



BLUEPIRAT

BY MAGNA




BLUEPIRAT Serie

WLAN Anleitung / 21.07.2020

Version 3.4.3

Inhaltsverzeichnis

1	LIZENZVERTRAG	3
2	PRODUKTHAFTUNG	4
3	Übersicht	5
4	Systemvoraussetzungen	7
4.1	Weiterführende Anleitungen	9
4.2	Zusätzliche Funktionen über optionale Lizenzen	10
4.3	Firmware Care	11
5	Konfiguration 	12
5.1	Betriebsarten	13
5.1.1	Managed	13
5.1.2	Master	13
5.2	Kanal	14
5.2.1.1	WLAN-Standard Auswahl.....	14
5.3	Netzwerk Name (ESSID)	14
5.4	Authentifizierungs-Modus	16
5.4.1	Authentifizierung über WPA-PSK	16
5.4.2	Authentifizierung über WPA-EAP Nur in Betriebsart [Managed]	16
5.4.2.1	EAP-Authentifizierungsmodus: TLS	17
5.4.2.1.1	Zertifikatstypen	18
5.4.2.1.2	Anwendungsarten der Zertifikate	18
5.4.2.2	EAP-Authentifizierungsmodus Tunnel TTLS	19
5.4.2.3	EAP-Authentifizierungsmodus Tunnel PEAP.....	20
5.5	Verschlüsselungstyp	22
5.6	Schlüssel	22
5.7	DHCP-Einstellungen	23
5.8	Zoneneinstellungen	23
5.8.1	Beispiel: Verbindung eines Smartphones mit dem Logger.....	24
6	Weitere Informationen und Einstellungen am Laptop/PC	25
7	Verbindung mit dem Datenlogger über WLAN	27
8	Anhang Technische Informationen zu den Adaptern	28
9	Abkürzungen	29
10	Abbildungsverzeichnis	31
11	Tabellenverzeichnis	32
12	Versionshistorie	33
13	Kontakt	34

1 LIZENZVERTRAG

Lesen Sie bitte die Lizenzvereinbarung dieses Lizenzvertrages sorgfältig, bevor Sie die Software installieren. Durch das Installieren der Software stimmen Sie den Bedingungen dieses Lizenzvertrages zu.

Diese Software-Lizenzvereinbarung, nachfolgend als „Lizenz“ bezeichnet, enthält alle Rechte und Beschränkungen für Endanwender, die den Gebrauch der begleitenden Software, Bedienungsanleitung und sonstigen Unterlagen, nachfolgend als „Software“ bezeichnet, regeln.

