

Functional Description and Configuration

high security remote access

Mobile Computing with Enterprise Clients





Mobile Computing

with the Secure 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, November 2010

Mobile Computing with the Secure Enterprise Client	5
Overview of Contents	5
3G Card	6
Create a Profile for Mobile Radio Connections via UMTS / 3G	7
Basic Settings	7
GPRS / 3G	7
The 3G Card in the Client Monitor	9
Wireless LAN	11
Wi-Fi Connection and Wi-Fi Profile	11
Assistant for Wi-Fi Profiles	12
Connection to the Wi-Fi Access Point and Wi-Fi Profiles	12
Wi-Fi Profiles	13
General Profile Settings	13
Encryption	13
IP Addresses	14
Authentication	14
Authentication with a Script	14
WISPr Login	15
Statistics	16
VPN Connection and WLAN State	17
WLAN Automatic	17
Establishing the VPN Connection	18
Roaming with IPSec Connections	18
Secure Mobile Computing in WLANs and at Hotspots	19
Automatic Hotspot Logon	20
Conditions	20
Hotspot Configuration	20
Hotspot Logon	21

Mobile Computing with Enterprise Clients

The first part of this document describes the configuration of the secure client when a **3G card** is used for the **GPRS / 3G** connection medium.

The second part describes the **Wi-Fi configuration** and setting options for logging into a **Hotspot** via a radio network, particularly using the **WISPr** protocol.

Overview of Contents

- **3G Card**
- **Create a Profile for Cell Phone Connections via GPRS / 3G**
- **The 3G card in the Client Monitor**
- **Scan for Available Networks**
- **Activating GPRS / 3G**
- **Wireless LAN**
- **Connection to the Wi-Fi Access Point and Wi-Fi Profile**
- **Wi-Fi Profile**
- **Configuring WISPr**
- **VPN Connection and Wi-Fi Status**
- **Wi-Fi Automatism**
- **Secure Mobile Computing**
- **Automatic Hotspot Logon**
- **Configuring Hotspots**
- **Hotspot Logon**



When configuring a VPN profile, the possible parameter settings are described in the **Enterprise Client Parameters** documentation.



The **Enterprise Client Navigation** provides an overview of everything. This PDF file lists all the documents currently available on your product.

You can skip straight to all the relevant documents from the Navigator and, if they have not yet been saved in your Navigator Index, download them from the NCP website.

3G Card



If a mobile radio data card (GRPS / 3G / HSDPA / HSUPA) is used, special mobile computing features can be used with the client software using the card's properties. The fact that the secure client provides direct support for a 3G card does away with the need to install management software from the card being used.

The NCP secure client combines all the communication and technical security mechanisms for cost-effective data communication based on the end-to-end security principle. The **Enterprise Client Monitor** PDF file describes the client monitor's visual displays of all the connection states like the field strength, the selected network and the provider.

From the moment the system is started, the integrated, dynamic personal firewall is also optimized for remote access and protects the mobile tele-workplace against all attacks and guarantees maximum security.

Please refer to the compatibility list to see which 3G cards your client version supports.

From Version 9.02 Build 5, once the g3detect.dll file has been imported, the secure client supports new PCMCIA radio cards which you will see listed on the latest compatibility list at:



<http://www.ncp-e.com/en/support/compatibility/mobile-connect-cards.html>

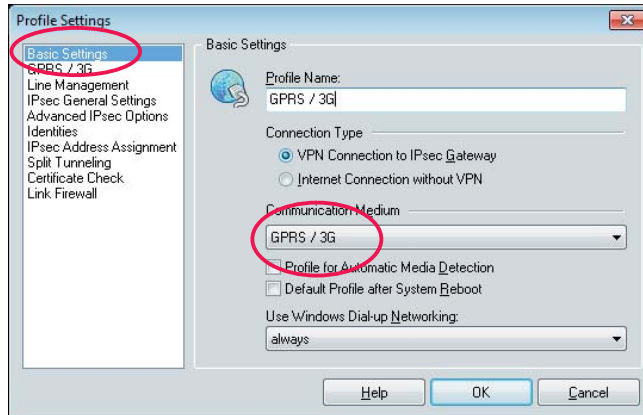
Please note that you need your network operator's access details:

- possibly user ID, password
- character string for phonenumber (destination)
- Access Point Name (APN)
- SIM PIN
- PUK

Create a Profile for Mobile Radio Connections via GPRS / 3G

After installing the 3G card and updating the client software with the file g3detect.dll, a profile can be created by which the 3G card is directly addressed as a modem. How to create the new link profile:

Basic Settings



Profil Name

Enter a freely selectable profile name.

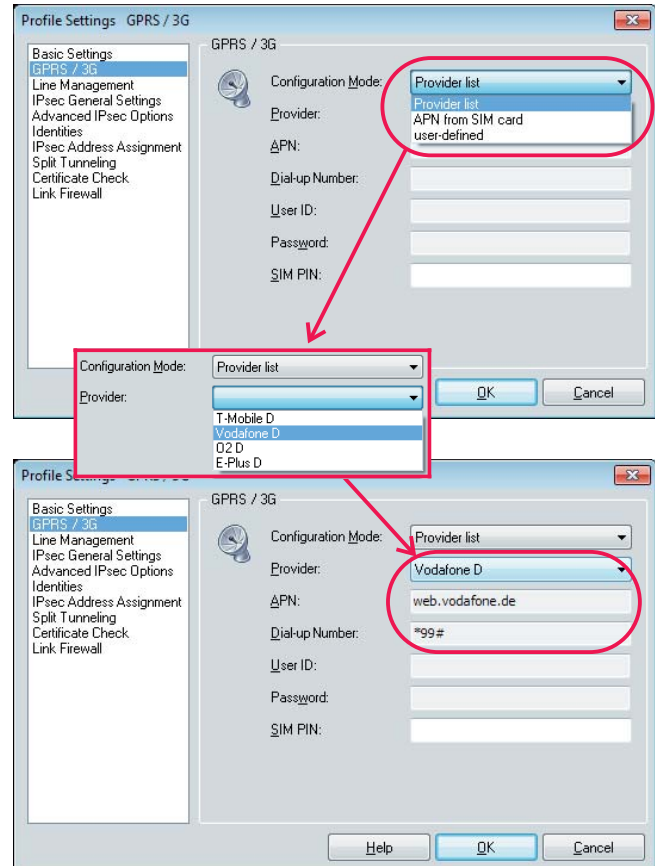
Communication Medium

Select the communication medium GPRS / 3G (illustration above). This causes the parameter folder GPRS / 3G to be automatically entered into the list (illustration above).

