Telemotive
a company of Magna

Wi-Fi User Guide

Version 3.4.1 / 22.01.2019

Table of contents

1 LICENSE AGREEMENT

Please read the license agreement of this license contract carefully, before you install the software. By the installation of the software you agree to the conditions of this license contract.
This software-license agreement, in the following called “license”, contains all rights and restrictions for final users that regulate the use of the accompanying software, operating instructions and other documents, in the following called as “software”.

1. This license contract is an agreement between licensor and licensee, who is being licensed to use the named software.
2. Licensee acknowledges that this is only a limited nonexclusive license. This means, that the licensee has no right to allocate sublicenses. Licensor is and remains the owner of all titles, rights and interests in the software.
3. The software is a copyright property of the MAGNA Telemotive GmbH. The program or parts of it may not be further licensed to third parts, rented, sold or be further marketed in any form without explicit written approval by MAGNA Telemotive GmbH. The user may neither change the software and their components, nor modify, nor redevelop or decompile otherwise in any form.
4. This software is subject to no warranty. This software is sold as is, without any warranty. If at any time, a user changes his system, we hold no responsibility to change our software to make it work again.
5. This license permits licensee to install the software on more than one computer system, as long as the software will not be used on more than one computer system simultaneously. Licensee will not make copies of the software or allow copies of the software to be made by others, unless authorized by this license agreement. Licensee may make copies of the software for backup purposes only. Licensee is not entitled to transmit or to transfer the software or its rights from this license agreement.
6. Licensor is not liable to licensee for any damages, including compensatory, special, incidental, exemplary, punitive or consequential damages, connected with or resulting from this license agreement or licensee’s use of this software.
7. Licensee agrees to defend and indemnify licensor and hold licensor harmless from all claims, losses, damages, complaints or expenses connected with or resulting from licensee’s business operations.
8. Licensor has the right to terminate this license agreement and licensee’s right to use this software upon any material breach by licensee. The duration of the license contract is indefinitely determined.
9. Licensee agrees to return all copies of the software to licensor or to destroy them upon termination of the license contract.
10. This license agreement replaces and supersedes all prior negotiations, dealings and agreements between licensor and licensee regarding this software.
11. This license contract is subject to German law.
12. If a regulation of this license contract is void by law, the validity of the remaining regulations is not affected. If there is such a regulation it will be replaced by a valid, according to the legal regulations and enforceable regulation with similar intention and similar economic consequence.
13. The license contract is effective by delivery of the software of the licensor to the licensee and/or by usage of the software by the licensee. This license contract is also valid without licensor’s signature.
14. The license automatically goes out if the licensee does not agree to the license regulations described here or offend against the license regulations of this license contract. With ending the license contract the licensee is obliged to extinguish or to destroy the software and all copies of it no matter if installed or stored on disk or to hand all of it back to MAGNA Telemotive GmbH.
15. The licensee is liable for all damages caused to the licensor by the violation of these license regulations.

2 PRODUCT LIABILITY

The General Terms and Conditions of Sale and Delivery of MAGNA Telemotive GmbH can be found on our website at:
General_Terms_and_Conditions_of_Sale_and_Delivery_Telemotive_AG.pdf

3 Overview

This user guide describes the feature of the license **Wi-Fi** for the data loggers

- blue PiraT2
- blue PiraT2 5E
- blue PiraT Mini
- blue PiraT Remote

of MAGNA Telemotive GmbH.

This license enables the following options:

- wireless connection to the data logger
- configuring the data logger
- downloading data from the data logger
- reading the actual configuration of the data logger
- up from firmware release 3.1.1 a connection to a TSL cluster is possible too

This user guide describes the configuration and usage of this feature. The general configuration is described in the user guides of the used data logger as well as the Telemotive System Client, which is valid together.

This document refers to **firmware version 03.04.01** and the **Telemotive System Client** from **version 3.4.1**. Some features depending on model and feature license or may not be available in older versions.

Software updates and user guides for other, optional, licensed enhancements are available in the Telemotive ServiceCenter. (Please find the address under Contact at the last page.)

To ensure the most reliable operation of your system as possible, please make sure to use always current firmware and software versions.

Please note these important instructions about the handling of devices of MAGNA Telemotive GmbH!

There's a linux system running on the devices and sometimes when the device has a dirty shutdown due to a power break down or unplugging the power supply, the system is corrupt from this time. You know this situation from a PC, when you switch it off some times it maybe will not work any more or show you some mistakes.

In most cases this issue is catched up and repaired by the linux system we use, but sometimes it can happen that the system on the logger is damaged and there's no access to the device any more.

We are optimizing the handling of corrupted systems permanently and are integrating some new enhancements regarding this kind of issues with every new release to save the system. But we can't make the system for 100% save against these influences.

So please use always the provided mechanism for shutting down the device or the implemented standby function in which the device shutting down when no traffic is detected any more in an adjustable time.

Index

4 System requirements

Control Unit
A Windows based Laptop or PC is needed to configure the devices by **Telemotive System Client**. It also allows to save the recorded data and to use them offline later.

Telemotive System Client
The software client is used for configuring the data logger as well as downloading the recorded data or convert these into your needed file format. An firmware update can be performed by the **Telemotive System Client** too to ensure that your devices are always up to date.

blue PiraT2 / blue PiraT2 5E / blue PiraT Mini
The communication between bus systems and control units is monitored and relevant data can be recorded very precisely with the data logger. The collected data are stored to the logger and can be downloaded via Ethernet to a PC.

The **blue PiraT2** is our top-class all-in-one data logger. Seven models cover a wide range of interfaces.

Additionally, the **blue PiraT2 5E** offers improved power management and power backup, five integrated Ethernet ports and super-fast start-up behavior. The blue PiraT2 can be flexibly expanded via Telemotive System Link.

The **blue PiraT Mini** is smallest data logger in the world with an outstanding functional scope. It offers a wide range of interfaces, stable temperature behavior, very low energy consumption, four GBit Ethernet ports, and much more. Different blue PiraT Mini can be flexibly expanded to one cluster and therefore handled very easily by using Telemotive System Link.

Remote Control Touch (optional)
Operate your blue PiraT Mini or blue PiraT2 data loggers safely and comfortably from the driver's or passenger seat. Via Telemotive System Link our new remote control becomes part of your logger network. One remote control can handle all connected loggers.

blue PiraT Remote (optional)
While Remote Control Touch is just a control unit for handling unique devices or a TSL network, the blue PiraT Remote additional has logger functionality by offering internal storage and some interfaces.

Extension
The blue PiraT2 can be extended by an internal GPS/Wi-Fi module. Alternatively it is possible to connect an external USB Adapter to blue PiraT2 / 5E, blue PiraT Mini or blue PiraT Remote. By using a blue PiraT Mini an adapter cable USB 2.0 connector A to USB 2.0 connector Micro B is necessary. These adapters are supported:

- NETGEAR® N150 Wireless-USB-Adapter WNA1100-100PES
- NETGEAR® A6100 WiFi USB Mini Adapter AC600 Dual Band
- Edimax® AC600 Wireless Dual-Band Mini-USB-Adapter EW-7811UTC
- Edimax® AC1200 Wireless Dual-Band USB Adapter EW-7822UAC
- Edimax® AC1750 Wireless Dual-Band USB Adapter EW-7833UAC (from release 3.3.1)

Technical information of the adapters can be found in the appendix.

