows logon will only be executed after the connection set up, after the initialization time set here has elapsed.



The default value is 45 seconds and can be changed if needed.

Subsequently you can select whether the connection from the Client software to the gateway is setup via the “display connection dialog before Windows logon” checkbox on a remote domain. For the connection to the gateway it may be necessary to enter the PIN for the certificate, as well as for the SIM card and the (non-saved) password for network dial-in, before the password for the Windows logon can be entered.

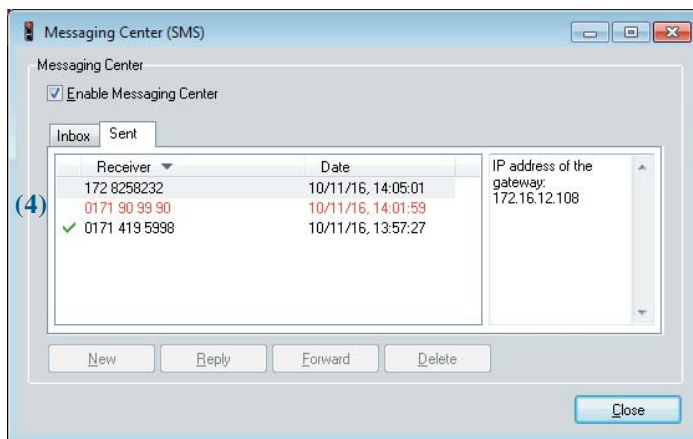
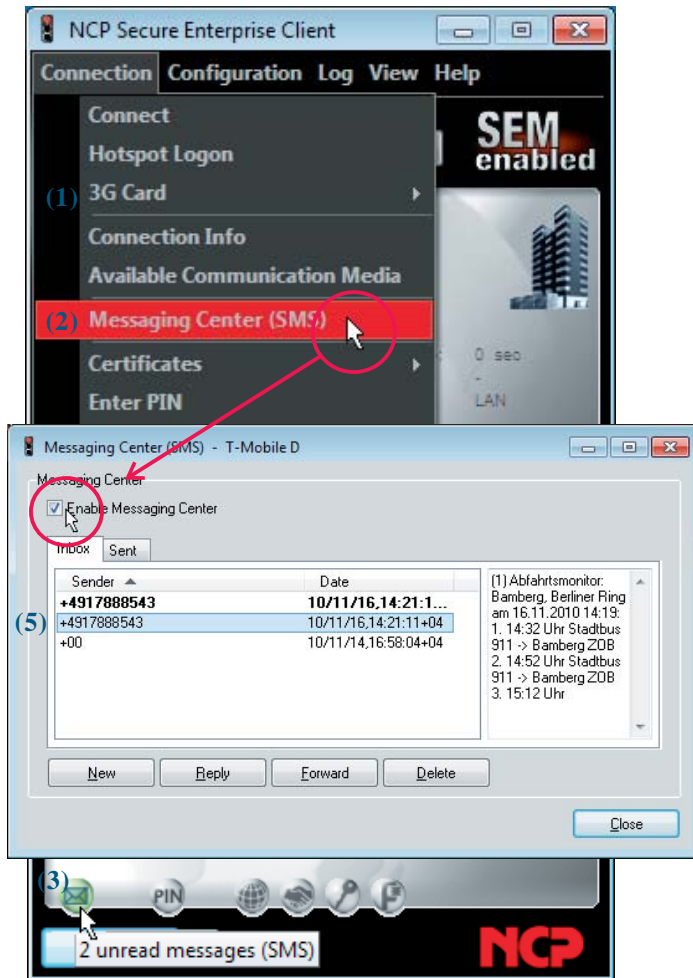
If you do not activate the function in the adjacent window, then the password and PIN for the client will only be queried after the Windows logon.

EAP Authentication before Profile Selection

If this parameter is activated then EAP authentication will be executed prior to the destination dialog in Gina and the system will ask for the necessary PIN, regardless of whether EAP will be required for subsequent dial-in. This parameter can be used, for example, if the client Gina will only be used for EAP authentication, without setting up a connection to destination system (use as a pure EAP client).

If this function is not activated, then EAP authentication will be executed after the destination selection.