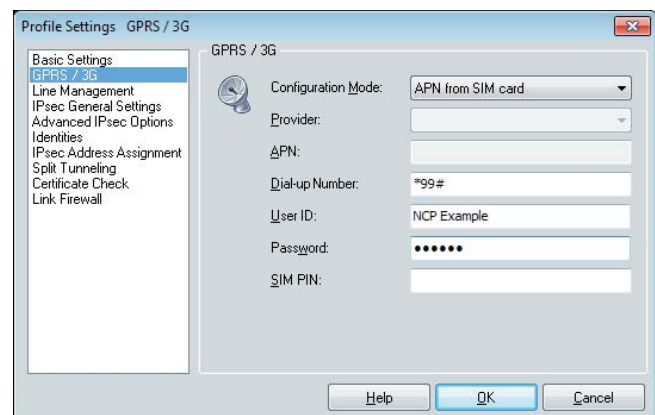
GPRS / 3G

Open the parameter folder GPRS / 3G. Three configuration modes are available:

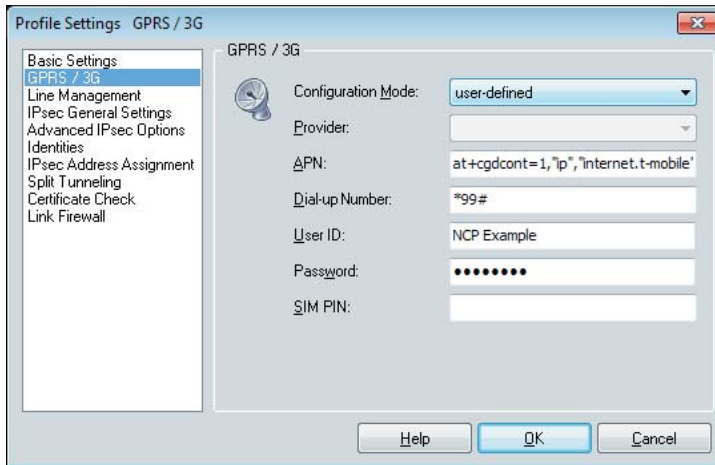
In the default setting (Illustration below) you can select your provider from a **Provider list**. (If your provider is not on the list, you can expand the list with the data of your provider; the list is stored as APN.INI file in the installation directory.)



In the second mode **APN from SIM card** the APN is read from the SIM card (currently only available for T-Mobile) (Illustration below).



The third mode is user-defined (Illustration below) and all data have to be entered manually.



APN

You receive the APN (Access Point Name) from your provider. It can either be entered manually or read from the provider list. It is “web.vodafone.de” for Vodafone and “internet.t-dl.de” for T-Mobile.

[The string
`at+cgdcont=1, "ip",`
 for the AT command is default for passing the APN to the SIM card. The continuation of the string varies depending on the provider. Examples:

```
at+cgdcont=1, "IP", web.vodafone.de
```

APN for Vodafone

```
at+cgdcont=1, "IP", "internet.t-dl.de"
```

APN for T-Mobile (SIM-D1-Card)

User ID / Password

In the mode “APN from SIM card” and in the user defined mode, a freely assignable user ID and password have to be entered as access details for the internet service provider (ISP), unless, of course the provider has given you special passwords. Dummy values suffice with Vodafone and T-Online.

Dial-up Number

For the “dial-up number”, a certain string of characters has to be entered. This depends on the 3G card (3G card) and provider and it tells the modem which type of data connection should be established. Usually, this is *99# but if no connection set-up is possible, please contact your cell phone provider. Afterwards enter your SIM PIN.

SIM PIN

If you are using a SIM plug-in card for GPRS or 3G, please enter the PIN for this card here. If you are using a cell phone, this PIN has to be entered into the phone.

The billing (and the identification) is done via the SIM card.



If the administrator has locked this configuration window, please **enter the SIM PIN** in the SIM PIN dialog and save it in the configuration. This dialog always appears when you select a link profile with the Communication Medium GPRS / 3G or establish a connection via GPRS / 3G.

Password Prompt at 3G Connection Setup

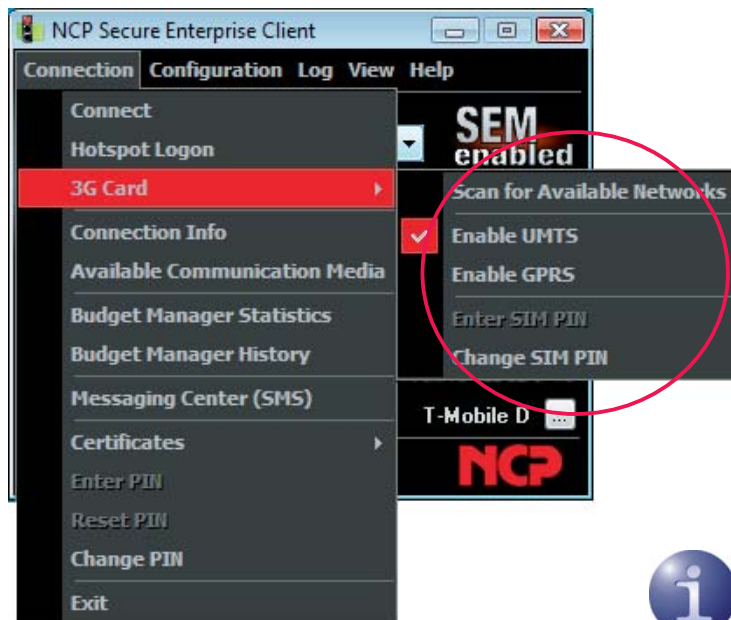


If the 3G connection requires the user to enter a user ID or password, because the company's internet access has an APN or provider of its own, for example, user identification prompt can be automatically displayed in a new window. In order to use the forced password prompt, enter <pwreq> (including angle brackets) in the password configuration field.

The 3G Card in the Client Monitor



Please also note the secure client monitor's performance characteristics and optional settings below.



After a 3G card has been installed, the menu item “3G card” is displayed in the connection menu of the monitor. (Illustration above)

Apart from that a GPRS / 3G display is shown in the monitor as soon as a profile with communication medium GPRS / 3G has been selected for connection set up (Illustration above to the right). (Please also refer to the section **Symbols of the Monitor**.)

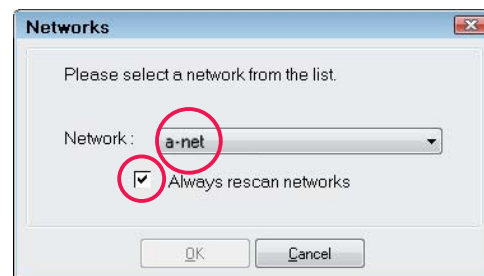
Scan for Available Networks

After the GPRS / 3G display has been opened, the installed 3G card automatically searches for a radio network and displays it with the corresponding field strength as soon as it is found. (“T-Mobile D” in the illustration below).



If the field strength is too low, the card automatically switches from the 3G data transmission technology to GPRS, at which point the connection is retained. If the field strength increases again, the card automatically switches back to 3G.

A search for alternative networks can be triggered manually by selecting the menu item “Scan for Available Networks” or by clicking the [...] button in the GPRS / 3G display.



If the search for an alternative network has been run, a window appears displaying a choice of networks. Here you can select the network you want from a list.