License
For the additional feature **WI-FI** an installed license is required. Settings for licensed features can be performed with a valid license only.

If you need a license for your logger, please contact our sales department (please find the address under contact at the last page).

4.1 Further manuals

Beside this user guide we offer the main manuals for our client as well as for the different data logger generations in our ServiceCenter at https://sc.telemotive.de/bluepirat.

User manual for the Telemotive System Client
https://sc.telemotive.de/4/uploads/media/TelemotiveSystemClient_UserManual.pdf

User manual for blue PiraT2 / blue PiraT2 5E
https://www.telemotive.de/4/uploads/media/blue_PiraT2_UserManual.pdf

User manual for blue PiraT Mini
https://www.telemotive.de/4/uploads/media/blue_PiraT_Mini_UserManual.pdf

User manual for Remote Control Touch
https://sc.telemotive.de/4/uploads/media/RCTouch_UserGuide.pdf

User manual for blue PiraT Remote
https://sc.telemotive.de/4/uploads/media/blue_PiraT_Remote_UserGuide.pdf

For having an easy access if necessary, the most important manuals are linked in the client under the menu item **[Help]** and are reachable easily from there.

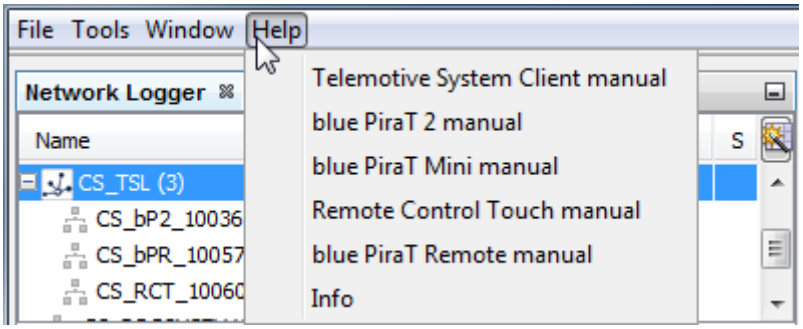


Figure 4.1: links to the manuals

Our licensed enhancements have own manuals which are stored in the ServiceCenter too. You will find a list of these enhancements in the user manuals in the chapter **Additional features by optional licenses**.

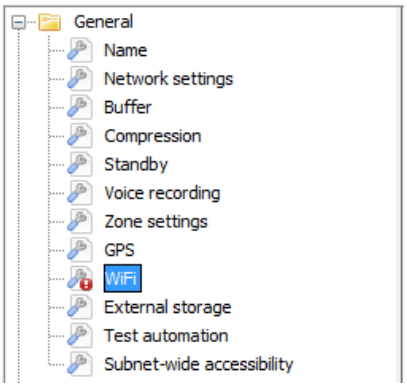
5 Configuration

Note:
Any network changes have to be applied to the device by clicking on [Write to logger]. If changes are applied only after restart, the client software will inform you and offers the direct restart.

For configuring the Wi-Fi feature (Managed / Master) a connection between the data logger and the Telemotive System Client on the PC is required. Please connect the data logger to the PC. If you configure the logger the first time for Wi-Fi, you have to connect via LAN cable. Later you can also change the configuration via an existing Wi-Fi connection.

Start the Telemotive System Client and select the data logger in the window <Network Logger>. Start the application **[Open configuration]** 5.

Expand the folder **[General]** in the configuration tree and choose the sub category **[Wi-Fi]**.



Enable the checkbox **Wi-Fi active** on the right.

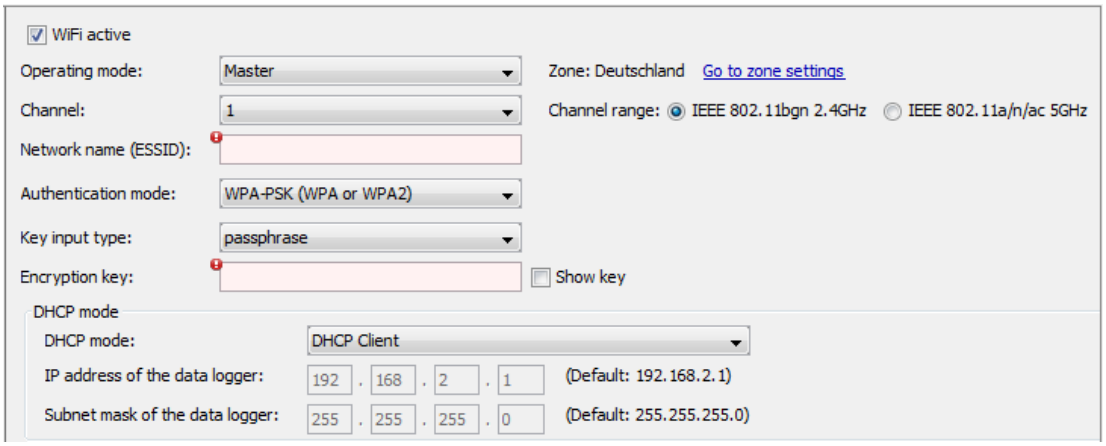


Figure 5.1: Wi-Fi configuration

If Wi-Fi is activated on the data logger, connected Wi-Fi modules are automatically detected and activated by the logger.

Index

5.1 Operating Modes

Choose the operating mode from the dropdown menu. There are two ways using the WLAN feature in the data logger.

5.1.1 Managed

The common way is using the data logger in the “Infrastructure” mode (**[Managed]** mode). In this mode you can integrate the data logger in an existing LAN/Wi-Fi infrastructure.

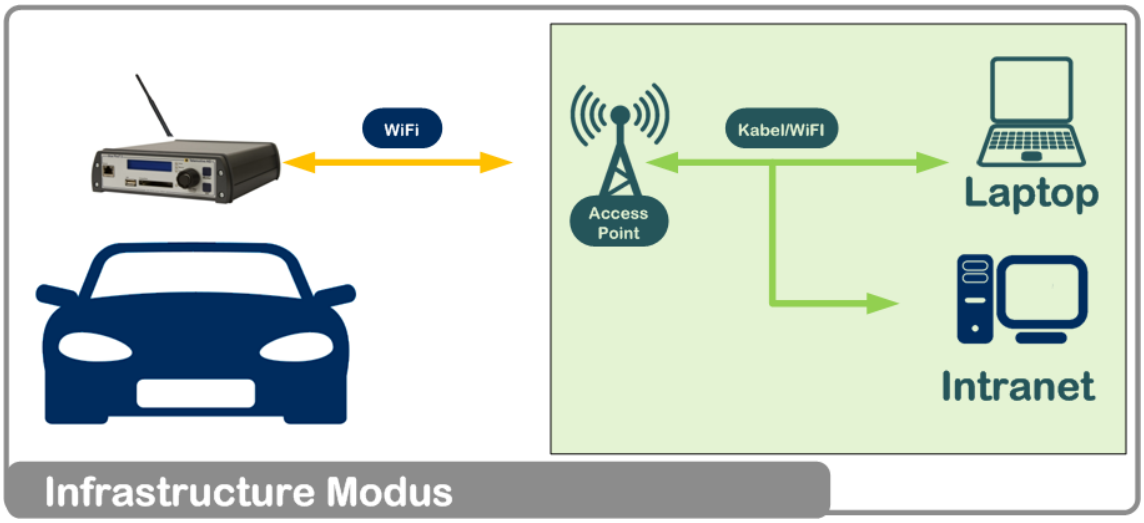


Figure 5.2: Managed or “Infrastructure” mode

5.1.2 Master

In **[Master]** mode the data logger takes the function of the Access Point. Devices (Laptops, Smartphones) can be connected to the logger directly to use DHCP services.