Messaging Center (SMS)



Enable Messaging Center

It is possible to enable the messaging center if a GPRS / 3G card is installed. The GPRS / 3G card is recognized by the system and activated as soon as the SIM PIN is entered. (If it is not recognized, the message “modem not found” is displayed.) The currently selected telephone network is displayed in the header of the messaging center window.

In order to activate, open the “SMS Center” in the connection menu. The monitor displays successful activation with a letter symbol (3).

In future you can open the SMS Center by simply clicking this **letter symbol**.

Writing and sending messages



In order to write a new text message click on “New”. The text message may not exceed a length of 125 characters! All alphanumerical characters and special characters of western European fonts are permitted.

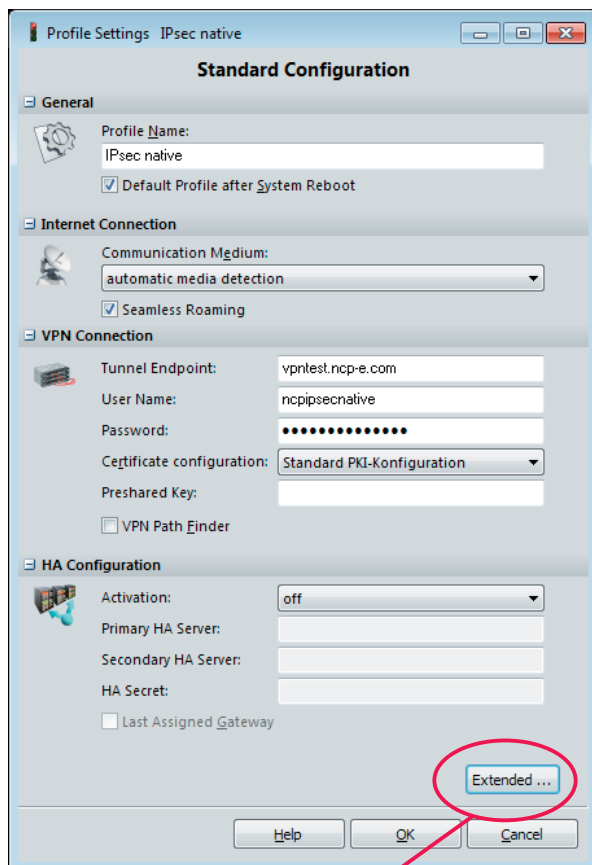
Type the phone number of the remote side conventionally. Click OK in order to send your text message.

If the text message cannot be forwarded to the provider, i.e. the mobile connect card is faulty, the text message is displayed in red font in the “sent” list.

Receive messages

The number of messages to be read is displayed in the quick tip with the green letter symbol. Click the letter symbol, in order to display the list of received text messages. All text messages which have not yet been read are displayed in bold. All text messages are saved within that list until you delete them.

Configuration Modes



Profile settings can be configured using one of three modes: Standard, Extended and Expert.

Providing the administrator has enabled Expert mode profile settings can be modified using any of the different modes.

When OK is pressed any changes made to the configuration of the currently selected profile will become effective, regardless of which configuration mode is selected. The changes will be then reflected across all three modes.

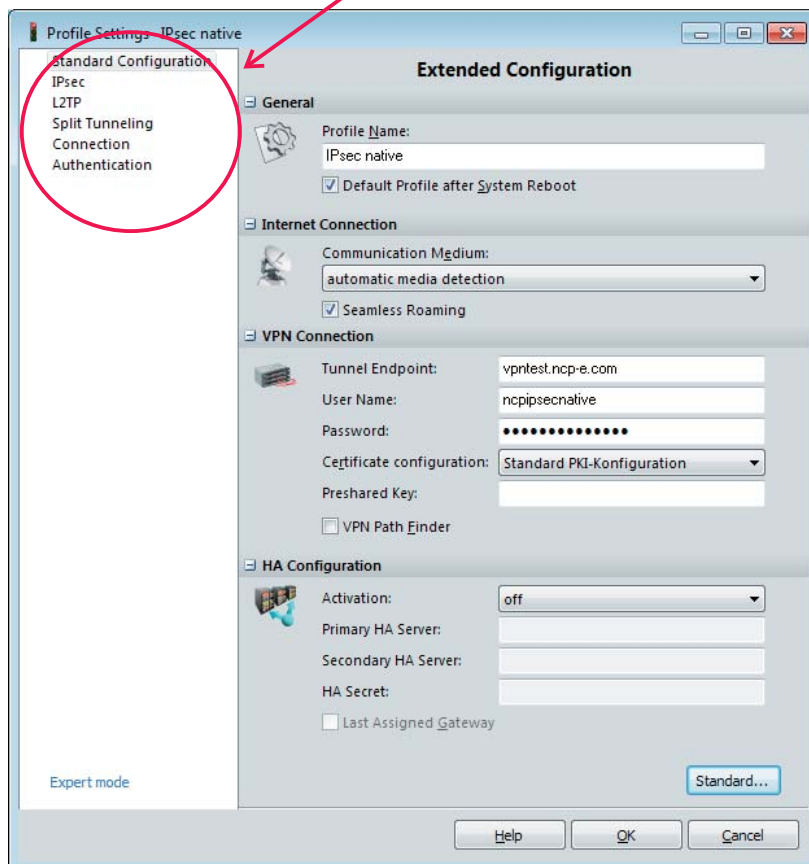
When a profile is first opened via the configuration menu “Configuration / Profiles”, the default values are displayed in a single configuration window (see fig. on the left).