If the checkmark is removed from the window, after clicking the [...] button in the GPRS / 3G display, the new network search is not started -rather, this window is reopened.

The connection can be established in exactly the same way as with a fixed network, or alternatively with the “automatic, manual or variable” modes.

The current communication medium is coloured in green in the GPRS / 3G display.

If the connection is set up, work can proceed as in the local company network. This also applies when the card automatically switches from the 3G communication medium to GPRS because the field strength is insufficient because the connection remains. If the field strength increases again, the card automatically switches back.

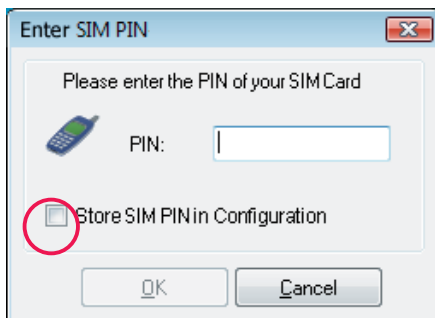
Activate GPRS / 3G

The data transfer technology can also be changed manually. To do this, you click the text with the desired transfer technology you want or you select this menu item. When you change the medium manually, the connection is first of all terminated.



The connection is set up again automatically if this has been configured in the parameter folder **Line Management**.

Enter SIM PIN



The dialogue box for entering the SIM PIN automatically appears at connection set-up if the **SIM PIN** has not been saved yet.

Any unsaved SIM PIN remains valid until the next boot process.



Save SIM PIN in Configuration

The SIM PIN can also be saved in the configuration by activating this function if the administrator has locked the configuration window modem to inputs.



In this respect, please also refer to the **Enterprise Client Configuration Lock** in the **Enterprise Client Monitor** description.

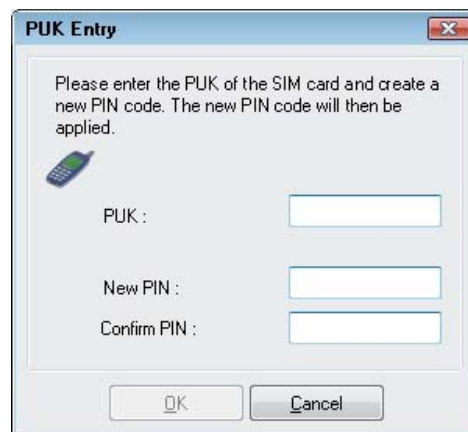
The **SIM PIN** can be entered without being saved **prior to establishing** the connection using the 3G Card submenu (previous page).

Change SIM PIN

The SIM PIN can only be changed if the SIM PIN that was previously valid is entered correctly.

Enter PUK

If the SIM PIN is incorrectly entered three times, the window for entering the PUK (Personal Unblocking Key) that is enclosed with the SIM card appears.



When the PUK has been entered correctly, a new SIM PIN can be entered.

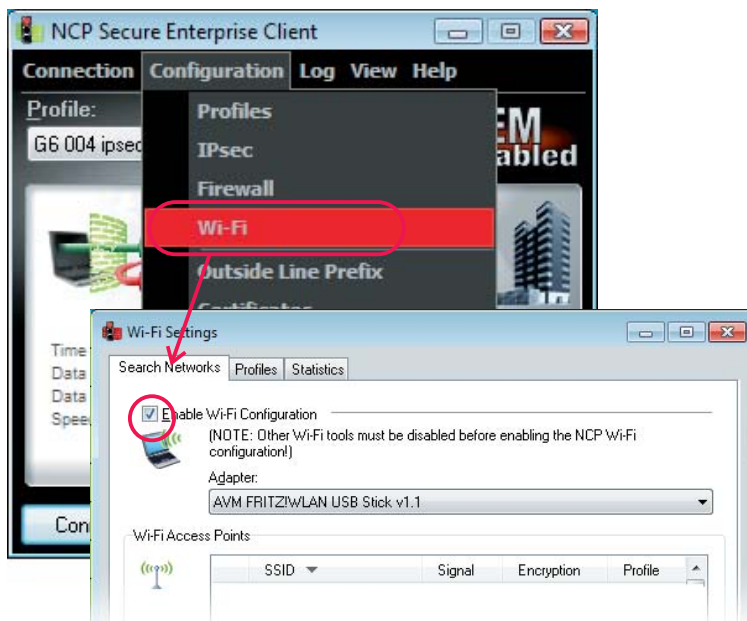
Wireless LAN



If a VPN connection needs to be established from the client to the company network via a wireless LAN, the **Wi-Fi** communication medium is selected in the profile settings of the client.

For the radio network connection to the access point, a Wi-Fi adapter must be installed and a **Wi-Fi Profile** created on the client.

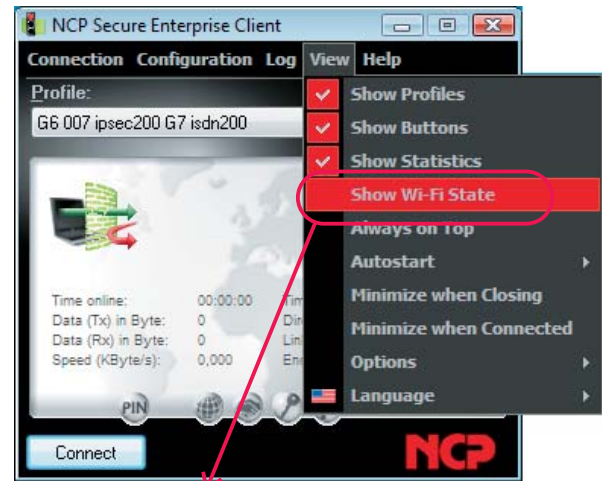
Once the Wi-Fi adapter is ready to operate, start the client monitor. The Wi-Fi menu item is located in the configuration menu. If you select this menu item, you can enable the NCP Wi-Fi tool by checking “enable Wi-Fi configuration” (Illustration below).



This management tool is displayed as tray icon (Illustration below to the right). It can be used in exactly the same way as common management tools which are supplied with the Wi-Fi adapter. It has, however, additional features especially in connection with the Enterprise Client.



If you use the **NCP Wi-Fi Tool** it is advisable to deactivate or remove a competing Wi-Fi tool via the services administration.



Instead of the tray icon, the **Wi-Fi State** can also be displayed in the view menu of the Client Monitor (Illustration above). Clicking on the Wi-Fi button opens the Wi-Fi settings (Illustration to the left in the middle).

Wi-Fi Connection and Wi-Fi Profile

The client can establish a radio network connection to an access point independently of the VPN connection in a link profile if a Wi-Fi profile has been created for a particular radio network. This Wi-Fi profile is used to automatically establish the radio network connection in the background if you are establishing a VPN connection to the company network and the Wi-Fi communication medium has been configured in the VPN profile being used. (Multiple Wi-Fi profiles can be configured in the Wi-Fi settings in such a way that the appropriate one is selected in each case via a **Wi-Fi Automation** for the radio network concerned. See below.)