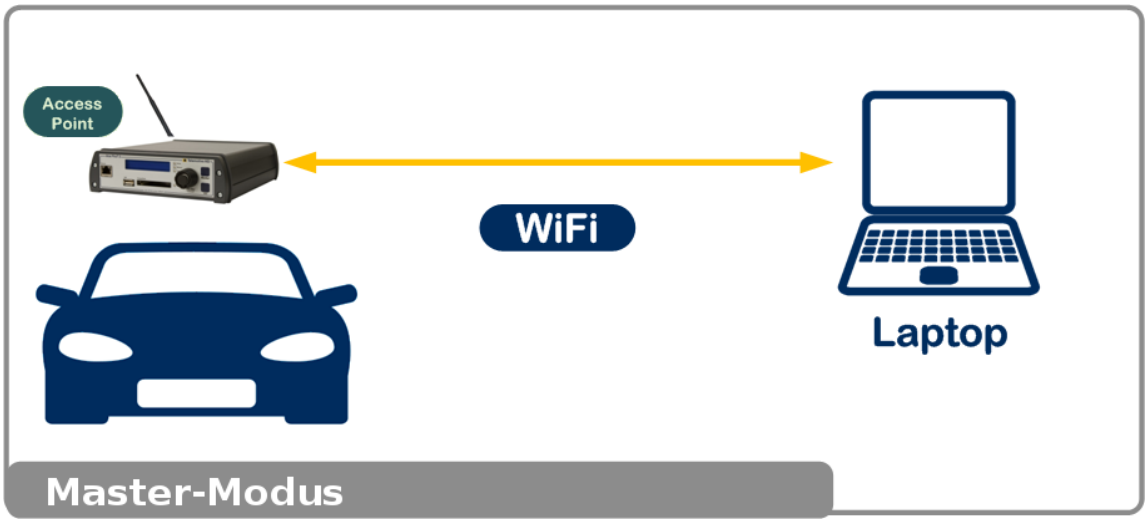


Figure 5.3: “Master” mode

5.2 Channel

In the Operating Mode **[Master]** you can switch to another Wi-Fi channel. Select a channel that is as far away as possible from other wireless networks in your environment.

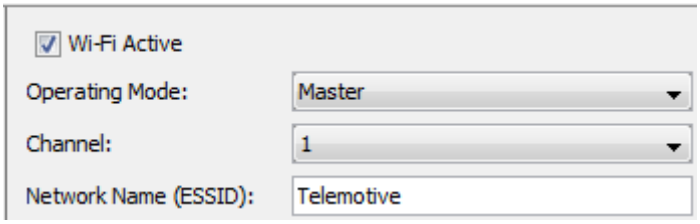


Figure 5.4: Enter Channel

5.2.1.1 Wi-Fi Standard Selection

From firmware version 2.4.1 on the wireless standard 802.11ac is supported in the Operating Mode **[Master]**.

You can choose the standard which is supported by your WiFi module in the settings.

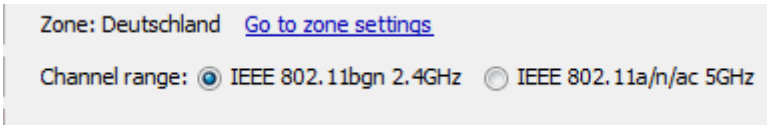


Figure 5.5: Wi-Fi Standard Selection

5.3 Network Name (ESSID)

The Network Name is set individually by the user.

Managed:
For Managed mode the user has to set the ESSID (Network Name) for the network, to which the logger should be connected.

Master:
Here the user can freely configure the ESSID, to later connect manually to the logger.

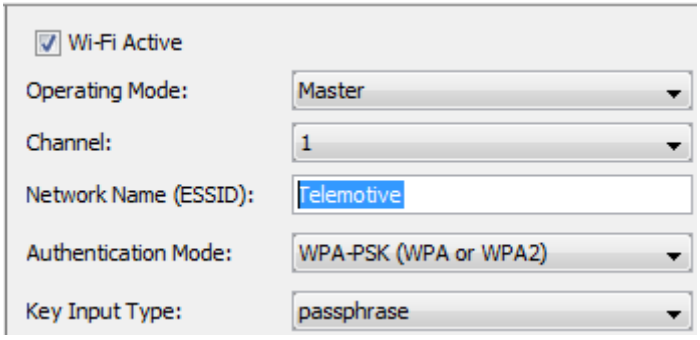


Figure 5.6: Enter Network Name

Index

5.4 Authentication Mode

If you set the Operating Mode **[Managed]**, select the Authentication Mode, which is used by your Access Point (AP).

For the Operating Mode **[Master]** only the Authentication Mode **WPA-PSK (WPA or WPA2)** is available to be used for the connection between logger and terminal.

The following Authentication Modes can be used.

5.4.1 Authentication by WPA-PSK

WPA-PSK (WPA or WPA2): PSK (Pre Shared Key)
The key of the user is known in advanced. Keys are exchanged before communication starts. The transmitted key and the stored key must match.

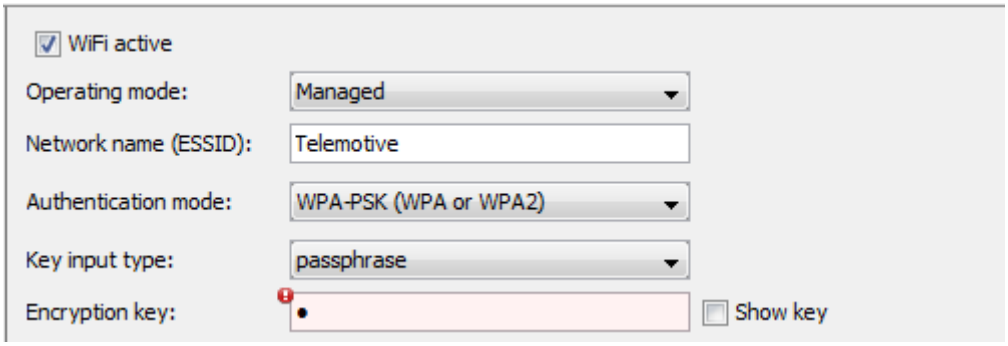


Figure 5.7: Authentication Mode WPA-PSK

5.4.2 Authentication by WPA-EAP | In operation mode [Managed] only

WPA-EAP: EAP = Extensible Authentication Protocol
While using EAP the negotiation of the used authentication method is done during the authentication process only. In the meantime EAP is widely used and supported by different transport protocols.

