

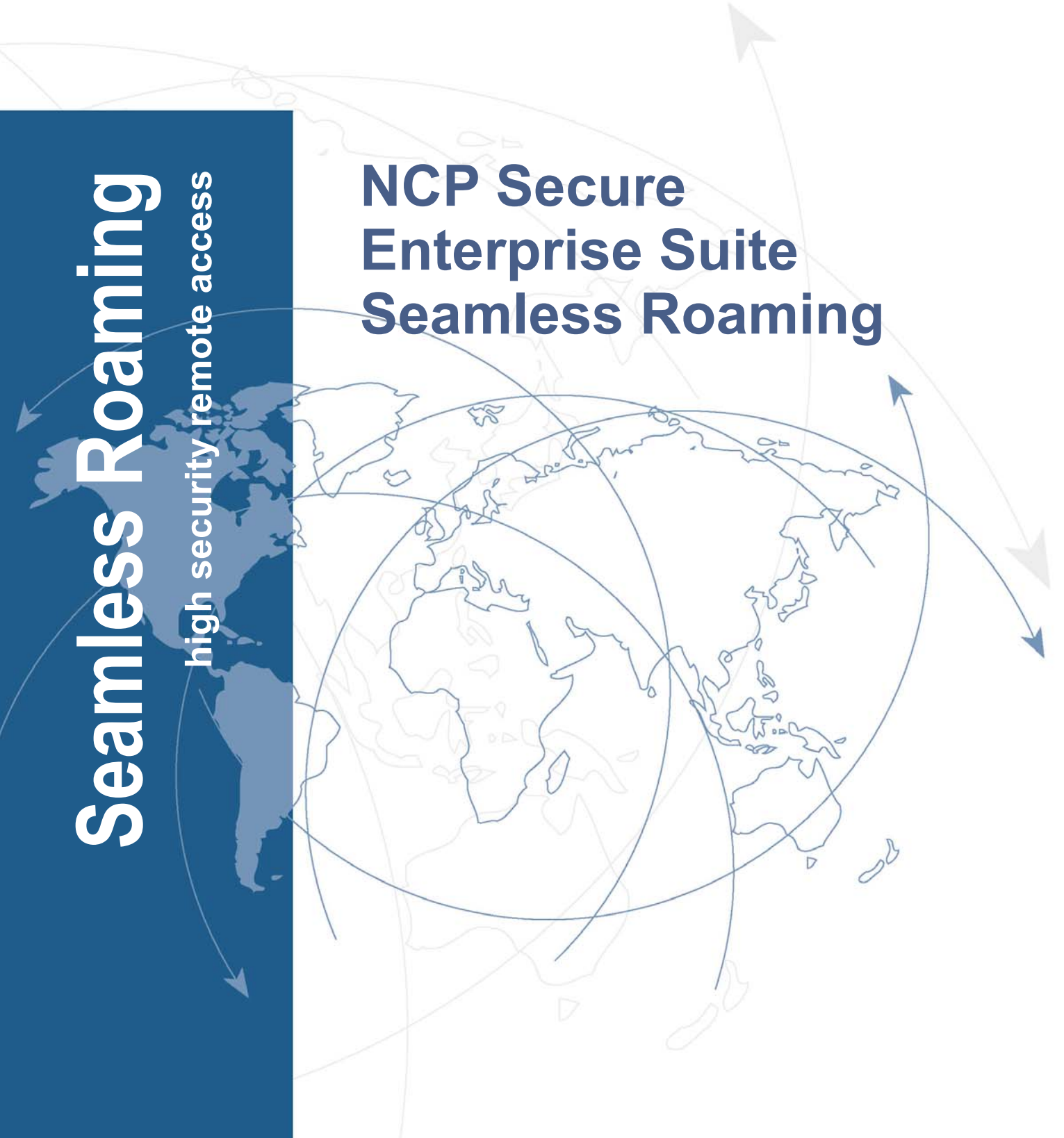


SECURE COMMUNICATIONS

Seamless Roaming

high security remote access

NCP Secure Enterprise Suite Seamless Roaming





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, March 2012

Seamless Roaming Functionality and Configuration



The first section of this manual describes the components associated with Seamless Roaming and how Seamless Roaming works.

The second section describes the configuration options.



This manual forms part of the **Enterprise Client Navigation** series. This pdf file contains links to all manuals currently available for your product; however, the full navigation capabilities can only be used when all manuals are stored together in a single directory.

