



# BLUEPIRAT


BY MAGNA



## BLUEPIRAT Series WiFi User Guide / 21.07.2020

Version 3.4.3

## Table of contents

<b>1</b>	<b>LICENSE AGREEMENT</b> .....	<b>3</b>
<b>2</b>	<b>PRODUCT LIABILITY</b> .....	<b>4</b>
<b>3</b>	<b>Overview</b> .....	<b>5</b>
<b>4</b>	<b>System requirements</b> .....	<b>7</b>
4.1	Further manuals.....	9
4.2	Additional features by optional licenses .....	10
4.3	Firmware Care .....	11
<b>5</b>	<b>Configuration</b>  .....	<b>12</b>
5.1	Operating Modes .....	13
5.1.1	Managed .....	13
5.1.2	Master .....	13
5.2	Channel .....	14
5.2.1.1	Wi-Fi Standard Selection.....	14
5.3	Network Name (ESSID) .....	14
5.4	Authentication Mode .....	15
5.4.1	Authentication by WPA-PSK.....	15
5.4.2	Authentication by WPA-EAP   In operation mode [Managed] only .....	15
5.4.2.1	EAP authentication mode TLS .....	16
5.4.2.1.1	Certificate types.....	17
5.4.2.1.2	Use of the certificates .....	17
5.4.2.2	EAP authentication mode Tunnel TTLS .....	18
5.4.2.3	EAP authentication mode: Tunnel PEAP.....	19
5.5	Key Input Type.....	21
5.6	Encryption Key.....	21
5.7	DHCP mode.....	22
5.8	Zone settings .....	22
5.8.1	Example: Connect a Smartphone with the logger .....	23
<b>6</b>	<b>Additional information and settings for laptop/PC</b> .....	<b>24</b>
<b>7</b>	<b>Connecting to the data logger via Wi-Fi</b> .....	<b>26</b>
<b>8</b>	<b>Appendix   Technical information about the adapters</b> .....	<b>27</b>
<b>9</b>	<b>Abbreviations</b> .....	<b>28</b>
<b>10</b>	<b>List of figures</b> .....	<b>30</b>
<b>11</b>	<b>List of tables</b> .....	<b>31</b>
<b>12</b>	<b>Version history</b> .....	<b>32</b>
<b>13</b>	<b>Contact</b> .....	<b>33</b>

# 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 (<https://telemotive.magna.com>) under imprint.

### 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 System Client, which is valid together.

This document refers to **firmware version 03.04.03** and the **System Client** from **version 3.4.3**. 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 our Service Center. (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 caught 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 **System Client**. It also allows to save the recorded data and to use them offline later.

### 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. A firmware update can be performed by the **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 expanded flexibly via [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 expanded flexibly to one cluster and therefore handled very easily by using [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 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 System Client

[https://sc.telemotive.de/4/uploads/media/TelemotiveSystemClient\\_UserManual.pdf](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](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](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](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](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.

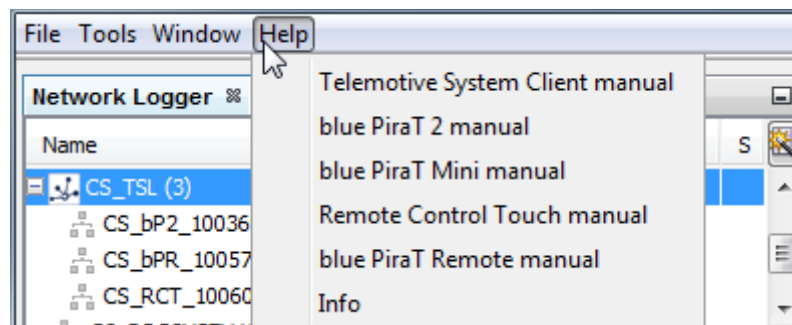


Figure 4.1: links to the manuals

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

## 4.2 Additional features by optional licenses

Additional features can be activated by purchasing and installing licenses. Licenses can be ordered at our sales team. You find the user guides for these additional features in our Service Center. Currently the following licensed features are available.

Feature	Description
<b>Camera Link</b>	video recording via video server or network cameras
<b>WLAN</b>	supporting wireless LAN (802.11, 802.11a, 802.11n), (802.11ac from FW 02.04.01)
<b>GPS logging</b>	tracking of GPS data
<b>Measurements with CCP</b>	CAN Calibration Protocol
<b>Measurements with XCP</b>	Universal Measurement and Calibration Protocol Currently the functionality for Ethernet (XCP on Ethernet) and the CAN-bus (XCP on CAN) are available.
<b>MOST150 Streaming</b>	logging MOST150 synchronous/isochronous data
<b>MLBevo</b>	The license Connected-Gateway MLBevo enables the recording of data of the ATOP control unit MLBevo via USB to the Telemotive data logger and convert these data with the System Client. (from FW 02.03.01)
<b>Download Terminal</b>	Download Terminal allows an automatization of configured tasks for a defined group of devices. (from FW 02.03.01)
<b>TPE</b>	TPE = Telemotive Performance Extension Increasing the logging rate for Ethernet data up to 100Mbit/s (from FW 02.04.01)
<b>Test automatisation</b>	Interface for connecting to test automation tools. At the moment, the sending of CAN messages is supported. (from FW 02.04.01)
<b>Cellular network</b>	Allows the logger to send status messages over cellular network. (from FW 03.01.01)