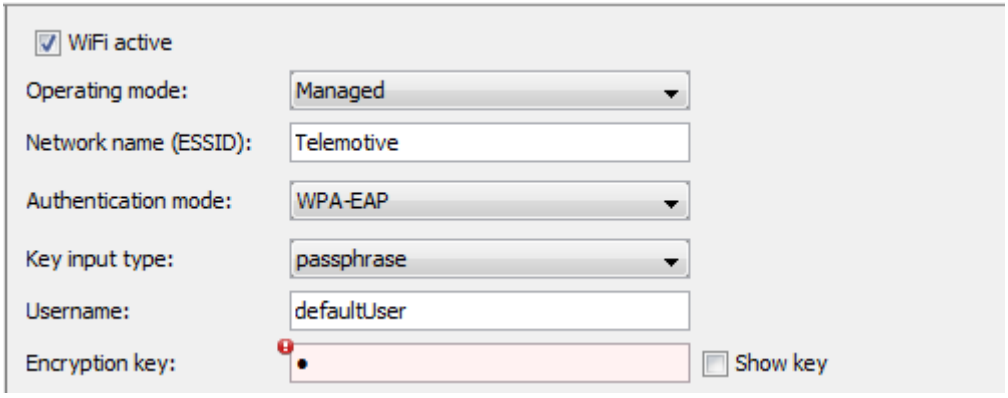


Figure 5.8: Authentication Mode WPA-EAP

When using **WPA-EAP**, a user name and an encryption key must be entered for authentication. If no username is filled in, the system uses the hostname of the device.

Changing the Authentication mode to WPA-EAP shows some more setting options in the configuration.

Additionally, the EAP authentication mode can be selected in WPA-EAP mode. The available settings are:

5.4.2.1 EAP authentication mode TLS

For EAP authentication mode TLS the available key input types for the encryption key are [passphrase] and [hexadecimal].

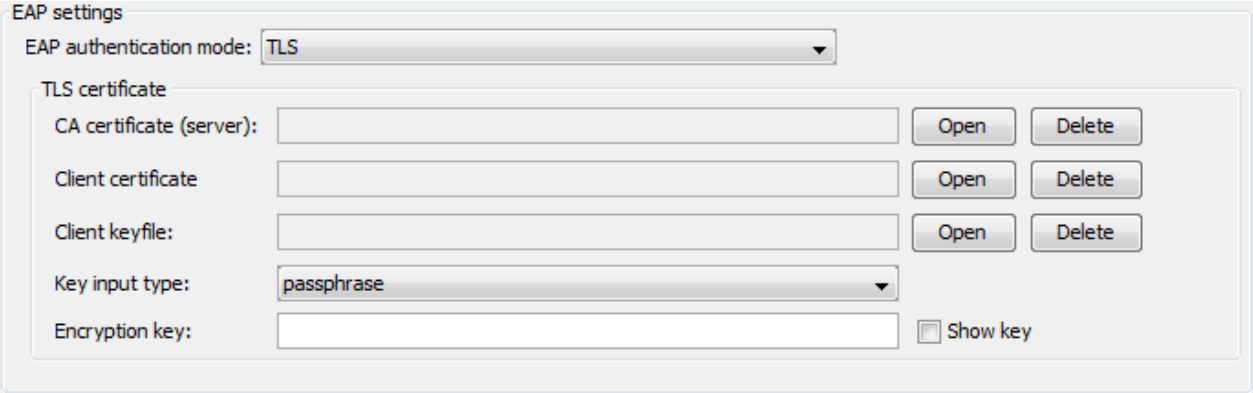


Figure 5.9: EAP authentication mode TLS

5.4.2.1.1 Certificate types

CA certificate (server)
Company intern certificate (CA = Certificate Authority)

Client certificate
Device certificate (may be valid for one or more devices)

Client keyfile / public key
Encrypted key for the client certificate

Encryption key / client key password / public key password
Password for decrypting the client key / public key

5.4.2.1.2 Use of the certificates

If device specific certificates are defined on the radius server:

- CA- and client certificate, client key and client key password
- Client-certificate, client key and client key password

If no device specific certificates are defined:

- CA-Zertifikat

No certificates are needed if no certificates are defined on the radius server.

5.4.2.2 EAP authentication mode Tunnel TTLS

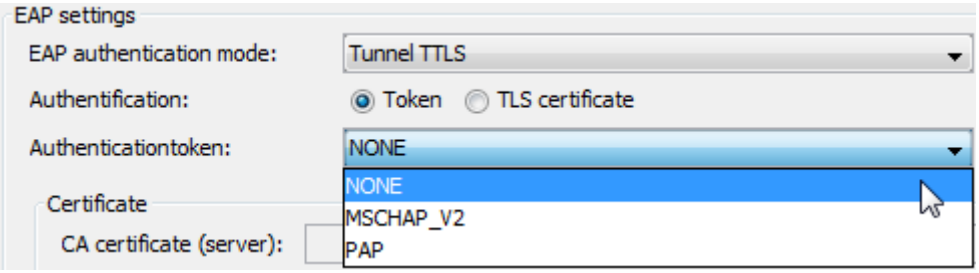


Figure 5.10: EAP authentication mode Tunnel TTLS

For **Tunnel TTLS** the authentication can be realized by a TLS certificate or a Token where additional the kind of authenticationtoken can be selected.

Figure 5.11: Tunnel TTLS with Token and Certificate

A **TLS certificate** can be transferred to the device too, if this is selected in the configuration.

Certificates can be deleted by the button **[Delete]**.