Further information about the products underlying Seamless Roaming is described in the following manuals:

Contents

- Seamless Roaming Functionality
- Technical Overview
- Default settings for Seamless Roaming
- Visual Feedback
- Maintain wireless connections in Expert Mode
- Switching off the default Behavior
- Application example
- Configuration example
- Profile Settings for Automatic Media Detection and Seamless Roaming



– the **Enterprise Client Parameter** manual includes an overview of configuration modes and all configuration parameters,



– configuration and use of a **mobile wireless card** (3G / 4G) with the corresponding communication medium are described in the **Mobile Computing** manual, and



– configuration and use of **Wi-Fi profiles**, **Wi-Fi automation** and secure **Mobile Computing in wireless LANs** and hotspots is also described in the **Mobile Computing** manual.

Seamless Roaming Functionality

Prerequisites for Seamless Roaming are an NCP Secure Enterprise Client (from version 9.30 build 102) and, at the central Virtual Private Network (VPN) gateway, an NCP Secure Enterprise VPN Server (from version 8.05 build 87).

A core problem in systems designed to support remote access, to a corporate network, from Microsoft Windows based laptops, is catering for the frequent changes in communication medium: a wireless LAN at the airport, a 3G mobile wireless connection during the drive to the hotel and a LAN in the corporate offices.

The NCP solution guarantees that when using the centrally managed NCP Secure Enterprise Client for MS Windows 32/64 bit operating systems, there is a smooth changeover when moving between networks, without any reduction/shortfall in security.

During a session, the Secure Client automatically changes the communication medium (LAN, WLAN, 3G / 4G) when necessary and dynamically diverts the VPN tunnel accordingly. In parallel, the Client also guarantees “location awareness”: the automatic detection / recognition of secure or unsecure networks.

There are three sets of technology (communication medium) available, over which a secure VPN tunnel can be established to a corporate network: the traditional wired Ethernet LAN; the wireless Ethernet LAN (Wi-Fi / WLAN) used in public hotspots, hotels or companies; and mobile wireless networks (GSM / GPRS / UMTS / 3G). Various technologies must be supported in the mobile wireless arena: from GSM networks to 3G connections to high speed connections via 4G networks (Long Term Evolution - LTE).

Although this variety is in itself an advantage, the flexibility to use any available medium is only an advantage if the user is not fixed to one type of communication medium for the whole duration of a VPN tunnel connection. In order to fulfill this flexibility requirement, the NCP remote access solution supports the following features:

- automatic changeover of communication medium
- when changing to another medium, dynamic rerouting of the VPN tunnel to that new medium, and
- preservation of the logical VPN connection and any application sessions using that VPN tunnel

Technical Overview

Seamless Roaming represents the smooth changeover between the underlying heterogeneous Internet communication media while preserving the established VPN tunnel. The IP address of the tunnel endpoint remains unchanged, meaning that applications communicating over the VPN tunnel are not disturbed during that changeover.

The NCP Secure Client automatically changes the communication medium (LAN, WLAN, 3G / 4G) when necessary, and dynamically diverts the VPN tunnel accordingly. In doing so, the Client also guarantees “location awareness”: the automatic detection / recognition of secure and unsecure networks.

The seamless changeover of the underlying physical medium provides an “always-on” function that prevents an application session being broken; regardless of whether due to a fault or break in the connection or a changeover to another physical communication medium, Seamless Roaming ensures that all active application sessions remain intact, independent of changes to the underlying physical medium. An automatic rekeying is negotiated between Client and VPN gateway whenever there is a changeover in the underlying communication medium.

Default Settings for Seamless Roaming and Visual Feedback



Whenever an error or break occurs in the physical communication medium, the logical VPN tunnel connection is preserved. The physical communication medium to be used in replacement is selected on a priority basis: LAN, WLAN, GPRS / UMTS (3G).

The speed of the communication media available is also considered during the selection process, meaning that the LAN is usually selected first, if available, followed by WLAN or GPRS / UMTS. This represents the **default behavior** of the NCP Secure Client.

If, after a VPN tunnel has been successfully established, the communication medium becomes unavailable, the NCP Secure Client waits for the availability of a suitable alternative communication medium (LAN, WLAN or GPRS / UMTS). During this waiting period, the logical connection is preserved. This “waiting” is signaled to the user via the Client monitor: the solid green bar representing an established VPN connection changes to a dashed green bar and icon in the system tray flashes yellow and green. When the physical connection is re-established, the VPN bar and the system tray icon change back to solid green.