Please note that you require the access data of the Wi-Fi access point and of your network operator's Hotspot.:

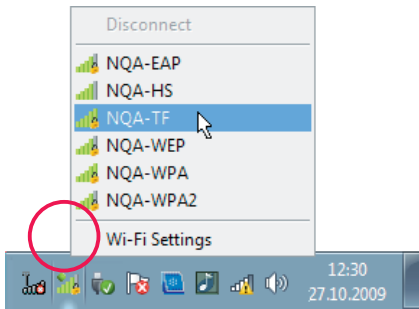
- SSID (Service Set Identifier)
- Encryption and Key
(Hotspot usually unencrypted)
- User ID, Password (for Hotspot Login)

Connection to the Wi-Fi Access Point and Wi-Fi Profile



This section describes how a connection to a Wi-Fi access point is established - if this is not yet possible - and how a Wi-Fi profile, featuring all access data to the radio network, is created with the client's internal Wi-Fi tool.

A click on the tray icon shows a list of the SSIDs of the available wireless networks (Illustration to the left).



Placed in front of the SSIDs, the color spectrum icons, ranging from grey to green, show the signal strength of the networks. The color grey is used for wireless networks with too little signal strength. The color green is used for wireless networks to which a Wi-Fi connection can be easily established. If a Wi-Fi connection is to be established, simply click on the SSID in the tray icon.



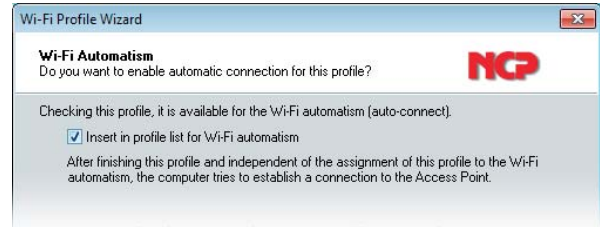
The connection to the access point is established immediately and displayed in the state display of the tray icon (Illustration to the left) if a Wi-Fi profile has already been created for this SSID.

Assistant for Wi-Fi Profiles

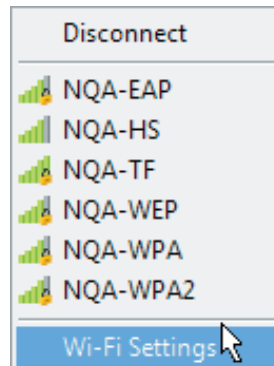
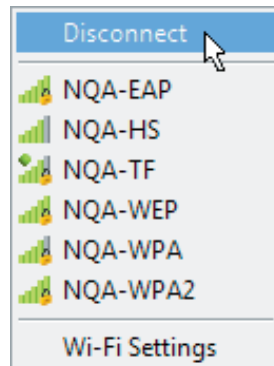
If no Wi-Fi profile for the SSID has been created yet, for example after the first installation of the client, a profile is created with the help of the Wi-Fi profile wizard in two steps only.

In the first step of the creation of a Wi-Fi profile, the Wi-Fi profile wizard only requests the security key, which you received from the access point administration.

In the second step of the wizard you have the possibility to place this Wi-Fi profile in a priority list for a Wi-Fi Automatism which can be configured later on (Illustration above to the right). After clicking on finish and independent of the assignment to the Wi-Fi automatism, the compu-

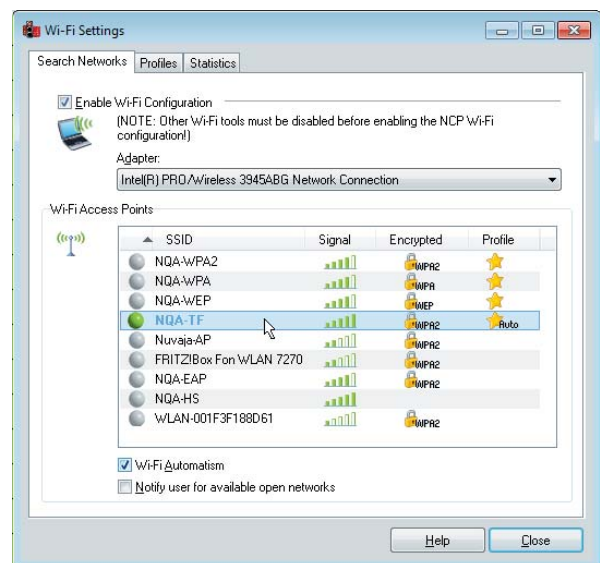


ter immediately tries to establish a connection to the Wi-Fi access point.



After a connection to the access point has been established, a click on the menu item "disconnect" (in the list of SSIDs) disconnects the Wi-Fi connection (Illustration to the left).

A click on "Wi-Fi configuration" (Illustration to the left) opens the Wi-Fi settings which can be used by the client for setting up a VNP connection. In this menu the SSIDs of the scanned wireless networks and their respective signal strength and encryption type is displayed. Furthermore, a star behind the network name displays an already existing Wi-Fi profile, while a star with "Auto" written on it displays whether this Wi-Fi profile has been assigned to Wi-Fi automatism (Illustration below).



Clicking on a selected profile establishes or disconnects a connection to this access point.

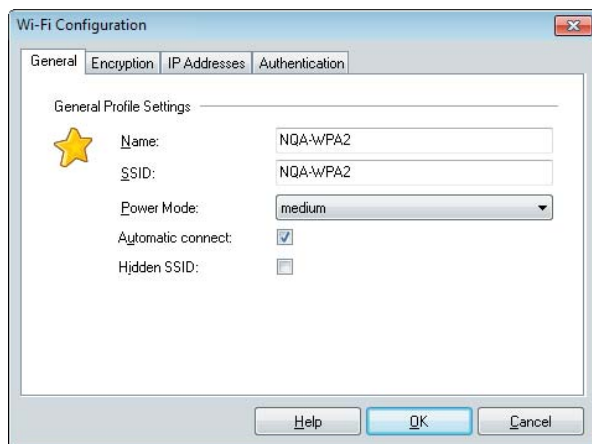
Wi-Fi Profiles

All access data are stored in the Wi-Fi profile and with that it defines how a radio network connection between client and access point or hotspot is established. Several profiles can be set for each radio network. The Wi-Fi configuration window can be opened via the tray icon or via the configuration menu of the monitor by clicking on “Wi-Fi”.

The Wi-Fi configuration has four configuration windows for the settings for the Wi-Fi profiles:

- General Profile Settings
- Encryption
- IP Addresses
- Authentication

General Profile Settings



SSID

When a new profile is being created, the **SSID** is, after double-clicking the network to be selected (Example: *NQA-WPA2*), automatically copied to the Wi-Fi profile as a **Name** and **SSID** if no profile has yet been created for this network.

Name

The name may be changed as you wish, but the SSID must match that of the network scanned.

Energy Mode

Wherever the Wi-Fi adapter permits, the energy mode can be selected for it.