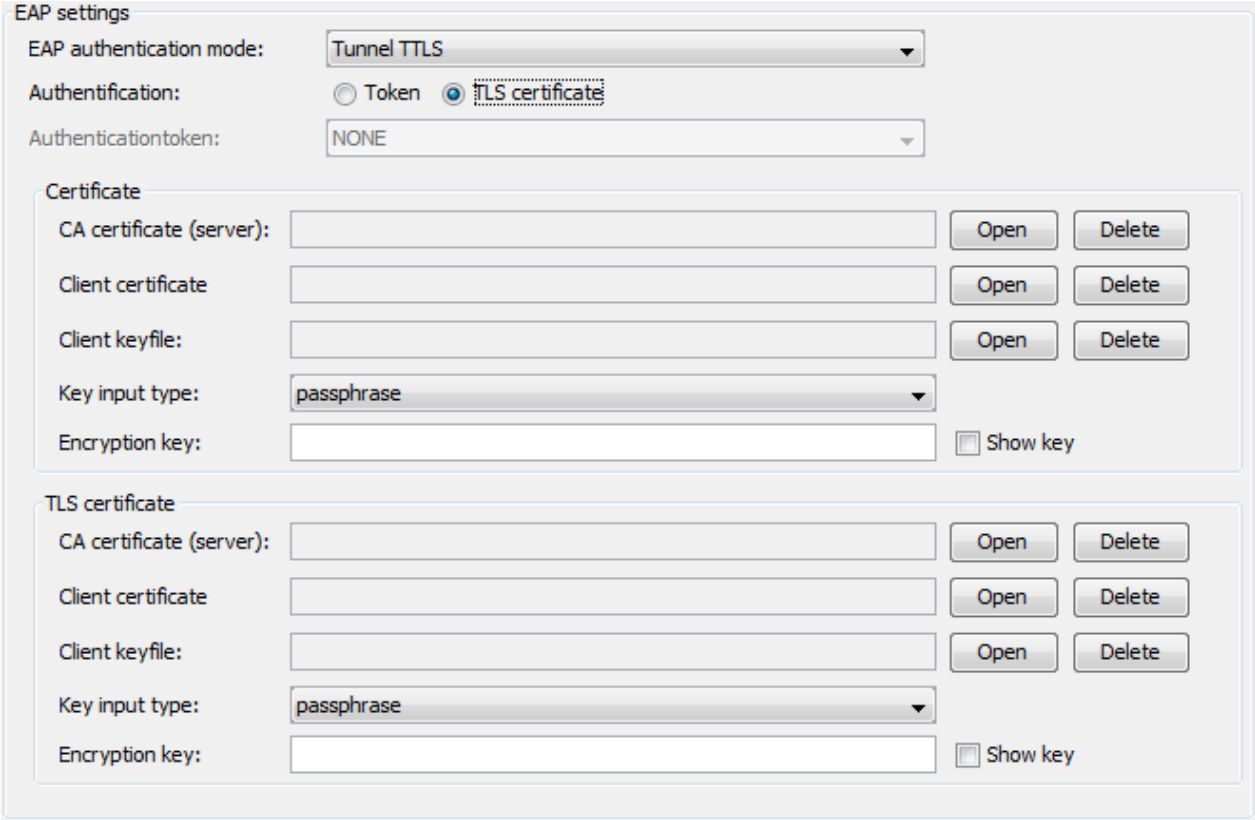


Figure 5.12: Tunnel TTLS with Token, Certificate and TLS certificate

5.4.2.3 EAP authentication mode: Tunnel PEAP

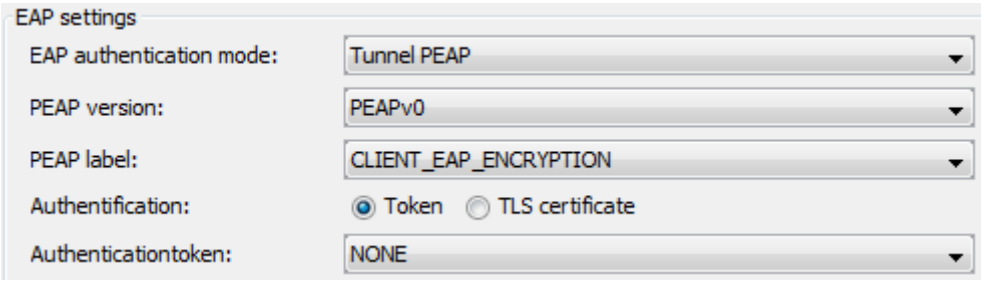


Figure 5.13: EAP authentication mode Tunnel PEAP

For the mode Tunnel PEAP additional to the art of the authentication token, the PEAP Version and PEAP Label can be defined.

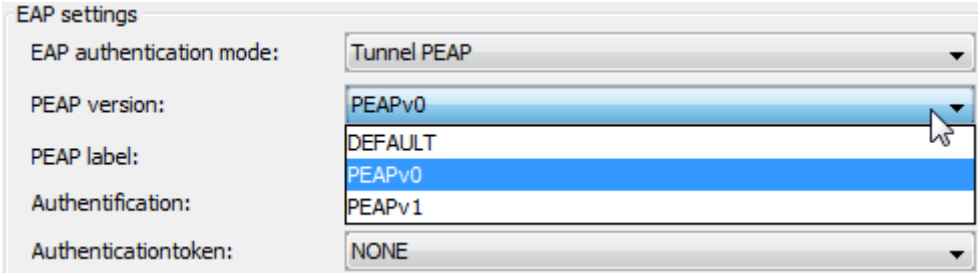


Figure 5.14: Tunnel PEAP | PEAP version

DEFAULT:
Deactivates the use of the PEAP version.

PEAPv0:
default: Is used most times

PEAPv1:

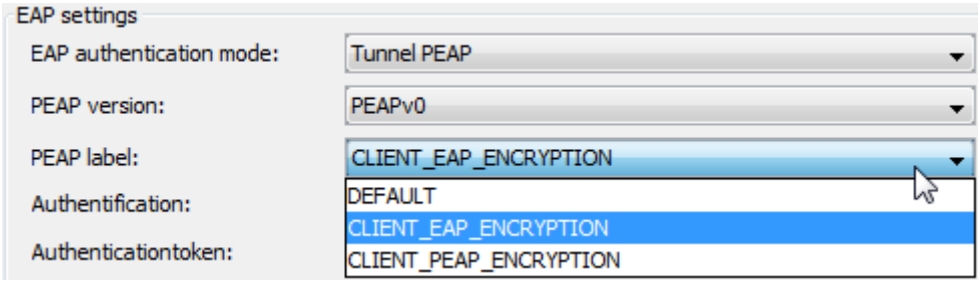


Figure 5.15: Tunnel PEAP | PEAP label

DEFAULT:
Deactivates the use of the PEAP label.

CLIENT_EAP_ENCRYPTION
default: old label: Is used most times

CLIENT_PEAP_ENCRYPTION
new label

In **Tunnel PEAP** mode the authentification can be realized by a Token as well as by a TLS certificate.

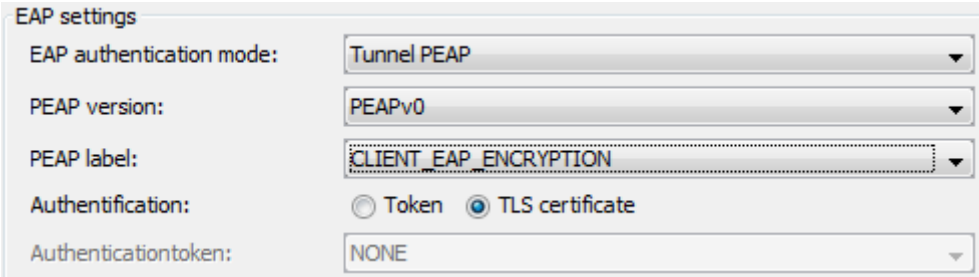


Figure 5.16: Tunnel PEAP | Token or TLS certificate

If token is used, the type of authentication token can also be specified. The following options are available:

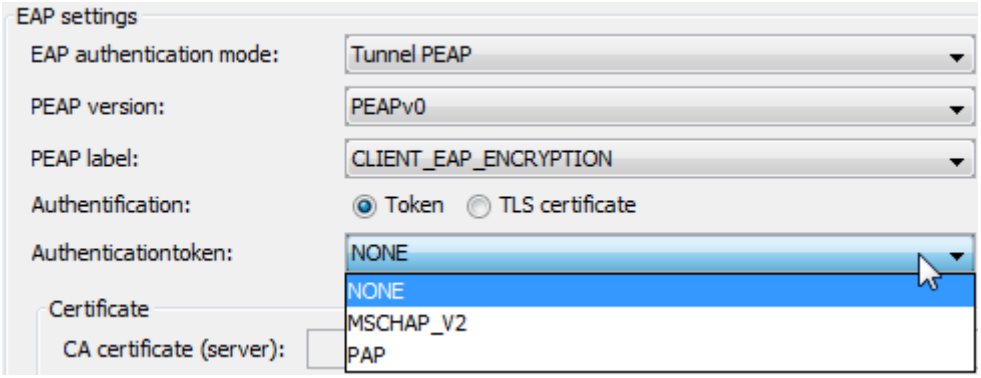


Figure 5.17: Tunnel PEAP | Token | Authenticationtoken

NONE
No encryption.