When the physical connection is re-established, the VPN bar and the system tray icon change back to solid green.



Dependent on which communication medium is selected, the Client monitor displays the **3G or Wi-Fi panel**, regardless of whether the **Wi-Fi status** display has been activated in the Client monitor's “View” menu.



Only after terminating the Client monitor after a security password prompt, or when the connection is manually closed (disconnect button) or when another profile is manually selected, does an orderly **disconnection** of the logical connection (including the disconnection of the physical connection) take place. **Timeout settings** (in the profile configuration under “Line Management”) or **DPD Interval** settings (in the profile configuration under “Advanced IPsec Options”) are ignored when Seamless Roaming is being used.

fig. top: logical connection (VPN tunnel) is preserved after the LAN cable has been pulled out.

fig. middle: connection is re-established via Wi-Fi, Wi-Fi panel is switched on.

fig. bottom: connection is re-established via GPRS / UMTS, 3G panel is switched on.

Application Example

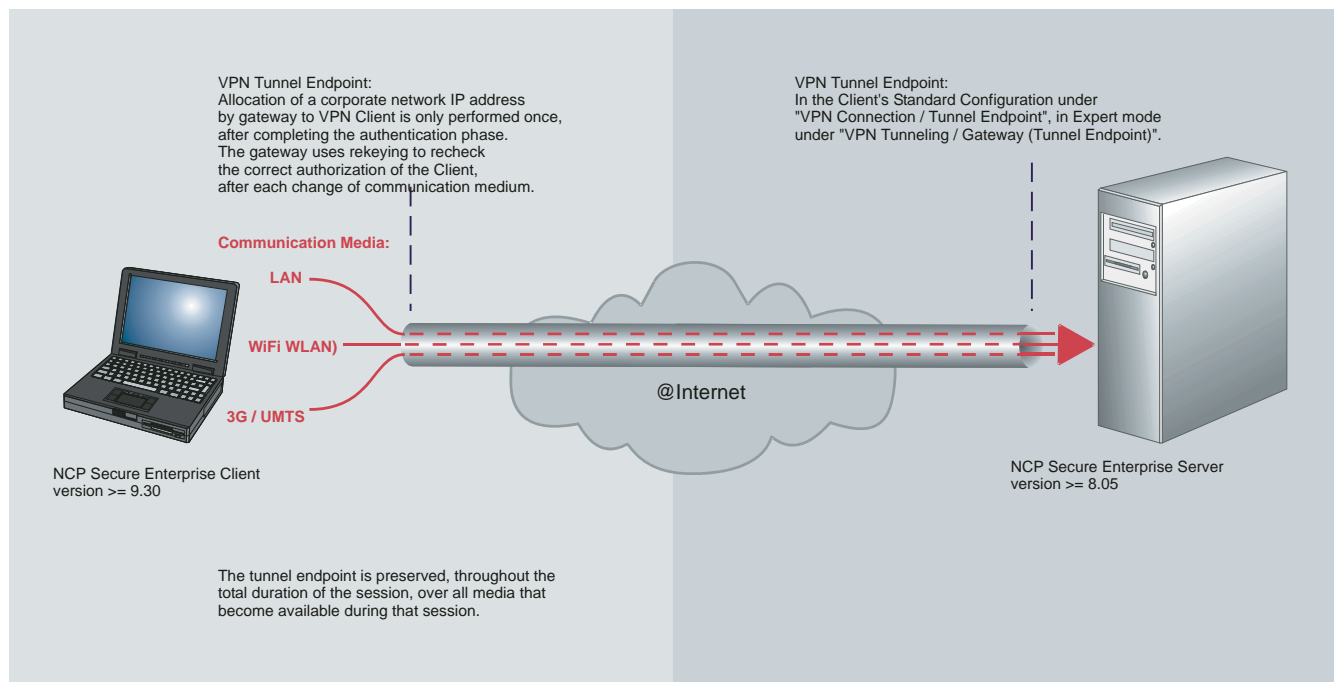
When a laptop is docked in a docking station the communication is automatically switched from the previously used wireless connection (WLAN or GPRS / UMTS) to LAN. When the switchover takes place, the VPN tunnel endpoint IP address is preserved and applications currently communicating over the VPN tunnel are left undisturbed.