Auto-Connect

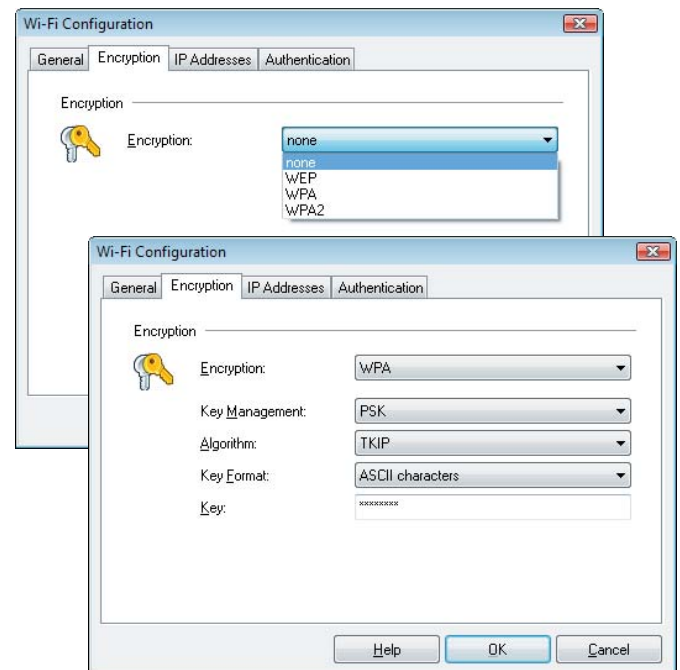
If the feature “auto-connect” is activated for this profile, it is listed in the Wi-Fi automatism profile list and selected if needed. See below: **Wi-Fi Automatism**.

Hidden SSID

Hidden networks are being displayed without SSID. I.e. they cannot be selected in the list of SSIDs for a connection to the access point.

If your Wi-Fi network is configured as hidden network activate this function and name the profile to be configured. This name can later be used as selection criteria for network search.

Encryption



The encryption mechanism must match that of the Wi-Fi router at the access point and the system administrator will issue it to you. The default setting is “none”. You can select **WEP**, **WPA** and **WPA2** with the according algorithms and key formats.



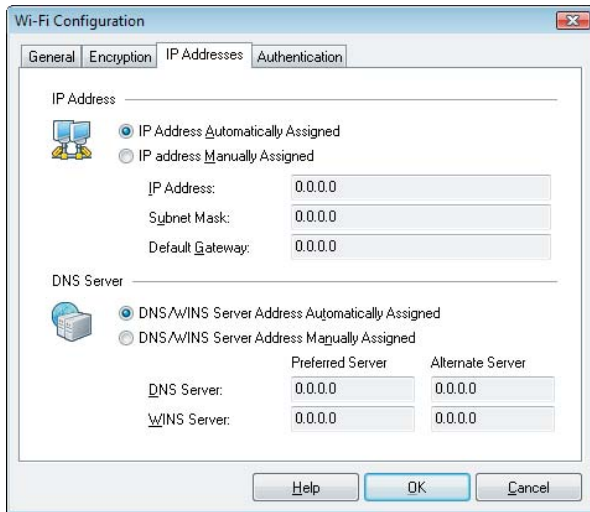
Note: Using WPA2 under Window XP a patch from Microsoft has to be downloaded.



If WPA with EAP (TLS) is used, the **EAP Options** in the monitor’s configuration menu must be activated and a certificate must be configured. In this respect, note the **Certificate Configuration** PDF file.

IP Addresses

The settings made here for the Wi-Fi adapter's IP address configuration take effect if the Wi-Fi configuration has been activated as described above. The default setting is the automatic mode using a DHCP server.



The configuration entered here is copied to the Microsoft configuration for the network connections. (See there Network connections / Internet protocol properties (TCP/IP)).

DNS Server

The addresses for DNS / WINS Server are, by default, automatically drawn from a DHCP server. A DNS / WINS server can, if necessary, use the Wi-Fi adapter for resolving the name of the VPN gateway.

Authentication



The access details for logging into a Hotspot can be entered in this window. These user details are only used for this Wi-Fi profile.

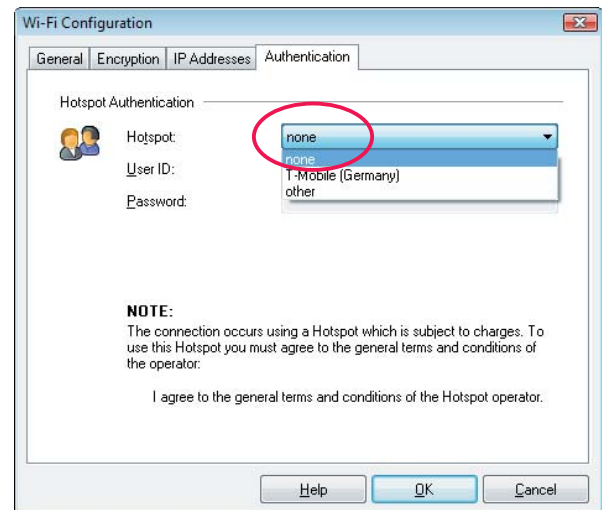
No Authentication at the Hotspot

If the connection to the company's own access point in the local area radio network is to be established without a Hotspot, select *none* Hotspot Authentication. (Illustration below)

You choose *no* Hotspot Authentication if the Hotspot operator does not support script-controlled authentication.



In this case, the provider's login screen for entering the user name and password will appear in the browser when the connection is established. Access to the Hotspot and the Hotspot operator's billing procedure uses this identifier. (See below **Hotspot Logon**).



Hotspot Authentication



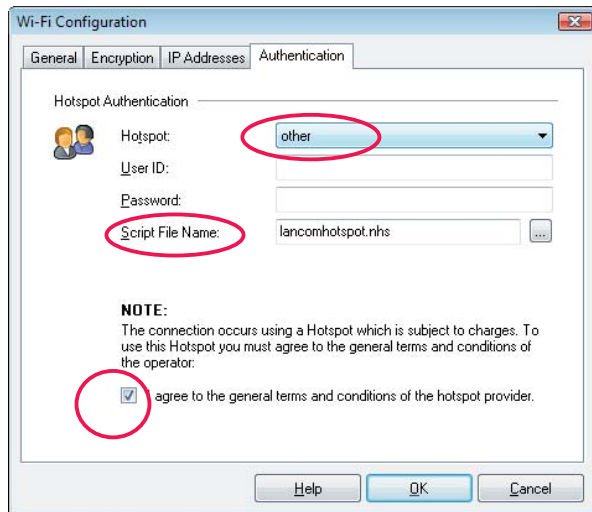
Please note that, for authentication at the Hotspot, you need to agree to the Hotspot operator's business terms before the profile can be saved and the connection established. (Illustration next page)

Authentication with a Script

The script automates the login with the Hotspot operator, since the logging in is done, controlled by a script, in the background, without using a browser.