From then on, five further configuration windows can be opened using the “Extended” button and then closed using the “Standard” button. “Expert” mode shows the current settings of all available parameters.

The configuration mode selected when the last “Edit” operation was finished will be re-opened when a subsequent edit is started.

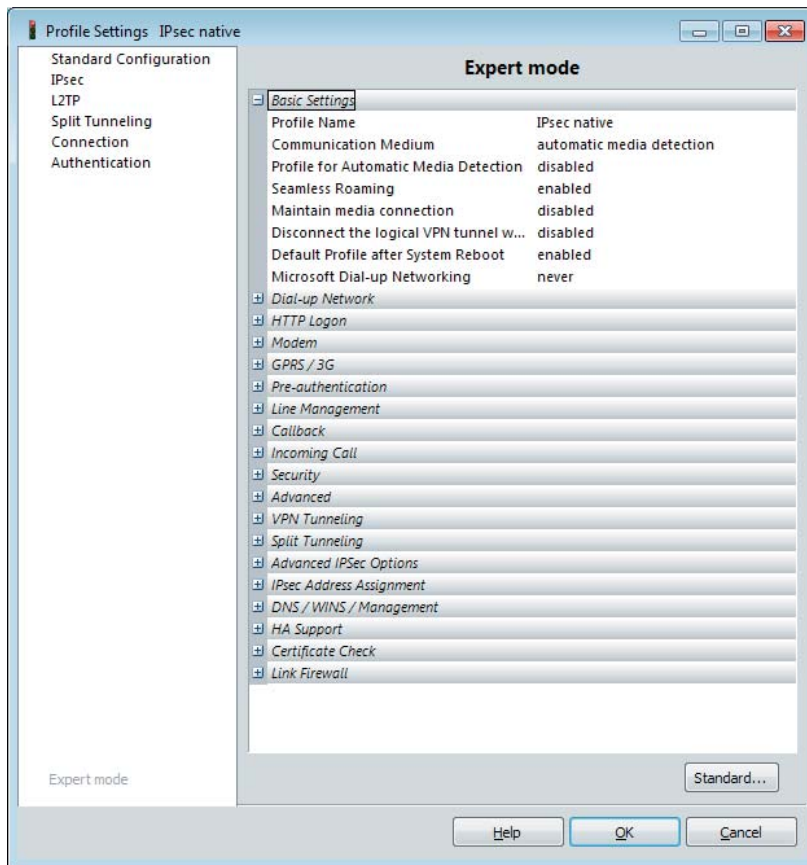
Standard Configuration

The Standard Configuration displays the most important parameters (about communication medium, network connection, VPN gateway access data and HA support).



Extended Configuration

The Extended Configuration displays additional parameter fields associated with Advanced IPsec Settings, L2TP capabilities, Split Tunneling, Connections and Authentication Options.



Expert Mode

In Expert Mode every setting of every parameter in the Client software can be modified. To do this a list of parameters is displayed in the RH window folder and the appropriate setting for a parameter can be selected as required.

In Secure Enterprise Management **Expert mode is disabled by default!**



The **Parameter Descriptions** mirror the list displayed in Expert mode.