If the cable connection to the LAN is broken, due, for example, to the laptop being undocked, the VPN Client automatically establishes a connection to the corporate network via the next available medium, for example, over the wireless LAN. The VPN tunnel remains undisturbed during the switchover.

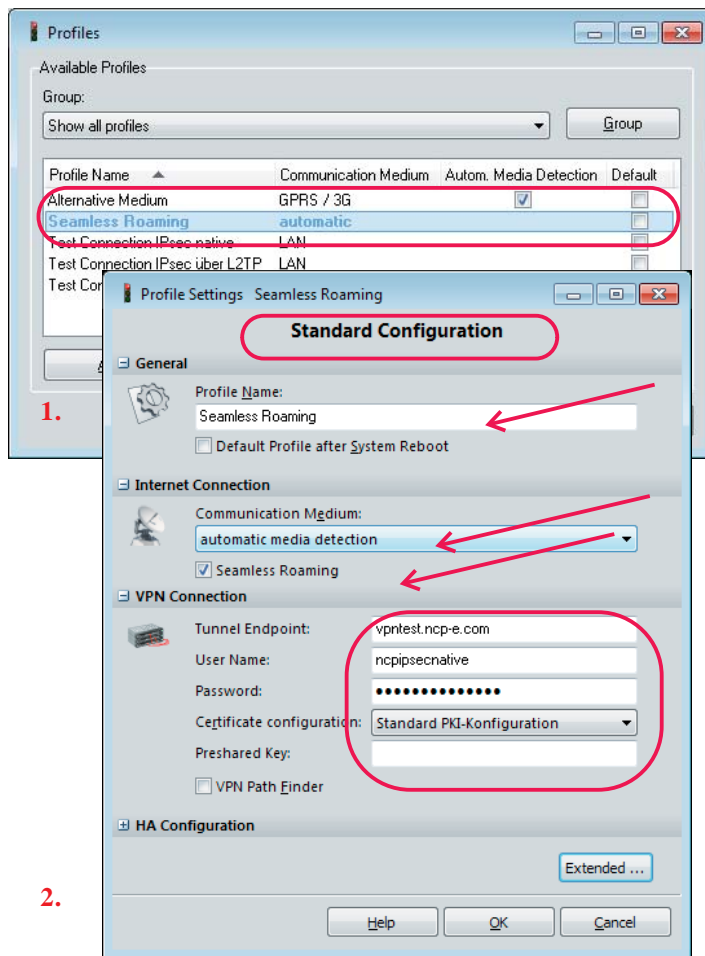
If the teleworker takes the laptop out of range of the wireless LAN and the Wi-Fi signal is lost, the VPN Client automatically switches to the 3G /4G medium.

Again, the switchover to another communication medium does not disturb the VPN tunnel and there is no session loss.

This process of selecting an alternative medium is repeated until all available media have been tried without successfully establishing the associated physical connection.



Configuration Example

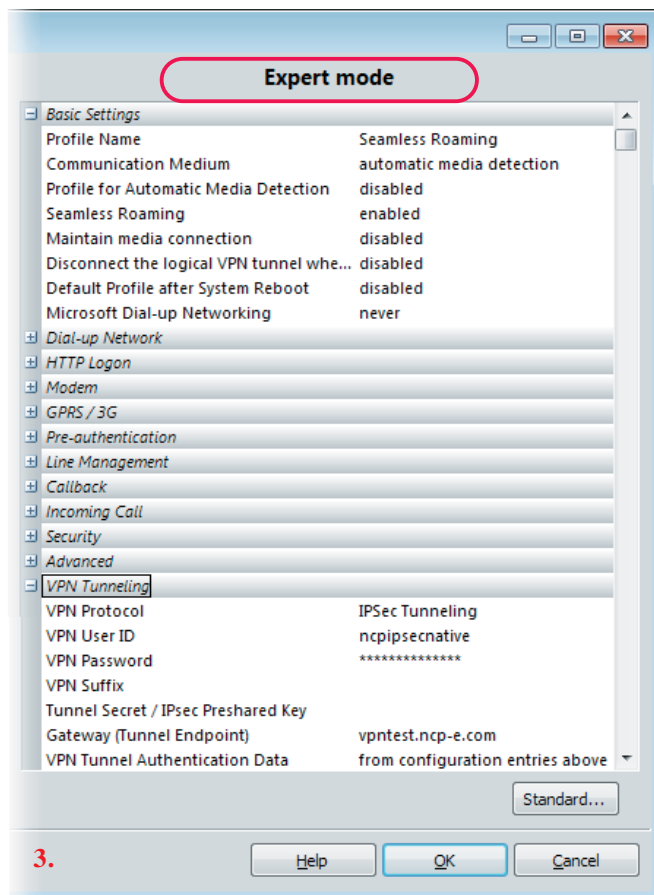


Seamless Roaming requires a total of three profile configurations. The two VPN profiles are created using the “Profile” configuration menu, the Wi-Fi profile via the “Wi-Fi” configuration menu.