Table 4.1: Additional features by optional licenses

## 4.3 Firmware Care

MAGNA Telemotive GmbH invests a great amount in the further development of its products.

For this we regularly provide new functions and enhancements via firmware and client releases.

### Basic conditions

As part of the " Service Product Firmware Care ", new software and firmware versions are made available for download for a limited period of time. This service is available for 12 months from the date of purchasing the **blue PiraT Rapid**. This period can be extended.

For details, please contact your sales partner (see contact at the end of the manual for addresses).

### Affected products

- **blue PiraT Mini**
- **blue PiraT2 5E**
- **blue PiraT2**
- **blue PiraT Remote**
- **Remote Control Touch**
- **blue PiraT Rapid**

### Note:

**Enhancements are only possible in current firmware releases.**

### Attention:

**Please note that updates to main firmware versions (04.00.01 / 05.00.01) need a special update license and can't be flashed to a device without this license.**

To buy these licenses please contact our sales department under [TMO.Sales@magna.com](mailto:TMO.Sales@magna.com) (please find the complete address under *Contact on the last page*).

## 5 Configuration

### Note:

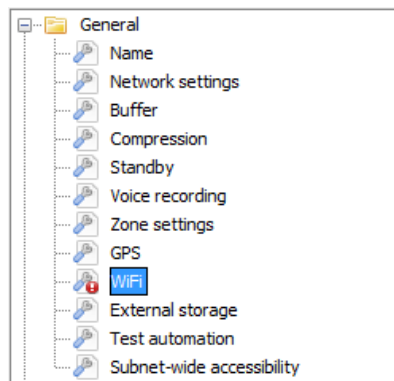
Any network changes have to be applied to the device by clicking on [Write to logger]. If changes are applied only after restart, the client software will inform you and offers the direct restart.

For configuring the Wi-Fi feature (Managed / Master) a connection between the data logger and the 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 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.