1. Dieser Lizenzvertrag ist eine Vereinbarung zwischen dem Lizenzgeber und Lizenznehmer, der die Lizenz erhält, um die genannte Software zu verwenden.
2. Dem Lizenznehmer ist bekannt, dass dies nur eine beschränkte, nicht exklusive Lizenz ist. Dies bedeutet, dass der Lizenznehmer keinerlei Recht auf Lizenzvergabe hat. Der Lizenzgeber ist und bleibt der Eigentümer aller Titel, Rechte und Interessen an der Software.
3. Die Software ist urheberrechtlich geschütztes Eigentum der MAGNA Telemotive GmbH. Das Programm oder Teile davon dürfen nicht an Dritte vermietet, verkauft, weiterlizenziert oder sonst in irgendeiner Form ohne ausdrückliche, schriftliche Genehmigung der MAGNA Telemotive GmbH weitervermarktet werden. Der Anwender darf die Software und deren Bestandteile weder verändern, modifizieren noch sonst in irgendeiner Form rückentwickeln oder dekompileieren.
4. Diese Software unterliegt keiner Garantie. Die Software wurde verkauft wie sie ist, ohne jegliche Garantie. Falls irgendwann ein Benutzer sein System ändert, trägt der Lizenzgeber keine Verantwortung dafür, die Software zu ändern, damit sie wieder funktioniert.
5. Diese Lizenz erlaubt dem Lizenznehmer, die Software auf mehr als einem Computersystem zu installieren, solange die Software nicht gleichzeitig auf mehr als einem Computersystem verwendet wird. Der Lizenznehmer darf keine Kopien der Software machen oder Kopien der Software erlauben, wenn keine Autorisierung dafür besteht. Der Lizenznehmer darf lediglich zu Sicherheitszwecken Kopien der Software machen. Der Lizenznehmer ist nicht berechtigt, die Software oder ihre Rechte aus dieser Lizenzvereinbarung weiterzugeben oder zu übertragen.
6. Der Lizenzgeber ist gegenüber dem Lizenznehmer weder für Schäden, einschließlich kompensatorischer, spezieller, beiläufiger, exemplarischer, strafender oder folgenreicher Schäden, verantwortlich, die sich aus dem Gebrauch dieser Software durch den Lizenznehmer ergeben.
7. Der Lizenznehmer ist bereit, den Lizenzgeber zu schützen, zu entschädigen und fern zu halten von allen Ansprüchen, Verlusten, Schäden, Beschwerden oder Ausgaben, die mit den Geschäftsoperationen des Lizenznehmers verbunden sind oder sich aus diesen ergeben.
8. Der Lizenzgeber hat das Recht, diesen Lizenzvertrag sofort zu kündigen und das Softwarebenutzungsrecht des Lizenznehmers zu begrenzen, falls es zu einem Vertragsbruch seitens des Lizenznehmers kommt. Die Laufdauer des Lizenzvertrages ist auf unbestimmte Zeit festgelegt.
9. Der Lizenznehmer ist bereit, dem Lizenzgeber alle Kopien der Software bei Kündigung des Lizenzvertrages zurückzugeben oder zu zerstören.
10. Dieser Lizenzvertrag beendet und ersetzt alle vorherigen Verhandlungen, Vereinbarungen und Abmachungen, zwischen dem Lizenzgeber und Lizenznehmer bezüglich dieser Software.
11. Dieser Lizenzvertrag unterliegt deutschem Recht.
12. Wenn eine Bestimmung dieses Lizenzvertrages nichtig ist, wird dadurch die Gültigkeit der verbleibenden Bestimmungen dieses Lizenzvertrages nicht berührt. Diese nichtige Bestimmung wird durch eine gültige, in Übereinstimmung mit den gesetzlichen Vorschriften stehende Bestimmung mit ähnlicher Absicht und ähnlichen, wirtschaftlichen Auswirkungen ersetzt.
13. Der Lizenzvertrag kommt durch Übergabe der Software von dem Lizenzgeber an den Lizenznehmer und/oder durch den Gebrauch der Software durch den Lizenznehmer wirksam zustande. Dieser Lizenzvertrag ist auch ohne die Unterschrift des Lizenzgebers gültig.
14. Die Lizenz erlischt automatisch, wenn der Lizenznehmer den hier beschriebenen Lizenzbestimmungen nicht zustimmt oder gegen die Lizenzbestimmungen dieses Lizenzvertrages verstößt. Bei Beendigung ist der Lizenznehmer verpflichtet, sowohl die Software als auch sämtliche Kopien der Software in bereits installierter Form oder gespeichert auf einem Datenträger zu löschen, zu vernichten oder der MAGNA Telemotive GmbH zurück zu geben.
15. Der Lizenznehmer haftet für alle Schäden, welche dem Lizenzgeber durch die Verletzung dieses Lizenzvertrages entstehen.

2 PRODUKTHAFTUNG

Die Allgemeinen Verkaufs- und Lieferbedingungen der MAGNA Telemotive GmbH finden Sie auf unserer Webseite (<https://telemotive.magna.com>) im Impressum

3 Übersicht

Diese Anleitung beschreibt die Funktion der Lizenz **WLAN** für die Datenlogger

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

der MAGNA Telemotive GmbH.