In this example the VPN profiles are named “Seamless Roaming” and “Alternative Medium” (fig. 1. left)

Using Standard Configuration mode, select “automatic media detection” as the Internet Connection for the first profile, “Seamless Roaming”; the “Seamless Roaming” function can only be activated if this is done as a first step.

Enter the access data for the VPN connection to the gateway (fig. 2 left).



When in "Expert mode", the corresponding configuration parameters are listed under "Basic Settings" and "VPN Tunneling".(fig. 3 left)

Use of the communication medium “automatic media detection” means that this profile is configured as if it had LAN or Wi-Fi media. Activating the “Seamless Roaming” function ensures that the fastest available medium will be selected. (In order to use Wi-Fi for Seamless Roaming, a Wi-Fi profile must be available, see below).

1.

Standard Configuration

General

Profile Name: Alternative Medium

☐ Default Profile after System Reboot

Internet Connection

Communication Medium: GPRS / UMTS

☒ Profile for Automatic Media Detection

VPN Connection

Tunnel Endpoint:

User Name:

Password:

Certificate configuration: Standard PKI-Konfiguration

Extended Configuration

3G Configuration

Configuration mode: Provider list

Country: Germany

Provider: T-Mobile D (Germany)

APN:

Dial-up number:

User:

Password:

SIM PIN:

Standard...

Help OK Cancel

The second VPN profile is used for the Internet connection when neither LAN nor Wi-Fi communication media are available. In this profiles, named "Alternative Medium" in this example, select "GPRS / UMTS" as the Communication Medium for Internet Connection.

In addition set this as a "Profile for Automatic Media Detection" (fig.1. left)

Use "Extended Mode" to enter the ISP access data in the 3G Configuration folder in the Extended Configuration. (fig. 2. left)

(Refer to **Mobile Computing**)

2.

Expert mode

Basic Settings

Profile Name	Alternative Medium
Communication Medium	GPRS / UMTS
Profile for Automatic Media Detection	enabled
Seamless Roaming	disabled
Maintain media connection	disabled
Disconnect the logical VPN tunnel w...	disabled
Default Profile after System Reboot	disabled
Microsoft Dial-up Networking	never

Dial-up Network

HTTP Logon

Modem

GPRS / 3G

Configuration mode	Provider list
Country	Germany
Provider	T-Mobile D (Germany)
User ID	
Password	
Dial-up number	
APN	
SIM PIN	

Pre-authentication

Line Management

Callback

Incoming Call

Security

Advanced

Standard...

Help OK Cancel

In Expert Mode these settings can be made in "Basic Settings" and "GPRS / 3G". (fig. 3. left)

The configuration system does not allow Seamless Roaming to be set in a profile with the setting "Profile for automatic media detection" - in this example the "Alternative Medium" profile.

3.