## 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.

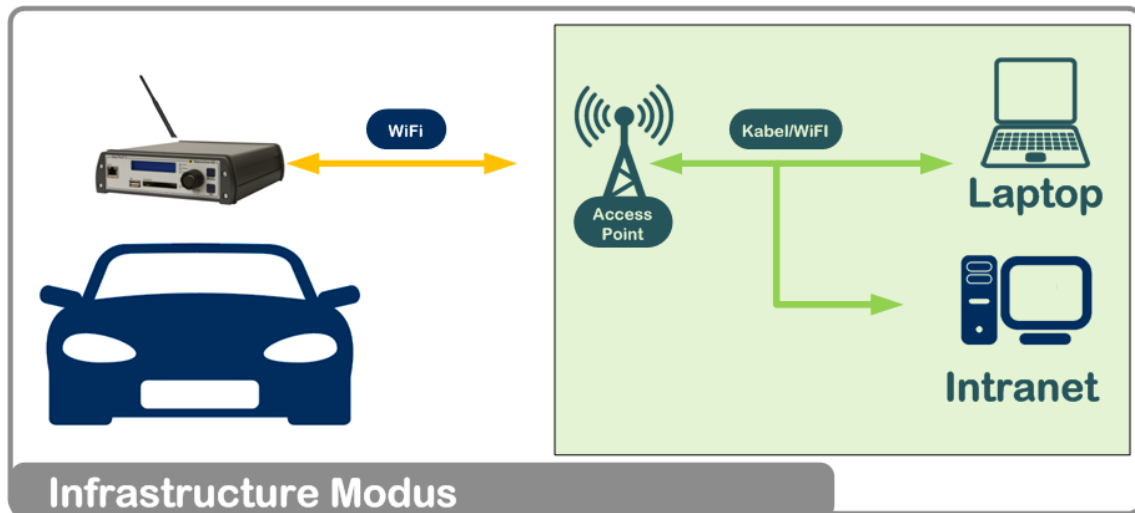


Figure 5.2: Managed or “Infrastructure” mode

### 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.

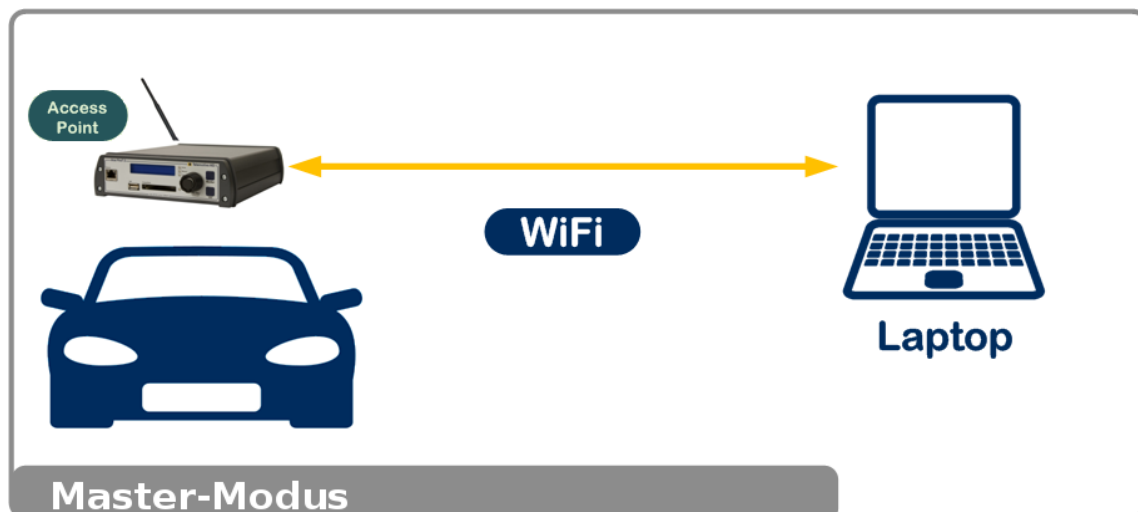
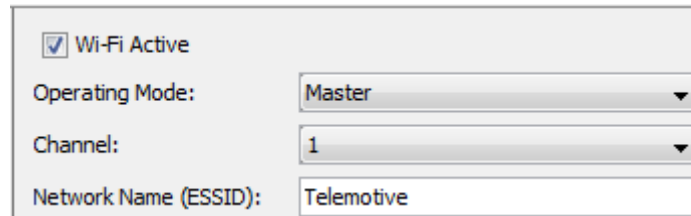


Figure 5.3: “Master” mode

## 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.



The screenshot shows a configuration panel with the following elements:

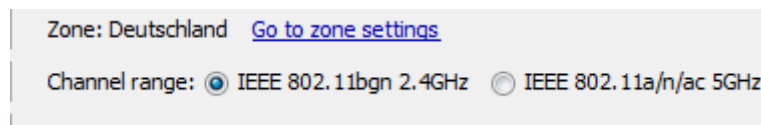
- Wi-Fi Active
- Operating Mode: **Master** (dropdown menu)
- Channel: **1** (dropdown menu)
- Network Name (ESSID): **Telemotive** (text input field)

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.



The screenshot shows the following configuration options:

- Zone: Deutschland [Go to zone settings](#)
- Channel range:  IEEE 802.11bgn 2.4GHz  IEEE 802.11a/n/ac 5GHz

Figure 5.5: Wi-Fi Standard Selection

## 5.3 Network Name (ESSID)

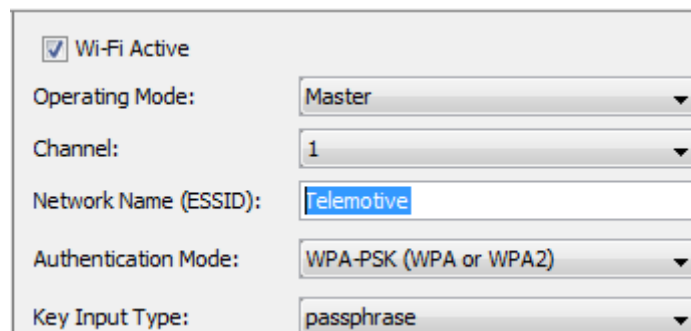
The Network Name is set individually by the user.

### 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.



The screenshot shows a configuration panel with the following elements:

- Wi-Fi Active
- Operating Mode: **Master** (dropdown menu)
- Channel: **1** (dropdown menu)
- Network Name (ESSID): **Telemotive** (text input field)
- Authentication Mode: **WPA-PSK (WPA or WPA2)** (dropdown menu)
- Key Input Type: **passphrase** (dropdown menu)

Figure 5.6: Enter Network Name

## 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.

The screenshot shows a configuration panel for WiFi. At the top, there is a checkbox labeled 'WiFi active' which is checked. Below this, there are several fields: 'Operating mode' is a dropdown menu set to 'Managed'; 'Network name (ESSID):' is a text input field containing 'Telemotive'; 'Authentication mode:' is a dropdown menu set to 'WPA-PSK (WPA or WPA2)'; 'Key input type:' is a dropdown menu set to 'passphrase'; and 'Encryption key:' is a text input field with a red error icon to its left and a 'Show key' checkbox to its right. The encryption key field contains a single black dot.