Folgende Optionen sind mit dieser Funktion möglich:

- Aufbauen einer drahtlosen Verbindung mit dem Logger
- Konfigurieren des Datenloggers über die WLAN-Verbindung
- Herunterladen der Daten über die WLAN-Verbindung
- Auslesen der aktuellen Konfiguration über die WLAN-Verbindung
- ab Firmware Release 3.1.1 ist auch ein Zugriff auf einen TSL-Verbund möglich

Es werden die Konfiguration und Anwendung dieser Funktion beschrieben. Für allgemeine Punkte wird auf die Benutzerhandbücher des verwendeten Datenloggers, sowie des gemeinsam gültigen System Client verwiesen.

Dieses Dokument bezieht sich auf die **Firmware Version 03.04.03** und den **System Client** ab **Version 3.4.3**. Einige Eigenschaften und Funktionen variieren je nach Modell und installierter Lizenz oder stehen in älteren Versionen nicht zur Verfügung.

Software-Updates und Anleitungen für andere, optional erhältliche, lizenzpflichtige Erweiterungen stehen im Service Center der MAGNA Telemotive GmbH zur Verfügung (*Adresse siehe unter Kontakt auf der letzten Seite*).

Um einen möglichst zuverlässigen Betrieb Ihres Systems zu gewährleisten, stellen Sie bitte sicher, dass Sie immer eine aktuelle Version der Firmware und Software verwenden.

Bitte beachten Sie diese wichtigen Hinweise zum Betrieb von Geräten der MAGNA Telemotive GmbH!

Auf den Geräten läuft ein Linux-System und wenn dieses z.B. durch Unterspannung oder „spontanes“ Abziehen der Spannungsversorgung plötzlich zum Abstürzen gebracht wird, kann es passieren, daß das System danach nicht mehr richtig funktioniert. Sie kennen so ein Verhalten von einem PC, der nach mehreren Abstürzen nicht mehr korrekt funktioniert.

In den meisten Fällen kann so ein Fall vom System abgefangen und repariert werden, aber es kann auch passieren, dass das System danach korrupt, und das Gerät dadurch nicht mehr einsatzbereit ist.

In die Firmware sind und werden kontinuierlich weitere Funktionen integriert, die solche Situationen abfangen/reparieren. Fast bei jeder neuen Firmware werden einige weitere Mechanismen implementiert, die Systemfehler nach Spannungseinbrüchen abfangen und die Systemstabilität nach solchen Abstürzen verbessern. Aber solche Systeme können nicht zu 100 % gegen solche Einflüsse geschützt werden.

Bitte fahren Sie die Geräte daher immer über die vorgesehenen Mechanismen herunter oder nutzen Sie die Funktion des eingebauten Ruhezustandes, in den die Geräte gehen, wenn über eine einstellbare Zeitspanne keine Daten eintreffen.

[Index](#)

4 Systemvoraussetzungen

Kontrolleinheit

Um die Geräte mit dem **System Client** konfigurieren zu können, ist ein PC oder Laptop mit Windows nötig. Damit können später auch die aufgezeichneten Daten vom Datenlogger heruntergeladen und offline (ohne angeschlossenen Datenlogger) weiterverarbeitet werden.

System Client

Der System-Client ermöglicht die Konfiguration der Geräte sowie das Herunterladen und Konvertieren der aufgezeichneten Daten. Ein Firmwareupdate der Geräte kann ebenfalls durch den **System Client** erfolgen, damit Ihre Geräte immer auf dem neusten Stand sind.

blue PiraT2 / blue PiraT2 5E / blue PiraT Mini

Die Buskommunikation zwischen den Steuergeräten und Busteilnehmern wird von den Datenloggern der MAGNA Telemotive GmbH sehr präzise aufgezeichnet. Die aufgezeichneten Daten können über Ethernet von den Datenloggern heruntergeladen und z. B. auf einem Testrechner analysiert werden.

Der blue PiraT2 ist unser All-in-one-Datenlogger der Spitzenklasse. Sieben Modelle decken alle relevanten Schnittstellen ab.

Der **blue PiraT2 5E** bietet zusätzlich optimiertes Power Management mit Power Backup, fünf eingebaute Ethernet-Buchsen sowie besonders schnelles Aufstarten. Der **blue PiraT2 / 5E** ist über [System Link](#) flexibel erweiterbar.

