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.

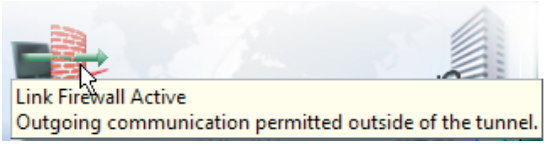
The hotspot automatism in the client's personal firewall ensures that IP address assignment by DHCP is all that is permitted, other accesses to or from the Wi-Fi are prevented. The firewall dynamically approves the ports for http or https for logging into or off the hotspot as soon as the hotspot Logon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

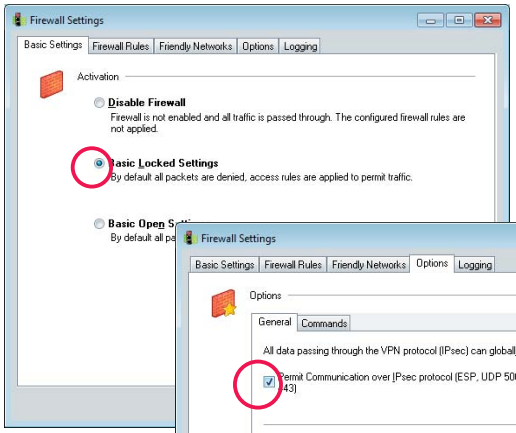
If the above conditions are met, a click on the **Hotspot Logon** menu item opens the website for logging in in the standard browser. After entering the access details, the VPN connection e.g. to the company head office, can be established and securely communicated.

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)*

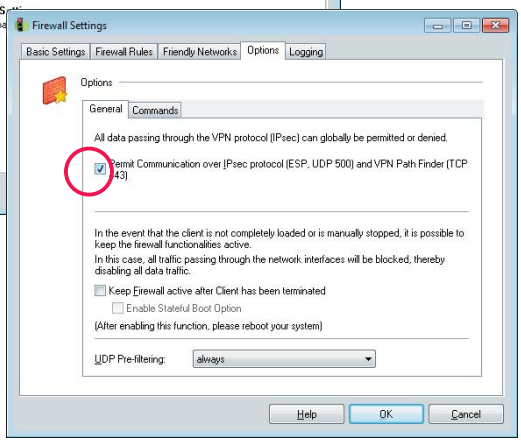


However, you should note that: If the option "Only Tunneling Permitted" is also activated, the hotspot logon page will no longer be accessible.

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 firewall, the **Basic Locked Settings** *are activated ...*



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

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

Personal Firewall

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).