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.

The screenshot shows a configuration panel for WiFi. At the top, there is a checkbox labeled 'WiFi active' which is checked. Below this, there are several fields: 'Operating mode' is a dropdown menu set to 'Managed'; 'Network name (ESSID):' is a text input field containing 'Telemotive'; 'Authentication mode:' is a dropdown menu set to 'WPA-EAP'; 'Key input type:' is a dropdown menu set to 'passphrase'; 'Username:' is a text input field containing 'defaultUser'; and 'Encryption key:' is a text input field with a red error icon to its left and a 'Show key' checkbox to its right. The encryption key field contains a single black dot.

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].

The screenshot shows the 'EAP settings' configuration window. At the top, 'EAP authentication mode:' is set to 'TLS'. Below this, a section titled 'TLS certificate' contains three rows: 'CA certificate (server):', 'Client certificate', and 'Client keyfile:'. Each row has a text input field followed by 'Open' and 'Delete' buttons. The 'Key input type:' dropdown is set to 'passphrase'. At the bottom, the 'Encryption key:' field is empty, with a 'Show key' checkbox to its right.

**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

EAP settings

EAP authentication mode: Tunnel TTLS

Authentication:  Token  TLS certificate

Authentication token: NONE

Certificate

CA certificate (server):

**Figure 5.10: EAP authentication mode Tunnel TTLS**

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

Certificate

CA certificate (server):

Client certificate

Client keyfile:

Key input type:

Encryption key:   Show key

**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]**.

EAP settings

EAP authentication mode: Tunnel TTLS

Authentication:  Token  TLS certificate

Authentication token: NONE

Certificate

CA certificate (server):

Client certificate

Client keyfile:

Key input type:

Encryption key:   Show key

TLS certificate

CA certificate (server):

Client certificate

Client keyfile:

Key input type:

Encryption key:   Show key

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

### 5.4.2.3 EAP authentication mode: Tunnel PEAP

EAP settings	
EAP authentication mode:	Tunnel PEAP
PEAP version:	PEAPv0
PEAP label:	CLIENT_EAP_ENCRYPTION
Authentication:	<input checked="" type="radio"/> Token <input type="radio"/> TLS certificate
Authentication token:	NONE

**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.

EAP settings	
EAP authentication mode:	Tunnel PEAP
PEAP version:	PEAPv0
PEAP label:	CLIENT_EAP_ENCRYPTION
Authentication:	<input checked="" type="radio"/> Token <input type="radio"/> TLS certificate
Authentication token:	NONE

**Figure 5.14: Tunnel PEAP | PEAP version**

**DEFAULT:**

Deactivates the use of the PEAP version.

**PEAPv0:**

default: Is used most times

**PEAPv1:**

EAP settings	
EAP authentication mode:	Tunnel PEAP
PEAP version:	PEAPv0
PEAP label:	CLIENT_EAP_ENCRYPTION
Authentication:	<input checked="" type="radio"/> Token <input type="radio"/> TLS certificate
Authentication token:	NONE

**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 authentication can be realized by a Token as well as by a TLS certificate.

The screenshot shows the 'EAP settings' configuration panel. The 'EAP authentication mode' is set to 'Tunnel PEAP'. The 'PEAP version' is set to 'PEAPv0'. The 'PEAP label' is set to 'CLIENT\_EAP\_ENCRYPTION'. Under the 'Authentication' section, the 'TLS certificate' radio button is selected. The 'Authenticationtoken' dropdown menu is set to 'NONE'.

**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:

The screenshot shows the 'EAP settings' configuration panel with 'Token' selected under 'Authentication'. The 'Authenticationtoken' dropdown menu is expanded, showing three options: 'NONE', 'MSCHAP\_V2', and 'PAP'. A mouse cursor is pointing at the 'NONE' option. Below the dropdown, there is a 'Certificate' section with a 'CA certificate (server):' checkbox.

**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.

The screenshot shows a configuration window for Wi-Fi. At the top, there is a checkbox labeled 'Wi-Fi Active' which is checked. Below it are several configuration fields: 'Operating Mode' set to 'Master', 'Channel' set to '1', 'Network Name (ESSID)' set to 'Telemotive', and 'Authentication Mode' set to 'WPA-PSK (WPA or WPA2)'. The 'Key Input Type' dropdown menu is open, showing three options: 'passphrase' (which is highlighted in blue), 'passphrase', and 'hexadecimal'. A mouse cursor is pointing at the 'passphrase' option.

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.