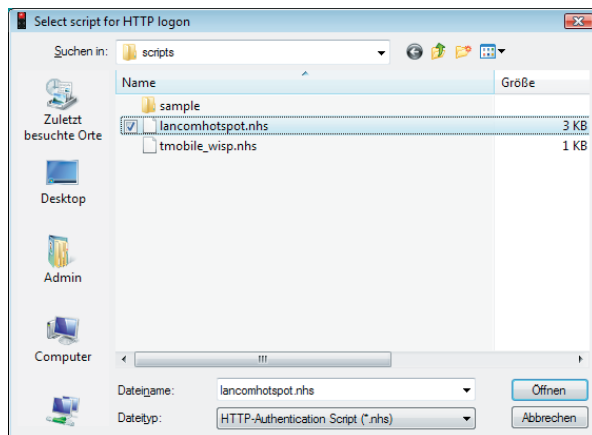
Other

You select “other” if you are using a different Hotspot, *not specifically listed*, for the script-controlled login. (*T-Mobile, e.g., is specifically named.*) (Illustration below)



Script File Name

Script file names can be displayed for selection with other Hotspot operators. You select the appropriate script for your Hotspot from this list*. (Illustration below)

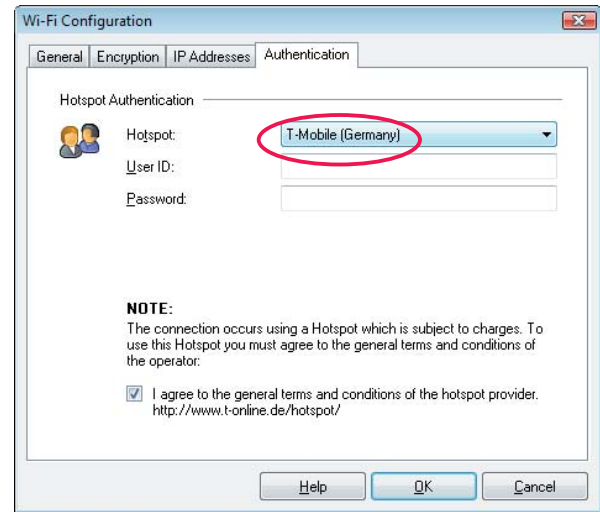


User ID / Password

The user ID and password are entered in line with the provider's guidelines.

T-Mobile

The T-Mobile Hotspot can be selected for logging in using WISPr technology. A script name need not necessarily be selected. The corresponding script is automatically loaded in the background. (Illustration below)



User ID / Password

Now you just need to enter the user ID and password in line with the provider's guidelines.

WISPr Login



The NCP Secure Client supports the new Hotspot login technology via the WISPr (Wireless Internet Service Provider roaming) protocol. This ensures compatibility with T-Mobile Hotspots in Germany, Austria, the Netherlands, the Czech Republic and Great Britain, as well as in Lufthansa lounges in certain international airports.

The WISPr login is done, script-controlled, without a browser with VPN tunneling. The script is automatically loaded in the background for the Hotspot operators *specifically named* (e.g. T-Mobile).



You create a Wi-Fi profile with default settings. I.e. the encryption remains switched off and the IP addresses are assigned automatically.

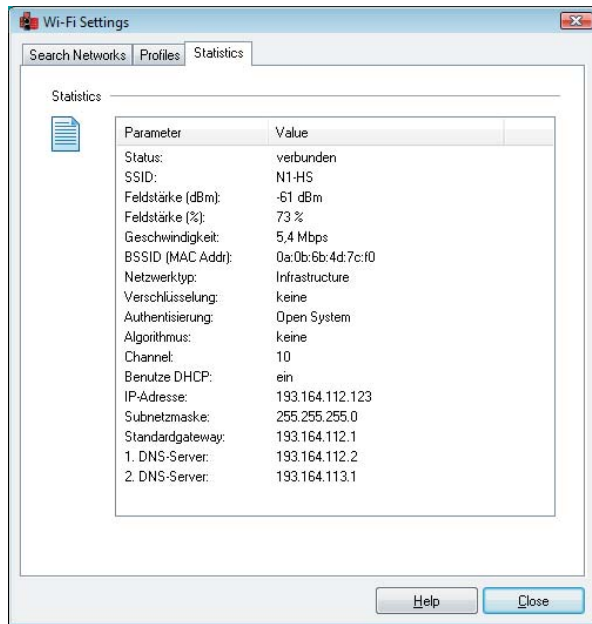
In the configuration field for authentication, you select a *specifically named* Hotspot operator from the list. There you will find T-Mobile (see above) and Other. NCP are constantly updating this list of WISPr-capable Hotspot operators.

With **others**, not listed here, the script-controlled, browserless login is done in a different way. (See Script file name, above).

* (NCP produces scripts upon request. A script is imported into the installation directory under <scripts>.)

Statistics

The Statistics window in the Wi-Fi settings shows, in clear text, the status of the connection to the access point. (Illustration below)



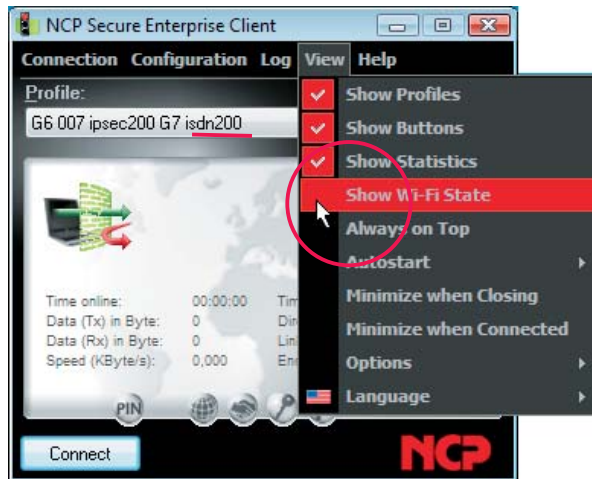
The statistics supplement the graphic display on the monitor with additional data such as the IP address of the Wi-Fi adapter and the DHCP setting.

VPN Connection and Wi-Fi State



After configuring a Wi-Fi profile and a link profile with the Wi-Fi communication medium, a VPN connection can be established via the access point.

When you select the corresponding profile in the monitor, the Wi-Fi profile for the radio network route that has been selected in the Wi-Fi settings is deployed automatically in the background. (See above **Wi-Fi Automatism**)



Whether the access point can be reached can be read in the tray icon or in the Wi-Fi state information field.

This field is enabled via the monitor's view menu under Wi-Fi status (Illustration above) or it is automatically inserted if a profile with Wi-Fi has been selected for a VPN connection.. (See also **Enterprise Client Monitor**)



If the field strength is insufficient or if no SSID appears, open the Wi-Fi settings in order to choose a different profile or create a new profile.

(The Wi-Fi state and the Wi-Fi configuration can also be opened independently of the VPN profile selected.)