Certificates are optional.

MSCHAP_V2
Microsoft Challenge Handshake Authentication Protocol Version 2.

Certificates are optional.

PAP
Password Authentication Protocol.

Certificates are optional.

5.5 Key Input Type

Choose one of the following Key Input Types.

Passphrase:
Security key is generated from a password. The token length of key must be between 8 and 64.

Hexadecimal:
Security key has to be set and is displayed in hexadecimal digits. The token length of key must be exactly 64.

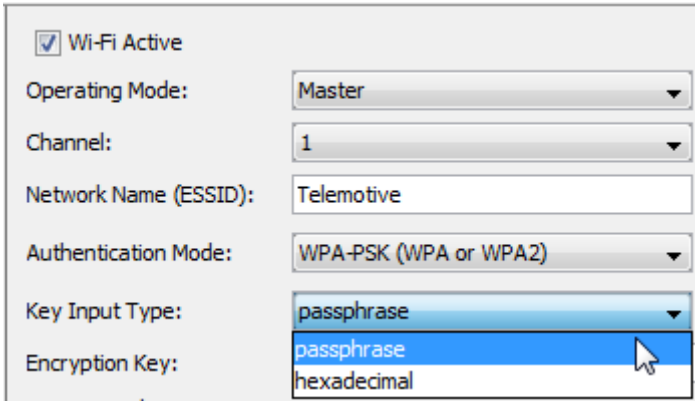


Figure 5.18: Select Key Input Type

5.6 Encryption Key

The Encryption key is set by the user. Red symbols with exclamation mark and a notification message indicate if a wrong encryption key is set.

Entering a key is optional and not mandatory.

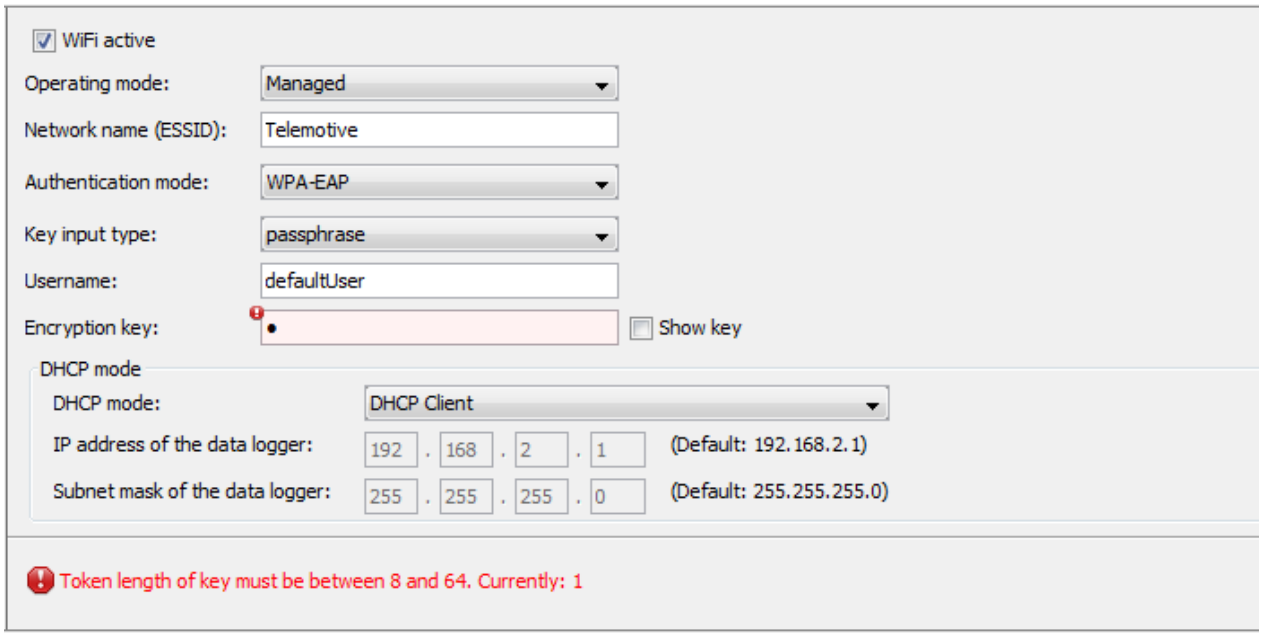


Figure 5.19: Warning for an invalid encryption key

Index

5.7 DHCP mode

At the bottom you can select the DHCP mode for your WiFi connection.

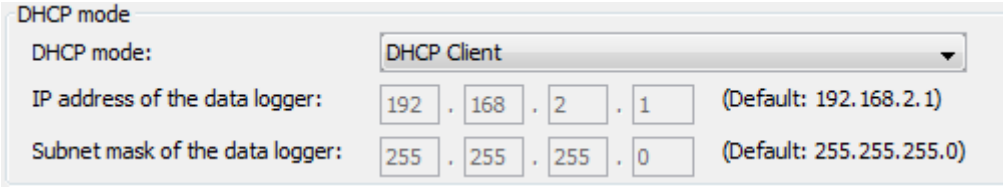


Figure 5.20: DHCP settings for the WiFi connection

These DHCP modi are available:

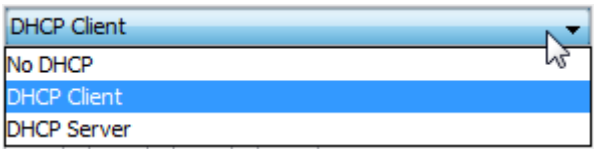


Figure 5.21: DHCP mode

DHCP master can be used in operating mode **[Master]** only.

5.8 Zone settings

By changing the <Country zone> you can set the frequency and transmission power which should be used in the respective country where you want to use the logger.