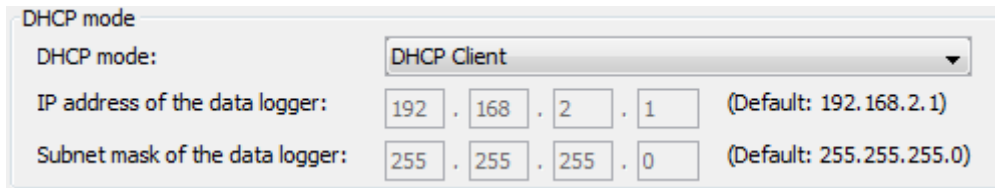
Entering a key is optional and not mandatory.

The screenshot shows a configuration window for Wi-Fi. At the top, there is a checkbox labeled 'WiFi active' which is checked. Below it are several configuration fields: 'Operating mode' set to 'Managed', 'Network name (ESSID)' set to 'Telemotive', 'Authentication mode' set to 'WPA-EAP', 'Key input type' set to 'passphrase', and 'Username' set to 'defaultUser'. The 'Encryption key' field is empty and has a red exclamation mark icon next to it. To the right of the field is a checkbox labeled 'Show key'. Below the encryption key field is a section for 'DHCP mode' with a dropdown set to 'DHCP Client'. Underneath are two rows of IP address and subnet mask input fields. At the bottom of the window, there is a red notification message: 'Token length of key must be between 8 and 64. Currently: 1'.

Figure 5.19: Warning for an invalid encryption key

## 5.7 DHCP mode

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



DHCP mode

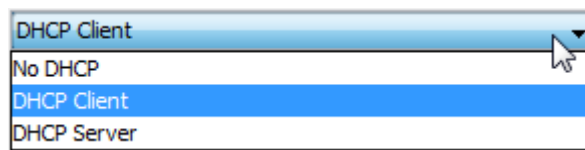
DHCP mode: DHCP Client

IP address of the data logger: 192 . 168 . 2 . 1 (Default: 192.168.2.1)

Subnet mask of the data logger: 255 . 255 . 255 . 0 (Default: 255.255.255.0)

**Figure 5.20: DHCP settings for the WiFi connection**

These DHCP modi are available:



DHCP Client

No DHCP

DHCP Client

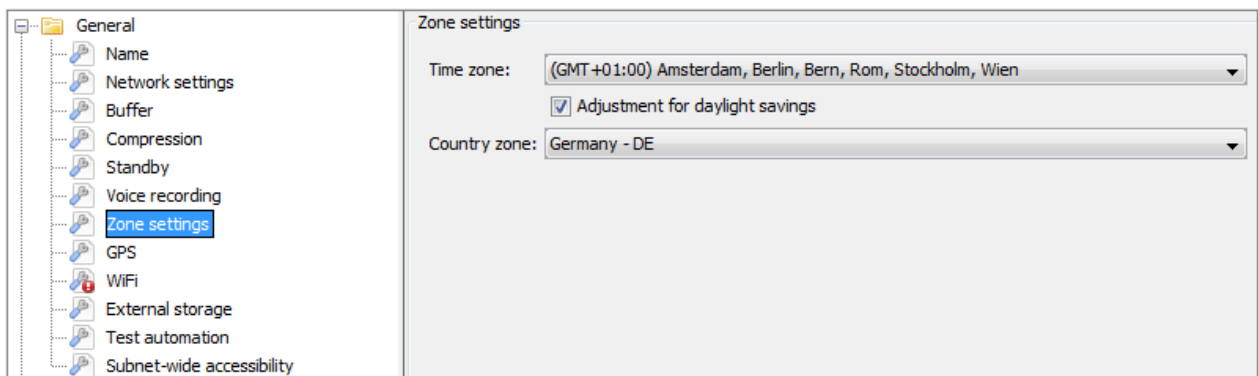
DHCP Server

**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.



General

- Name
- Network settings
- Buffer
- Compression
- Standby
- Voice recording
- Zone settings**
- GPS
- WiFi
- External storage
- Test automation
- Subnet-wide accessibility