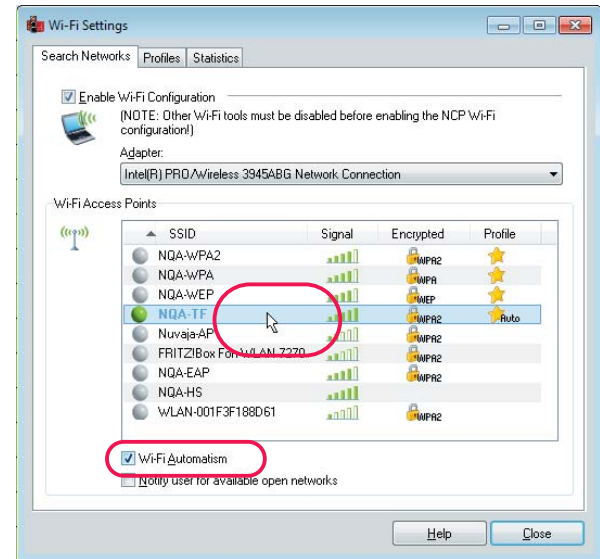
If the connection to an access point can be established via a selected Wi-Fi profile, the Wi-Fi status field must display the **SSID** and the **field strength** of the network. The Wi-Fi lettering appears in green.



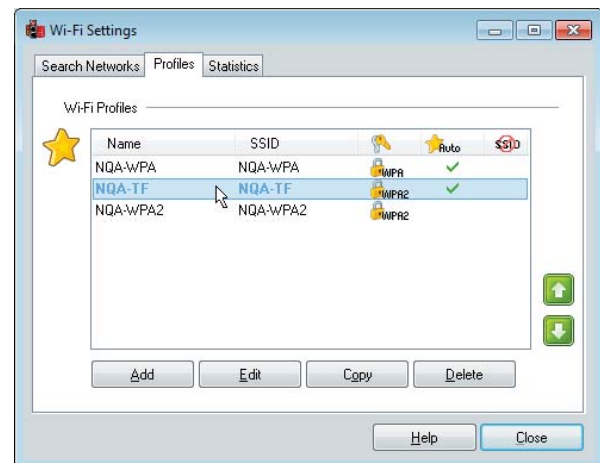
If *no connection* can be established to the access point, the field and the Wi-Fi lettering will remain grey and not display the field strength or SSID.

Wi-Fi Automatism

If the Wi-Fi automatism is activated (Illustration below) the connection to the respective access point is established, as soon as your notebook is within reach of the wireless network for which you created a profile with Wi-Fi automatism.



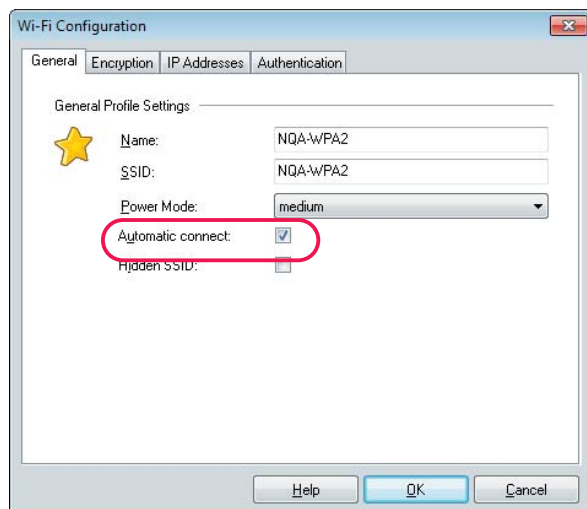
A double click on the line of the respective wireless network can disconnect or establish a connection to this access point.



In the "Profile" tab (Illustration above) all existing profiles are displayed in a priority list. The profiles with Wi-Fi automatism are marked with a check. The green arrows allow you to move the selected profile. The Wi-Fi automatism always works the list from top to bottom until it reaches a profile via which a connection to an access point can be established.

If a profile is to be assigned to the list of Wi-Fi automatism profiles, its configuration has to be

opened via double click or the edit button and auto-connect has to be checked (Illustration below).



Establishing the VPN Connection

The VPN connection can be established with a matching Wi-Fi profile via the access point.

In the monitor you select the profile for the VPN connection with the communication medium Wi-Fi and click on the connection switch. In the background, either, the last Wi-Fi profile you selected or one selected by the Wi-Fi automatism, will be drawn upon first to establish a connection (Illustration below).



Roaming with IPsec Connections

If the client is assigned a new IP address during a session with wireless LAN or LAN connection via DHCP, the client will take the new IP address and send an NCP-specific message to the gateway in order to communicate the change of address. While this is being done, the IPsec connection is not aborted and does not need to be re-established. On condition that: NCP Secure Server \geq 7.02 Build 25.

Secure Mobile Computing in Wi-Fi Networks and at Hotspots

The description in this section applies to both the hotspot logon with a script and via a logon page.



Any user with the appropriately equipped PC can access public hotspots. The individual themselves has to take data security precautions and protect their PC, because the hotspot operator takes no responsibility for this.

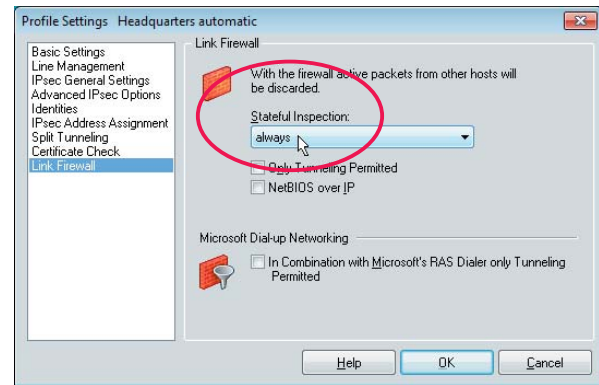
VPN tunneling and data encryption are used to protect confidentiality (data security). A personal firewall with "Stateful Packet Inspection" is required for the PC's security. Please refer to the right hand column.

The hotspot automatism in the client's personal firewall ensures that IP address assignment by DHCP is all that is permitted, other accesses to or from the Wi-Fi are prevented. The firewall dynamically approves the ports for http or https for logging into or off the hotspot as soon as the hotspot Logon menu item is clicked.

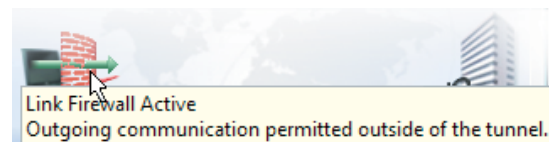
During this process, data traffic with the operator's hotspot server is all that is possible. In this way, a public Wi-Fi is used only for the VPN connection to the central data network. Direct Internet access is ruled out.

The client's hotspot logon currently only supports access points that work with the redirect of a query by browser on the login page of the public Wi-Fi operator (e.g. T-Mobile or Eurospot).

If the above conditions are met, a click on the **Hotspot Logon** menu item opens the website for logging in in the standard browser. After entering the access details, the VPN connection e.g. to the company head office, can be established and securely communicated.