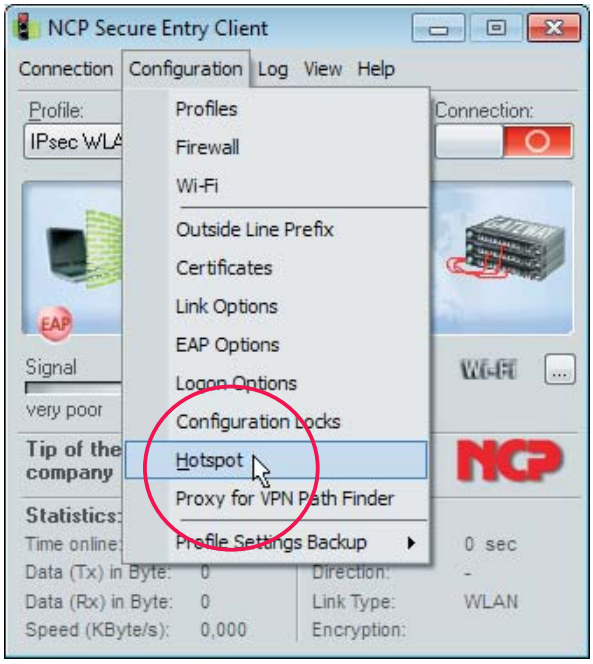
Prerequisites

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

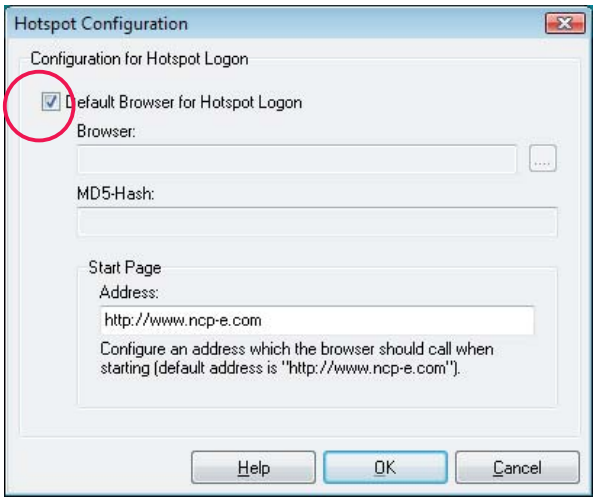
Configuring for hotspot logon is done under "Hotspot" in the monitor's configuration menu.



The following settings may be made:

Default Browser

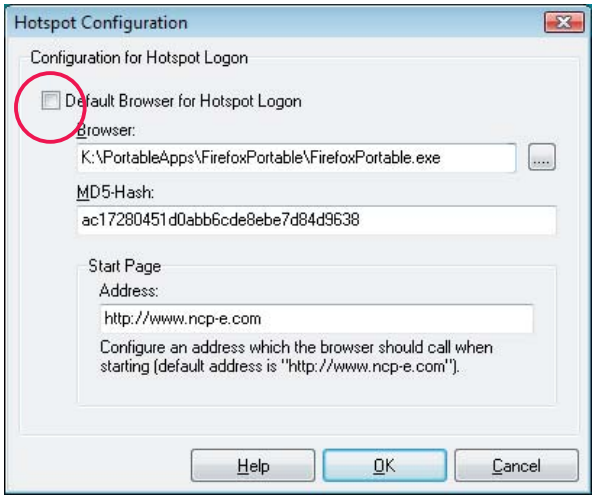
The basic setting is: **Default Browser for Hotspot Logon** (Illustration below). If the default browser has a configured proxy server, this may sometimes need to be deactivated. If the checkbox is unchekked, a different browser can be entered.



Alternative Browser

In order to enter an alternative browser uncheck the default browser checkbox. An alternative browser is entered as follows:

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



The alternative browser is not included in the client software and has to be installed by the administrator or the user.

The alternative browser can be configured specifically for the hotspot requirements. I.e. if a proxy server is not configured, all the active elements (Java, Javascript, ActiveX) are deactivated and the address bar is hidden. Thus this browser can only be used for logging into the hotspot.

The MD5 Hash value of the browser's Exe file is also ascertained and entered in the "MD5 Hash" field (Illustration above). This ensures that a this browser cannot be exchanged or altered.

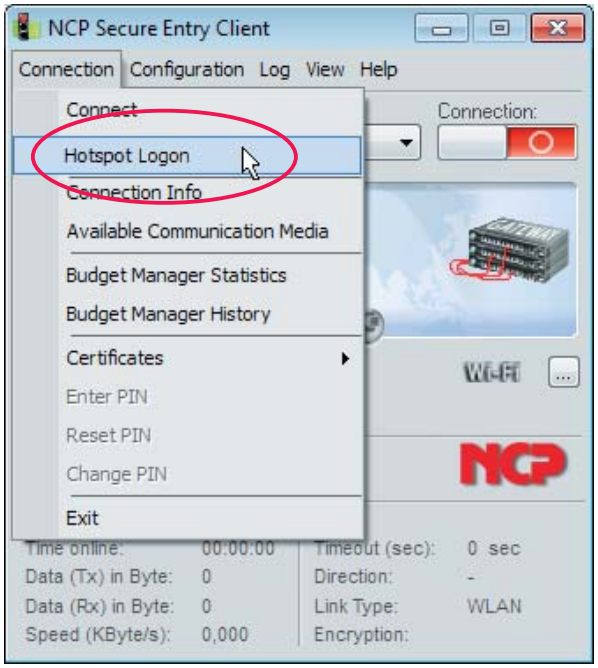
Homepage

The hotspot operator's logon page is entered as the homepage, either as an IP address or in the form:

```
http://www.mycompany.de
```

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.