Zone settings

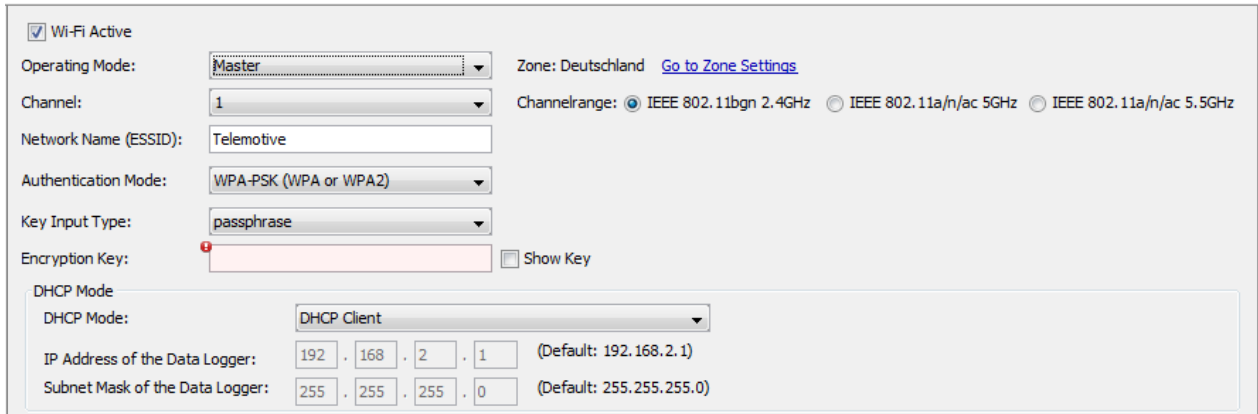
Time zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Adjustment for daylight savings

Country zone: Germany - DE

**Figure 5.22: Configuration – General – Zone settings**

### 5.8.1 Example: Connect a Smartphone with the logger



The screenshot displays a web-based configuration interface for a Wi-Fi network. At the top left, there is a checked checkbox labeled "Wi-Fi Active". Below this, the "Operating Mode" is set to "Master" in a dropdown menu. To the right, the "Zone" is set to "Deutschland" with a link to "Go to Zone Settings". The "Channel" is set to "1" in a dropdown menu. The "Channelrange" is set to "IEEE 802.11bgn 2.4GHz" with radio buttons for "IEEE 802.11a/n/ac 5GHz" and "IEEE 802.11a/n/ac 5.5GHz". The "Network Name (ESSID)" is "Telemotive" in a text input field. The "Authentication Mode" is "WPA-PSK (WPA or WPA2)" in a dropdown menu. The "Key Input Type" is "passphrase" in a dropdown menu. The "Encryption Key" is a redacted field with a "Show Key" checkbox. Below this, the "DHCP Mode" is "DHCP Client" in a dropdown menu. The "IP Address of the Data Logger" is set to "192 . 168 . 2 . 1" with a default value of "192.168.2.1". The "Subnet Mask of the Data Logger" is set to "255 . 255 . 255 . 0" with a default value of "255.255.255.0".

Figure 5.23: Example Wi-Fi configuration

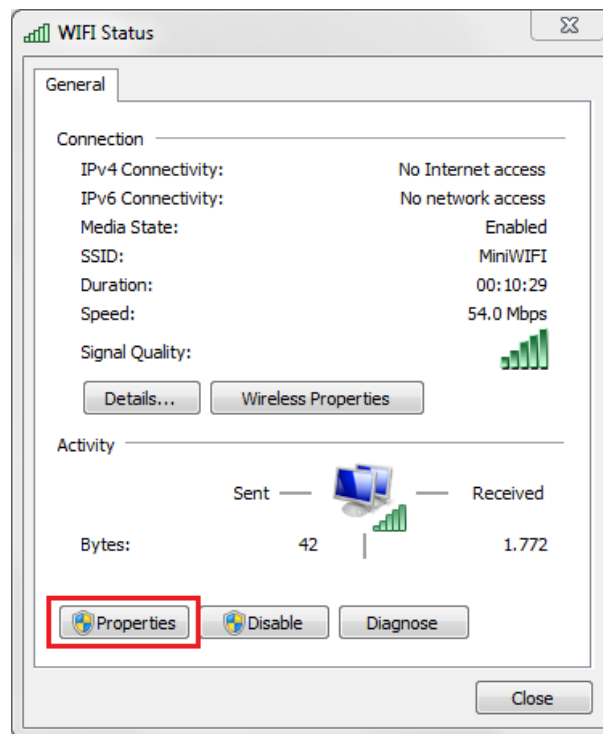
[Index](#)

## 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.

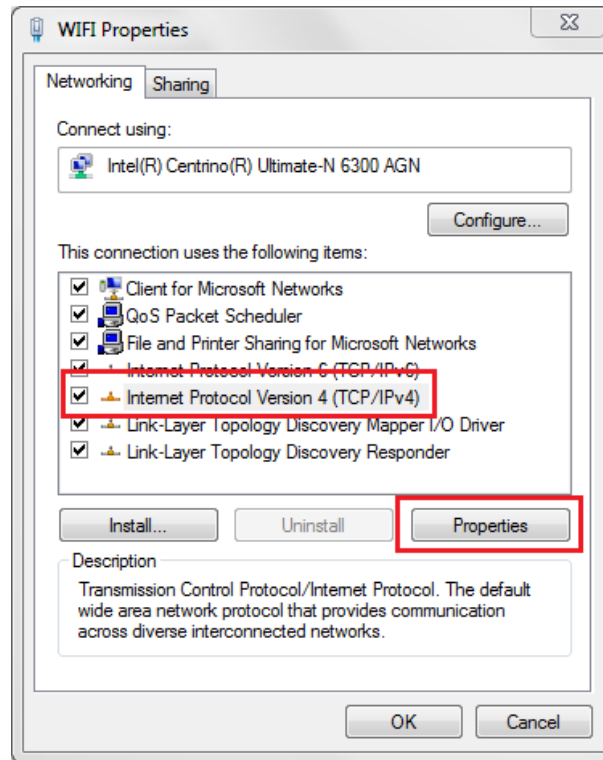


**Figure 6.1: Wi-Fi Status**

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.