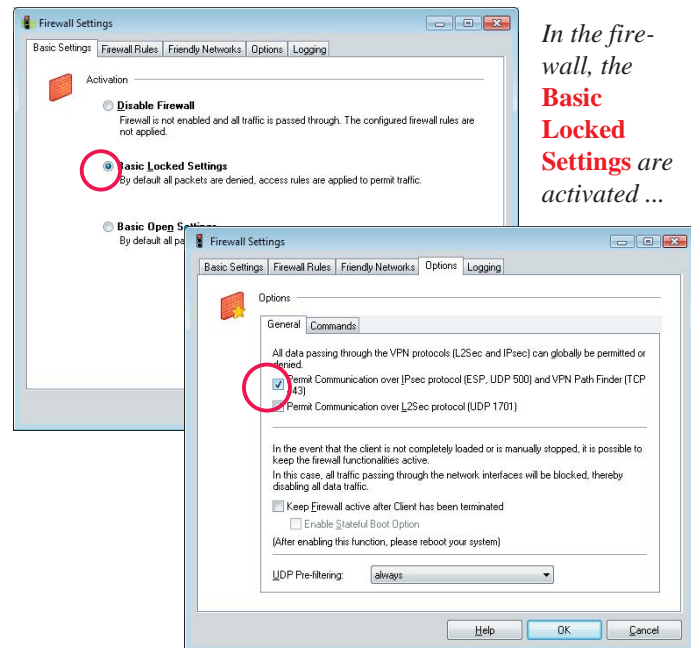
*Illustration, above: The client's **Link Firewall** should "always" be switched to stateful inspection. The stateful inspection security mechanisms work even if the client monitor has not been started up. The link firewall's function is illustrated by the **arrow symbols** in the monitor's graphic field. (See below)*



However, you should note that: If the option "Only Tunneling Permitted" is also activated, the hotspot logon page will no longer be accessible.



Logging in to the hotspot and the prevention of any direct Internet connection by bypassing the VPN tunnel is only made possible by the integrated personal firewall.



*In the fire-wall, the **Basic Locked Settings** are activated ...*



To configure other firewall rules, please refer to the description:



Personal Firewall



*... and, under **Options**, only the communication via the IPsec protocol and the VPN Path Finder is permitted.*

Automatic Hotspot Logon



The following section only describes a few variants of the hotspot logon. For further technical details, particularly configuring the integrated personal firewall, please refer to the documentation for **Personal Firewall** (Online Help).

Prerequisites

The computer has to be located in a hotspot's reception area and have an activated Wi-Fi card. The connection to the hotspot must be established and an IP address must be assigned for the Wi-Fi adapter.

As described above under **Configure Wi-Fi Profile**, you first scan the Wi-Fi networks. You recognise your hotspot operator from the SSID. For this SSID you create a Wi-Fi profile, no hotspot authentication needing to be set in the authentication configuration window. In the Wi-Fi settings statistics window you can see whether the Wi-Fi adapter has received an IP address.

Hotspot Configuration

Configuring for hotspot logon is done under "Hotspot" in the monitor's configuration menu.

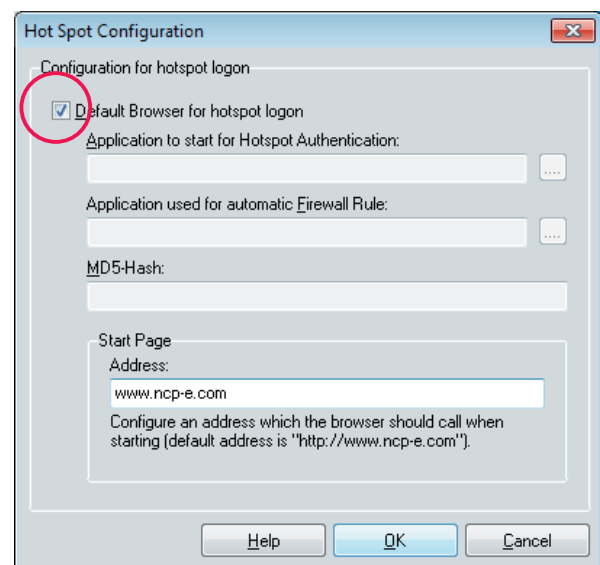


The following settings may be made:

Default Browser

"Default browser for hotspot logon" is the default setting. If unchecked, then a different browser or another application ("Application to start for Hotspot Authentication") can be specified. This is specified in the form:

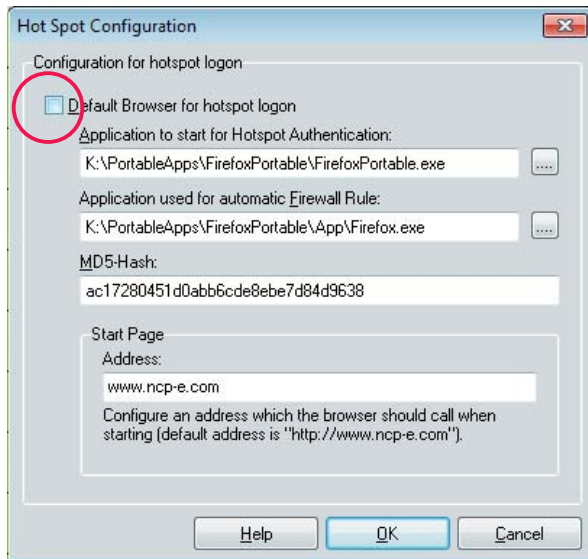
```
%PROGDIR%\Mozilla\Firefox\firefox.exe.
```



Application to start for Hotspot Authentication



This application features a special browser configuration, which is used for hotspot logon. For example, use this application in order to deactivate all active elements (Java, JavaScript and ActiveX) or a proxy server. Only afterwards, this application starts the browser.



Application used for automatic Firewall Rule

The firewall monitors this application. This means, you have to enter the application which is setting up outbound connections.

Example: If you use Portable Firefox, you have to enter “FirefoxPortable.exe”. The real browser, which is to be monitored, is stored in a Firefox subdirectory: ...\\App\\Firefox.exe



You may refrain from entering the application, which has to be monitored by the firewall, if the browser has no preceding starting procedure and the browser has been entered into the field: starting application for hotspot logon.

MD5 Hash

In addition the MD5 hash value of the browser exe file can be determined and entered in the “MD5 Hash” field. In this manner the system ensures that a hotspot connection is only realized with this browser.

Start Page

Under “Start Page / Address” the start page described above is entered in the form:
<http://www.mycompany.com>

Hotspot Logon

The hotspot logon is done via the menu item of the same name in the Connection menu on the monitor.



When this menu item is clicked (Illustration above), 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:

“You are already connected to the Internet. hotspot logon is not necessary or has already been executed.”

The administrator can replace this text by specifying the address of a different HTML page 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 cannot access a website**, because the hotspot cannot be reached, the Wi-Fi 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.