Figure 5.22: Configuration – General – Zone settings

5.8.1 Example: Connect a Smartphone with the logger

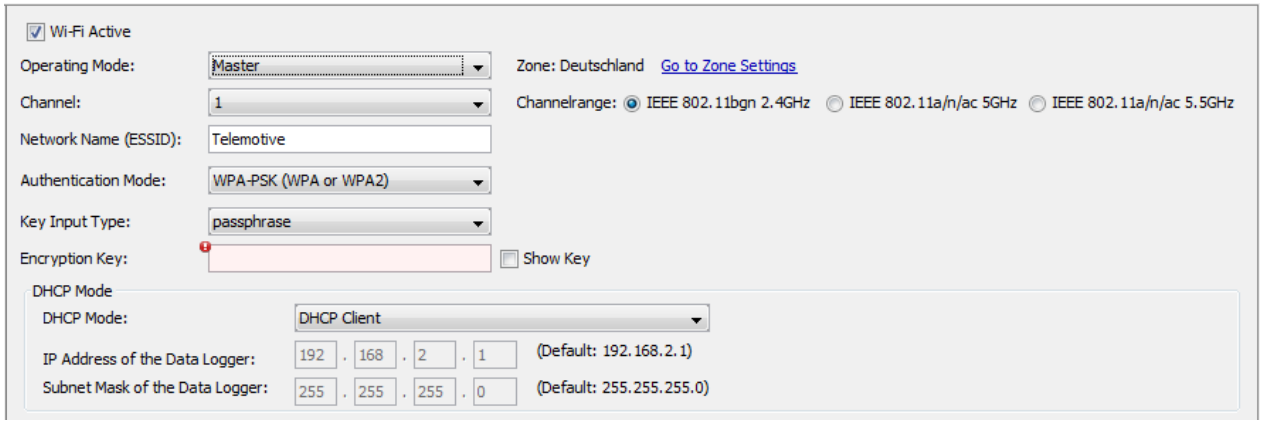


Figure 5.23: Example Wi-Fi configuration

Index

6 Additional information and settings for laptop/PC

If you have to set your IP address/subnet mask manually (e.g., when using the Operating Mode **[Ad-hoc]** or if no DHCP service is available in your infrastructure network), please open the "WIFI Status" of your wireless network card.

You can reach the Wi-Fi settings over the **[Properties]** button.

Note: **For changes administration rights are required.**

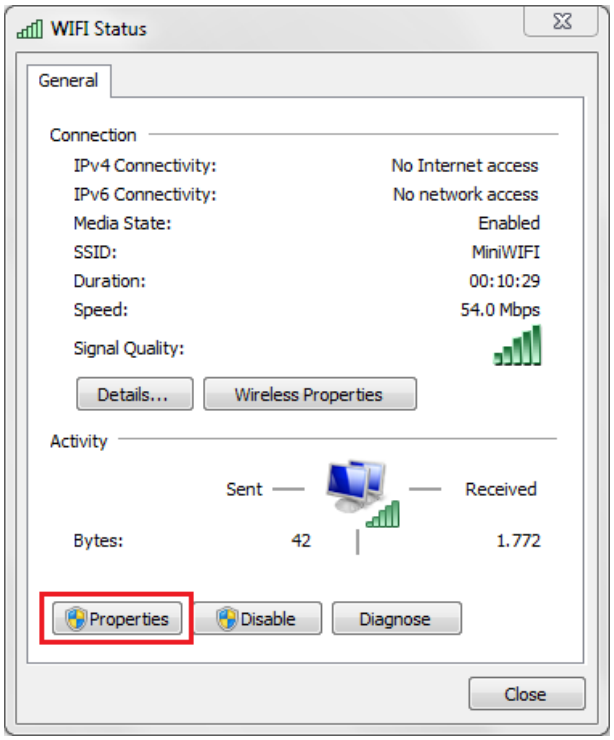


Figure 6.1: Wi-Fi Status

Now you have to choose your TCP/IP protocol. Please make sure to use the correct communication protocol. **(TCP/IPv4)** If necessary, contact your network administrator.

Select your used Wi-Fi protocol and click the **[Properties]** button.

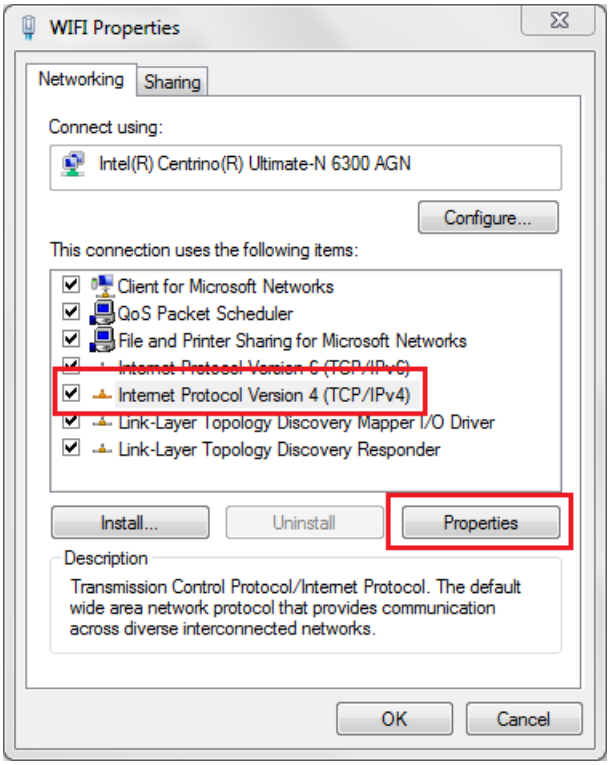


Figure 6.2: Wi-Fi Properties

Mark the checkbox **Use the following IP address:** to modify the IP address. Increase the last sign of the IP-address and use the default subnet mask. The settings for [Default gateway] and [DNS] do not have to be modified.

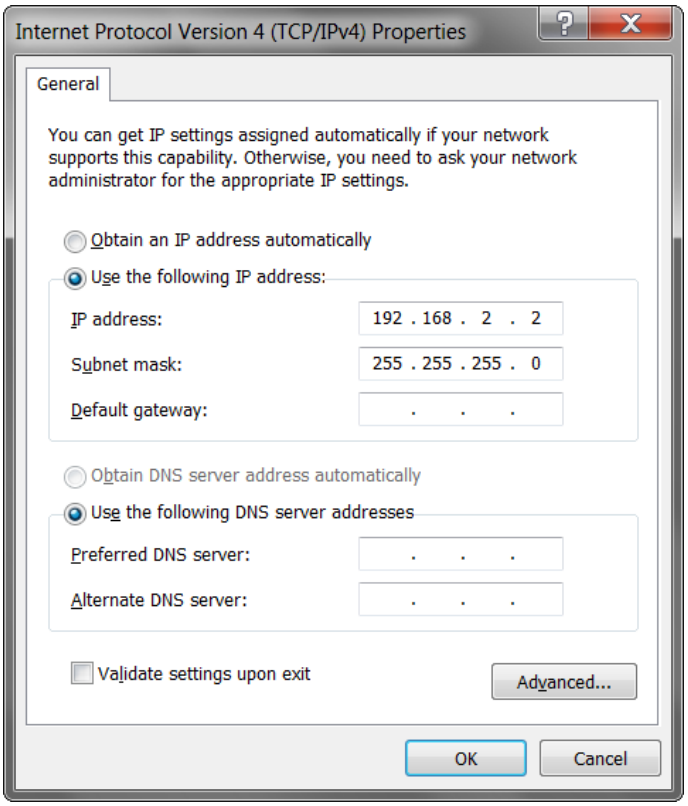


Figure 6.3: Internet Protocol Properties

7 Connecting to the data logger via Wi-Fi

Step 1:
Connect your PC/laptop with the previously configured network.