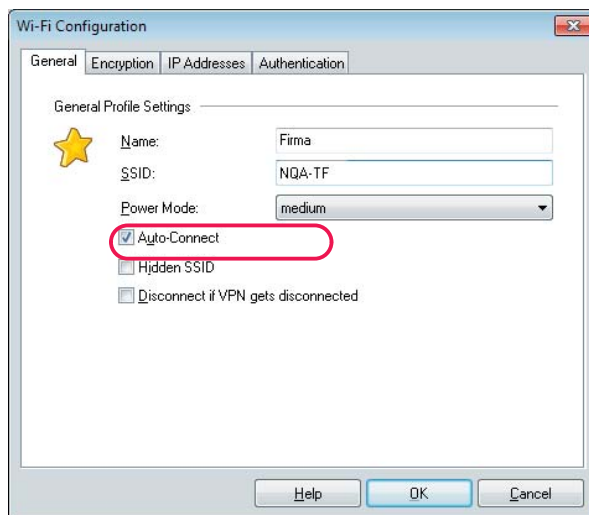
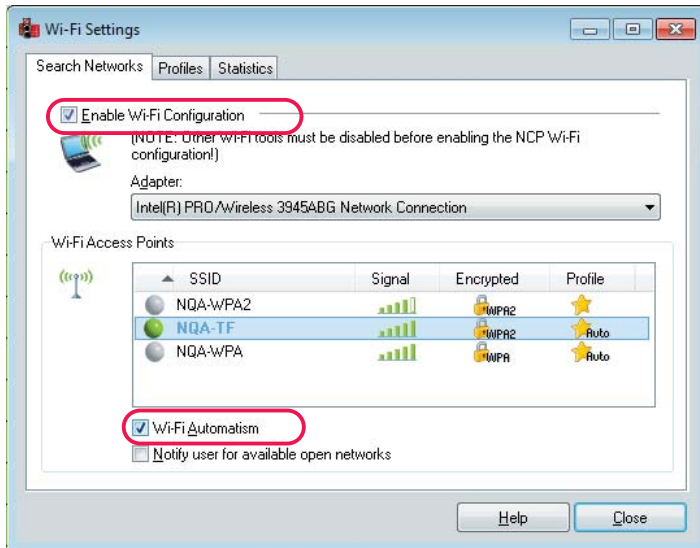


The Wi-Fi profile must be created as normal: enter all data required by the Wi-Fi access point, such as SSID, encryption, IP address settings and authentication. When using the NCP Wi-Fi tools, enable Wi-Fi configuration and Wi-Fi automation in the Wi-Fi Settings folder and “Auto connect” under the “General” tab of the Wi-Fi profile. (See the description in the **Mobile Computing** manual).

When using the NCP Wi-Fi tools, "Enable Wi-Fi Configuration" and "Wi-Fi Automatism" must be enabled in the "Wi-Fi Settings" (fig. 1 left), and "Auto-Connect" enabled in the Wi-Fi Profile Configuration under the "General" tab (fig. 2 left)

Multiple Wi-Fi profiles can be pre-configured and the appropriate one selected automatically using the Wi-Fi automation capability, when the LAN communication medium is not available and the laptop is located within range of the corresponding access point.

Existing Wi-Fi profiles are marked in the overview with a star, if “Auto-Connect” is set in the “General” tab then the word “Auto” is added to the star.



Maintain Mobile Wireless Connections with Seamless Roaming - in Expert Mode



The function **Maintain mobile wireless network connection with Seamless Roaming** optimizes the automatic changeover to the GPRS / UMTS communication medium.



The function ensures that the wireless connection via GPRS / UMTS to the Internet service provider is physically maintained even when, using Seamless Roaming, the VPN tunnel is temporarily switched to a faster medium such as LAN or Wi-Fi.

This function must only be activated in the configuration for the alternative medium GPRS / UMTS that is to be used by **automatic media detection** and over which the 3G connection will be established.



That has the effect of ensuring a faster switch back to 3G without loss of time, when the Wi-Fi is no longer available. Note however, that when both Wi-Fi and 3G adapters are activated simultaneously, this increases the power consumption.

It must also be remembered that, dependent on provider, excess fees could be incurred and that the in parallel to the VPN connection to the corporate network, an unprotected Internet connection could be open.

If the 3G connection loses reception, the logical connection will be preserved while the physical connection is being re-established. Any active application session is thus not broken.