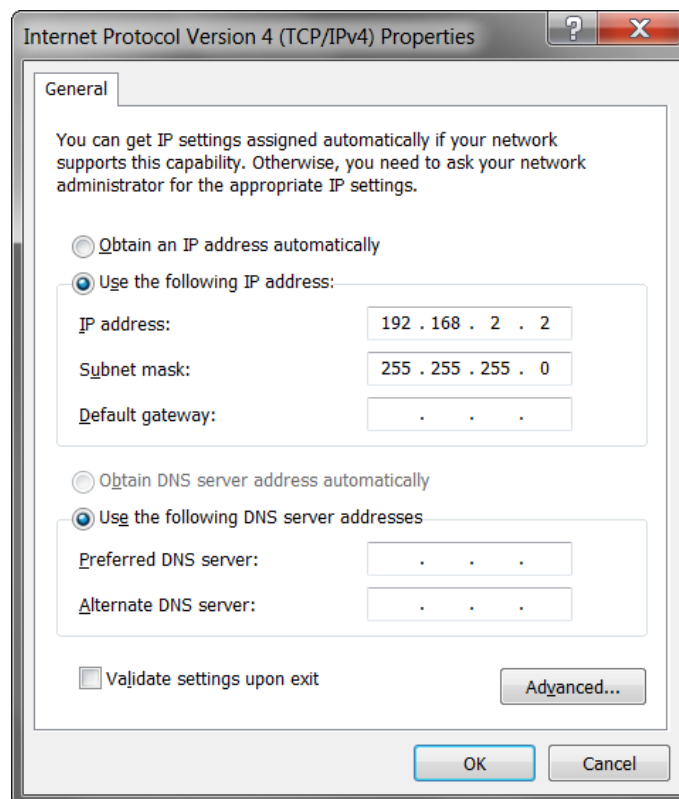
Select your used Wi-Fi protocol and click the **[Properties]** button.





**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 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.

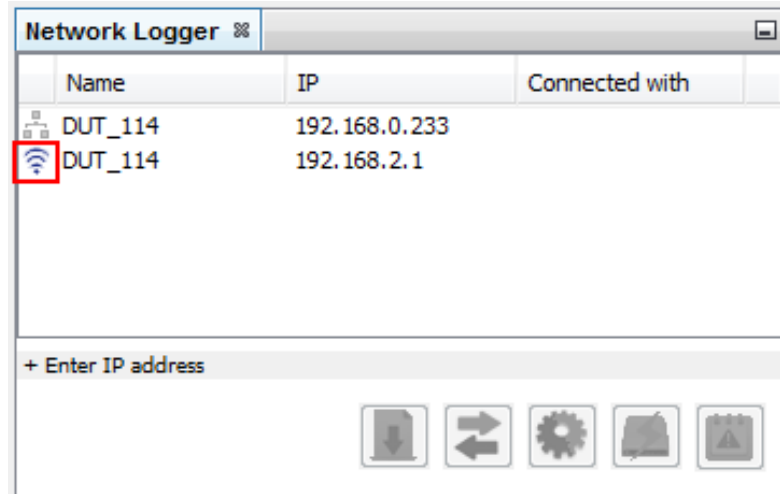


Figure 7.1: Tab “Network Logger”

## 8 Appendix | Technical information about the adapters

Adapter / adapter	NETGEAR® N150	NETGEAR® N300	NETGEAR® A6100	Edimax® AC600	Edimax® AC1200	Edimax® AC1750
Hersteller / Manufacturer	WNA1100-100PES Netgear	WNA3100M-100PES Netgear	A6100-AC600 Netgear	EW-7811UTC Edimax	EW-7822AUC Edimax	EW-7833AUC 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	bgn	bgn	abgn+ac	abgn+ac	abgn+ac	abgn+ac
Bandbreite / bandwidth	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 MAGNA Telemotive any more.