Step 2:
Open the Telemotive System Client and have a look at the Network Logger list. Upon successful connection to the data logger or TSL cluster via Wi-Fi, the logger appears with a symbol in the list.

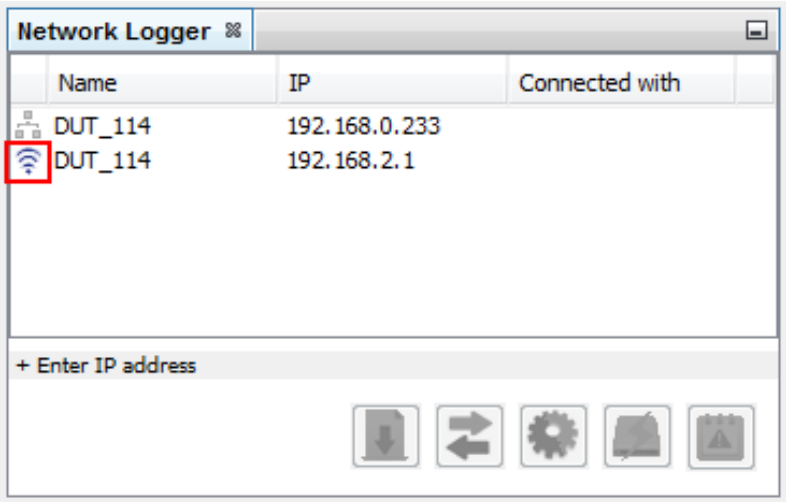


Figure 7.1: Tab "Network Logger"

Index

8 Appendix | Technical information about the adapters

Adapter / adapter	NETGEAR® N150	NETGEAR® N300	NETGEAR® A6100	Edimax® AC600	Edimax® AC1200	Edimax® AC1750
	WNA1100-100PES	WNA3100M-100PES	A6100-AC600	EW-7811UTC	EW-7822AUC	EW-7833AUC
Hersteller / Manufacturer	Netgear	Netgear	Netgear	Edimax	Edimax	Edimax
Chip / chip	AR9002U/AR9271	RTL8192CU	RTL8821AU	RTL8812AU	RTL8821AU	RTL8814AU
Treiber / driver	ath9k_htc	rtl8192cu	rtl8821au	rtl8821au	rtl8821au	rtl8814au
IEEE 802.11	bgn	bgn	abgn+ac	abgn+ac	abgn+ac	abgn+ac
Antenne / antenna	1x1	2x2	1x1	1x1	2x2	3x3
WPA/WPA2	WPA-EAP, WPA-PSK	WPA-EAP, WPA-PSK	WPA-EAP, WPA-PSK	WPA-EAP, WPA-PSK	WPA-EAP, WPA-PSK	WPA-EAP, WPA-PSK
Access Point*						
IEEE 802.11	bpn	bpn	abgn+ac	abgn+ac	abgn+ac	abgn+ac
Bandbreite / bandwith	20MHz	20MHz	20MHz , 40MHz (802.11 ac)	20MHz , 40MHz (802.11 ac)	20MHz , 40MHz (802.11 ac)	20MHz , 40MHz (802.11 n) 80MHz (802.11 ac)
Kanäle / channels**	1 - 11	1 - 11	1-11, 36, 44	1-11, 36, 44	1-11, 36, 44	1-11, 36, 44

* Bei Verwendung des Adapters im Master Modus als Access Point / By using the adapter in master mode as access point

** Die verfügbaren Kanäle sind länderabhängig / Available channels depend on the country settings.

Figure 8.1: Appendix | Technical information about the adapters

Note: Due to connection interrupts, the Netgear N300 adapter is not recommended and not sold by Telemotive any more.

9 Abbreviations

Kürzel / abbreviation	Bedeutung / meaning
blue PiraT	**P**rocessing **I**nformation **R**ecording **A**nalyzing **T**ool
bP	**b**lue **P**iraT
bP2	**b**lue **P**iraT**2**
bP2 5E	**b**lue **P**iraT**2** 5E
bPMini	**b**lue **P**iraT Mini
RC Touch	**R**emote **C**ontrol **T**ouch
bP Remote	**b**lue **P**iraT **R**emote
A2L	**A**SAM MCD-**2** MC **L**anguage
AE	**A**utomotive **E**lectronics
ACK	**ACK**nowledged
CAN	**C**ontroller **A**rea **N**etwork
CCP	**C**AN **C**alibration **P**rotocol
CF	**C**ompact **F**lash
CRO	**C**ommand **R**eceive **O**bject
DAQ	**D**ata **A**cquisition
DTO	**D**ata **T**ransmission **O**bject
ECL	**E**lectrical **C**ontrol **L**ine
ECU	**E**lectronic **C**ontrol **U**nit
FIBEX	**FI**eld **B**us **Ex**change Format
FW	**F**irm**w**are
GMT	**G**reenwich **M**ean **T**ime
INCA	**IN**tegrated **C**alibration and **A**pplication Tool
LAN	**L**ocal **A**rea **N**etwork = Netzwerk
LIN	**L**ocal **I**nterconnect **N**etwork
MAC	**M**edia **A**ccess **C**ontrol
MCD	**M**easure **C**alibrate **D**iagnose
MDX	**M**eta **D**ata E**X**change Format
MEP	**M**OST **E**thernet **P**acket
MOST	**M**edia **O**riented **S**ystems **T**ransport (www.mostnet.de)
ODT	**O**bject **D**escriptor **T**able
ODX	**O**pen **D**ata E**X**change
OEM	**O**riginal **E**quipment **M**anufacturer

PHY	**PHY**sical Bus Connect
PW	**P**ass**w**ort
RX	**R**eceiver Data
SD	**S**ecure **D**igital
SFTP	**S**ecure **F**ile **T**ransfer **P**rotocol
SHA	**S**ecure **Ha**sh
SSL	**S**ecure **S**ockets **L**ayer
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
TMP	**T**ele**m**otive **P**acketformat
TSL	**T**elemotive **S**ystem **L**ink
UDP	**U**ser **D**atagram **P**rotocol
USB	**U**niversal **S**erial **B**us
UTC	**U**niversal **T**ime, **C**oordinated
Wi-Fi	**Wi**reless **Fi**delity
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
XCP	Universal Measurement and **C**alibration **P**rotocol

Table 9.1: Abbreviations

Index

10 List of figures

Index

11 List of tables

Index

12 Contact

MAGNA Telemotive GmbH

Office München
Frankfurter Ring 115a
80807 München

Tel.: +49 89 357186-0
Fax.: +49 89 357186-520
E-Mail: TMO.info@magna.com
Web: www.telemotive.de

Sales
Tel.: +49 89 357186-550
Fax.: +49 89 357186-520
E-Mail: TMO.Sales@magna.com

Support
Tel.: +49 89 357186-518
E-Mail: TMO.productsupport@magna.com
ServiceCenter: https://sc.telemotive.de/bluepirat