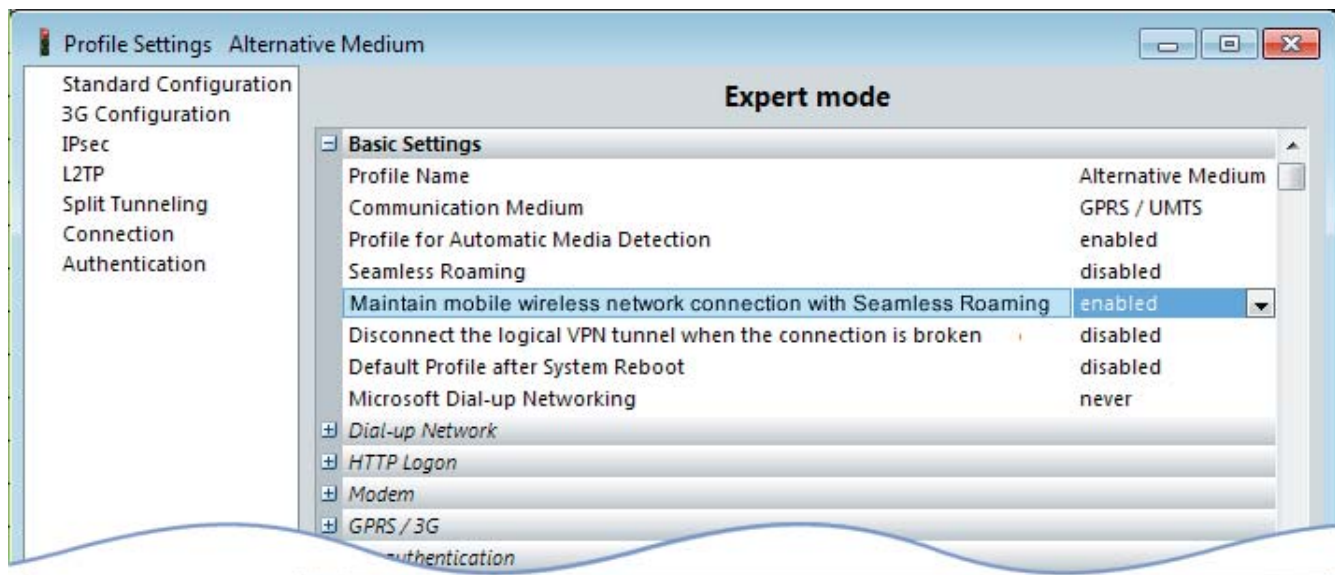


fig. above: GPRS / UMTS is the communication medium configured in the profile for automatic media detection (Alternative Medium) that will be used by Seamless Roaming and for which the mobile wireless connection will be maintained.

Switching off the Default Behavior



By selecting **Expert Mode** when configuring the Client profile, the Client's default behavior (maintain logical connection) can be switched off.

Enable the function **Disconnect the logical VPN tunnel when the connection is broken**.

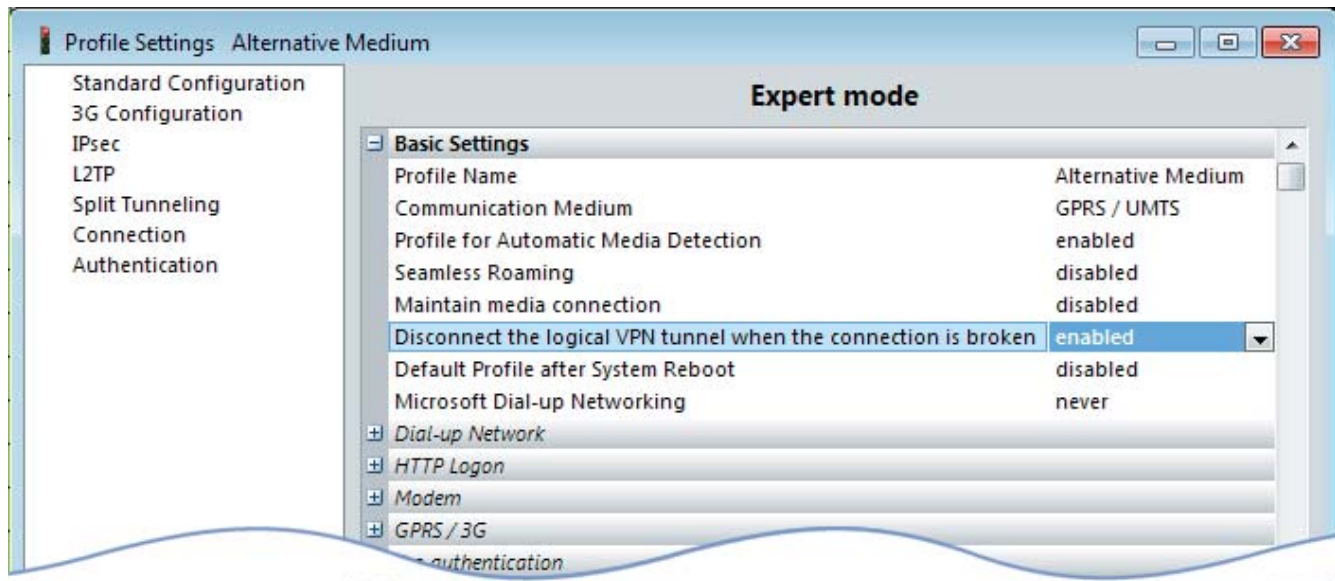


When this function is enabled (box ticked) and the physical connection is broken for whatever reason, the logical connection and any associated VPN tunnel are immediately disconnected.