## 9 Abbreviations

Kürzel / abbreviation	Bedeutung / meaning
blue PiraT	Processing Information Recording Analyzing Tool
bP	blue PiraT
bP2	blue PiraT2
bP2 5E	blue PiraT2 5E
bPMini	blue PiraT Mini
RC Touch	Remote Control Touch
bP Remote	blue PiraT Remote
A2L	ASAM MCD-2 MC Language
AE	Automotive Electronics
ACK	ACKnowledged
CAN	Controller Area Network
CCP	CAN Calibration Protocol
CF	Compact Flash
CRO	Command Receive Object
DAQ	Data Acquisition
DTO	Data Transmission Object
ECL	Electrical Control Line
ECU	Electronic Control Unit
FIBEX	Field Bus Exchange Format
FW	Firmware
GMT	Greenwich Mean Time
INCA	INtegrated Calibration and Application Tool
LAN	Local Area Network = Netzwerk
LIN	Local Interconnect Network
MAC	Media Access Control
MCD	Measure Calibrate Diagnose
MDX	Meta Data EXchange Format
MEP	MOST Ethernet Packet
MOST	Media Oriented Systems Transport ( <a href="http://www.mostnet.de">www.mostnet.de</a> )
ODT	Object Descriptor Table
ODX	Open Data EXchange
OEM	Original Equipment Manufacturer
PHY	PHYsical Bus Connect
PW	Password
RX	Receiver Data
SD	Secure Digital
SFTP	Secure File Transfer Protocol
SHA	Secure Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TMP	Telemotive Packetformat
TSL	Telemotive System Link
UDP	User Datagram Protocol
USB	Universal Serial Bus

<b>UTC</b>	<b>Universal Time, Coordinated</b>
<b>Wi-Fi</b>	<b>Wireless Fidelity</b>
<b>WLAN</b>	<b>Wireless Local Area Network</b>
<b>XCP</b>	<b>Universal Measurement and Calibration Protocol</b>

**Table 9.1: Abbreviations**

## 10 List of figures

Figure 4.1: links to the manuals.....	9
Figure 5.1: Wi-Fi configuration.....	12
Figure 5.2: Managed or “Infrastructure” mode .....	13
Figure 5.3: “Master” mode .....	13
Figure 5.4: Enter Channel .....	14
Figure 5.5: Wi-Fi Standard Selection .....	14
Figure 5.6: Enter Network Name .....	14
Figure 5.7: Authentication Mode WPA-PSK.....	15
Figure 5.8: Authentication Mode WPA-EAP.....	15
Figure 5.9: EAP authentication mode TLS.....	16
Figure 5.10: EAP authentication mode Tunnel TTLS.....	18
Figure 5.11: Tunnel TTLS with Token and Certificate .....	18
Figure 5.12: Tunnel TTLS with Token, Certificate and TLS certificate .....	18
Figure 5.13: EAP authentication mode Tunnel PEAP .....	19
Figure 5.14: Tunnel PEAP   PEAP version .....	19
Figure 5.15: Tunnel PEAP   PEAP label .....	19
Figure 5.16: Tunnel PEAP   Token or TLS certificate.....	20
Figure 5.17: Tunnel PEAP   Token   Authenticationtoken .....	20
Figure 5.18: Select Key Input Type .....	21
Figure 5.19: Warning for an invalid encryption key .....	21
Figure 5.20: DHCP settings for the WiFi connection .....	22
Figure 5.21: DHCP mode .....	22
Figure 5.22: Configuration – General – Zone settings .....	22
Figure 5.23: Example Wi-Fi configuration .....	23
Figure 6.1: Wi-Fi Status.....	24
Figure 6.2: Wi-Fi Properties.....	25
Figure 6.3: Internet Protocol Properties .....	25
Figure 7.1: Tab “Network Logger” .....	26
Figure 8.1: Appendix   Technical information about the adapters .....	27

[Index](#)

## 11 List of tables

Table 4.1: Additional features by optional licenses .....	10
Table 9.1: Abbreviations .....	29
Table 12.1: Version history .....	32

[Index](#)

## 12 Version history

Version	Änderung	Datum

Table 12.1: Version history



## 13 Contact



DRIVING **EXCELLENCE.**  
INSPIRING **INNOVATION.**

### **MAGNA Telemotive GmbH**

Office München  
Frankfurter Ring 115a  
80807 München / Germany

Tel.: +49 89 357186-0  
Fax.: +49 89 357186-520  
E-Mail: [TMO.info@magna.com](mailto:TMO.info@magna.com)  
Web: <https://telemotive.magna.com>

Sales  
Tel.: +49 89 357186-550  
Fax.: +49 89 357186-520  
E-Mail: [TMO.Sales@magna.com](mailto:TMO.Sales@magna.com)

Support  
Tel.: +49 89 357186-518  
E-Mail: [TMO.productsupport@magna.com](mailto:TMO.productsupport@magna.com)  
ServiceCenter: <https://sc.telemotive.de/bluepirat>

© by MAGNA Telemotive GmbH  
Subject to errors and to technical changes as part of product improvement.