Important



With Seamless Roaming, connection behavior is independent of this function; as soon as a connection is established using a profile that incorporates Seamless Roaming, the logical connection is preserved without breaks until that profile's connection is disconnected. Visually this is signaled with a **dashed green bar** in the Client monitor's GUI, as previously described.



Only when Seamless Roaming is not being used does the setting of the default behavior have an effect on the behavior of the logical connection. When the function **Disconnect the logical VPN tunnel when the connection is broken** is enabled and a connection, established using a profile without Seamless Roaming, is disconnected even for just a short time, the logical connection is immediately disconnected. The connection can then only be re-established by carrying out the procedure for **connection establishment**, including authorization. The disconnection of a logical connection is represented visually by the disappearance of the VPN bar in the monitor.



Profile Settings for Automatic Media Detection and Seamless Roaming



The overview of the “Available Profiles” lists in four columns the information about the connection profiles that have been configured so far. The column headings can be used to sort the profiles displayed and the checkboxes in the third and fourth columns allow the configurations to be rapidly altered when using Automatic Media Detection or a Standard Profile. The profiles do not need to be opened in order to change those two profile settings.



Only one profile can be selected for default use after a system reboot. When using Automatic Media Detection, this should be the profile which includes the VPN gateway access data and has the **Communication Medium** set to **Automatic Media Detection**. All other communication media can, if required, be marked **for use as** “Profile for Automatic Media Detection”.



When automatic media detection is to be combined with Seamless Roaming, the setting “Profile for Automatic Media Detection” can be safely turned off for all other communication media except GPRS / 3G. Note that Seamless Roaming only supports the communication media LAN, Wi-Fi and GPRS / 3G (only with broadband adapter).

(Refer to the example in the illustration below.)

Profile Name (1st Column)

For example the name of the Test Connection will be listed when a Test Connection profile has been created.

Communication Medium (2nd Column)

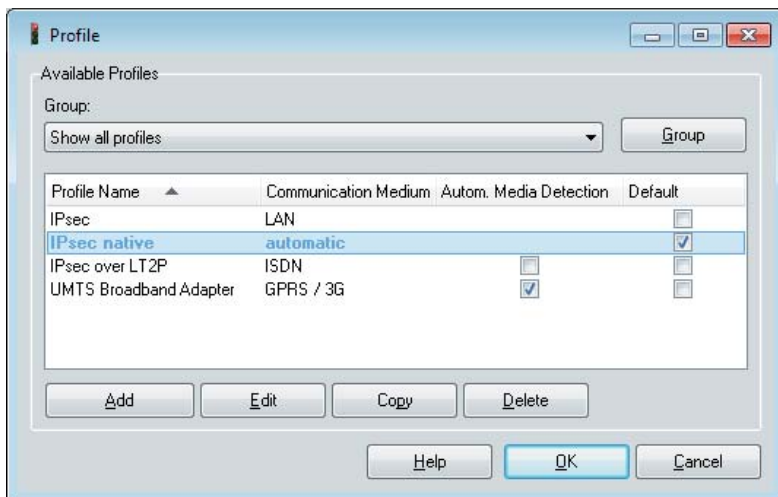
The communication medium selected is listed in the second column.

Automatic Media Detection (3rd Column)

If a LAN or Wi-Fi profile is configured with “Automatic Media Detection” communication medium to the VPN gateway, this will be labeled “automatic” in the second column of the profile overview. Other profiles configured with access data for an ISP (and with the communication medium xDSL, GPRS/3G, PPTP, ISDN or Modem options), can be set to “Automatic Media Detection” by a simple mouseclick in the third column. The tick here indicates that the “Profile for Automatic Media Detection” setting has been set in profile’s “Standard Configuration” settings (“Basic Settings” in Expert Mode). (See the configuration instructions for Automatic Media Detection).

Default (4th Column)

If an existing profile is activated with this checkbox, this profile will always be used for connection establishment after a system reboot. (See the configuration instructions **Default Profile after System Reboot**).



Configuring the Profile Settings

The buttons (Add, Edit etc.) under the profile list cannot be used if the associated locks have been set. If there are no restrictions on setting profiles then all buttons will be operable and will call the associated functions.

In order to edit the (default) values in the profile settings, select the required profile and then click the [Edit] button.

For a more detailed configuration of profiles and different configuration modes refer to **Client Parameters**.