Der blue PiraT Mini ist der weltweit kleinste Datenlogger mit diesem herausragenden Funktionsumfang. Er punktet mit weitreichender Schnittstellenabdeckung, stabilem Temperaturverhalten, sehr geringem Energieverbrauch, 4-fach GBit Ethernet und vielem mehr. Über [System Link](#) können mehrere unterschiedlicher blue PiraT Mini zu einem Gesamtsystem kombiniert, und so einfach verwaltet werden.

Remote Control Touch (optional)

Bedienen Sie Ihren blue PiraT Mini oder blue PiraT2 sicher und komfortabel vom Fahrer- oder Beifahrersitz aus. Über System Link wird unsere neue Fernbedienung Teil Ihres Logger-Netzwerks. Eine Fernbedienung kann so alle verbundenen Logger bedienen.

blue PiraT Remote (optional)

Während die Remote Control Touch eine reine Fernbedienung zur Verwaltung einzelner Geräte oder eines TSL Verbundes ist, bietet der blue PiraT Remote zusätzliche Loggerfunktionalität durch einen internen Speicher und einige Schnittstellen an.

Erweiterung

Der blue PiraT2 kann um ein internes GPS-/WLAN-Modul erweitert werden. Alternativ dazu kann beim blue PiraT2 / 5E und blue PiraT Mini, sowie beim blue PiraT Remote ein externer USB-Adapter angeschlossen werden. Beim blue PiraT Mini ist ein Adapterkabel von USB 2.0-Buchse A auf USB 2.0-Stecker-Micro B notwendig. Unterstützt werden die Adapter:

- 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 (ab Release 3.3.1)

Technische Informationen zu den Adaptern finden Sie im Anhang.

Lizenz

Eine installierte Lizenz auf dem Datenlogger ist für die Benutzung des Zusatzfeatures WLAN notwendig. Einstellungen bei lizenzierten Features können nur mit einer gültigen Lizenz vorgenommen werden.

Sollten Sie eine entsprechende Lizenz für Ihr Produkt benötigen, wenden Sie sich bitte an unseren Vertrieb. (Adresse siehe Kontakt auf der letzten Seite)

4.1 Weiterführende Anleitungen

Außer dieser Anleitung finden Sie in unserem ServiceCenter unter <https://sc.telemotive.de/blue-pirat> Haupt-Anleitungen für den Client sowie für die einzelnen Datenlogger-Generationen.

Benutzerhandbuch für den System Client

https://sc.telemotive.de/4/uploads/media/TelemotiveSystemClient_Benutzerhandbuch.pdf

Benutzerhandbuch für den blue PiraT2 / blue PiraT2 5E

https://www.telemotive.de/4/uploads/media/blue_PiraT2_Benutzerhandbuch.pdf

Benutzerhandbuch für den blue PiraT Mini

https://www.telemotive.de/4/uploads/media/blue_PiraT_Mini_Benutzerhandbuch.pdf

Benutzerhandbuch für die Remote Control Touch

https://sc.telemotive.de/4/uploads/media/RCTouch_Benutzerhandbuch.pdf

Benutzerhandbuch für die blue PiraT Remote

https://sc.telemotive.de/4/uploads/media/blue_PiraT_Remote_Benutzerhandbuch.pdf

Um bei Bedarf schnell darauf zugreifen zu können, sind die wichtigsten Handbücher auch im Client verlinkt und über den Menüpunkt [Hilfe] direkt aus dem Client erreichbar:

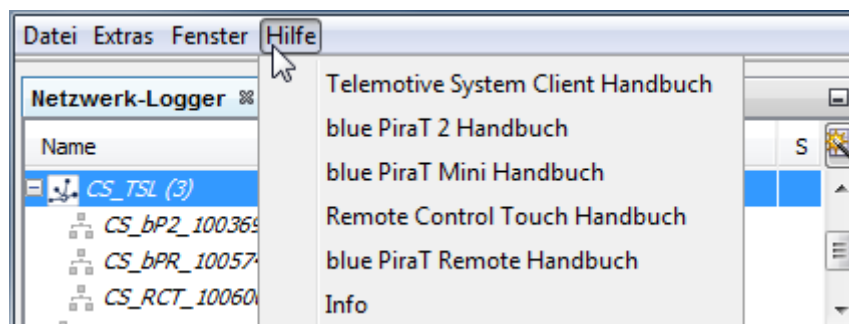


Abbildung 4.1: Verlinkung der Handbücher im Client

Für lizenzpflichtige Erweiterungen stehen im Service Center separate Anleitungen zur Verfügung. Eine Liste der lizenzpflichtigen Zusatzfunktionen finden Sie in den Benutzerhandbüchern im Kapitel **Zusätzliche Funktionen über optionale Lizenzen**.

4.2 Zusätzliche Funktionen über optionale Lizenzen

Zusätzliche Funktionen können durch den Kauf von Lizenzen und deren Installation aktiviert werden. Diese Lizenzen sind über unseren Vertrieb zu beziehen. Für jede lizenzpflichtige Zusatzfunktion finden Sie eine komplette Anleitung in unserem Service Center. Derzeit stehen folgende Lizenzen zur Verfügung.

Funktion	Beschreibung
Kameraanbindung	Video-Aufnahme über Videosever oder Netzwerk-Kameras
WLAN	Unterstützung von W-LAN (802.11, 802.11a, 802.11n), (802.11ac ab FW 02.04.01)
GPS Logging	Tracking der GPS-Daten
Messungen mit CCP	CAN Calibration Protocol
Messungen mit XCP	Universal Measurement and Calibration Protocol, Aktuell ist die Funktionalität für Ethernet (XCP on Ethernet) und den CAN-Bus (XCP on CAN) verfügbar.
MOST150 Streaming	Logging MOST150 synchronous / isochronous Daten
MLBevo	Mit der Lizenz Connected-Gateway MLBevo können Sie Daten des ATOP Steuergerätes MLBevo über USB auf den Telemotive Datenloggern aufzeichnen und später mit dem System Client konvertiert werden. (ab FW 02.01.01)
Download Terminal	Das Download Terminal erlaubt eine automatisierte Abarbeitung von konfigurierten Aufgaben für festgelegte Geräte-Gruppen. (ab FW 02.03.01)
TPE	TPE = Telemotive Performance Extension Erhöhung der Aufzeichnungsrate für Ethernet-Daten auf bis zu 100Mbit/s (ab FW 02.04.01)
Testautomatisierung	Schnittstelle zur Anbindung von Testautomatisierungs-Werkzeugen. Aktuell wird das Senden von CAN-Nachrichten unterstützt. (ab FW 02.04.01)
Mobilfunk	Ermöglicht das Versenden von Statusmeldungen des Loggers über das Mobilfunknetz. (ab FW 03.01.01)

Tabelle 4.1: Zusätzliche Funktionen über optionale Lizenzen

4.3 Firmware Care

Die MAGNA Telemotive GmbH investiert sehr viel in die Weiterentwicklung Ihrer Produkte.

Hierzu werden regelmäßig neue Funktionen und Erweiterungen über Firmware- und Client-Releases zur Verfügung gestellt.

Wichtigste Eckpunkte

Im Rahmen des Service Produkts „Firmware Care“ werden neue Software und Firmware Versionen zeitlich limitiert als Download zur Verfügung gestellt. Ab Kaufdatum des **blue PiraT Rapid** steht Ihnen dieser Service für 12 Monate zur Verfügung. Dieser Zeitraum ist verlängerbar.

Für Details wenden Sie sich bitte an Ihren Vertriebspartner (Adressen siehe Kontakt am Ende des Handbuchs).

Betroffene blue PiraT Produkte

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

Zu beachten:

Erweiterungen sind nur in der aktuellen Firmware möglich.

Achtung:

Bitte beachten Sie, dass Firmware-Updates für neue Hauptversionen (04.00.01 / 05.00.01) lizenzpflichtig sind und NICHT auf Geräte ohne entsprechende Lizenz aufgespielt werden können.

Sollten Sie eine entsprechende Lizenz für Ihr Produkt benötigen, wenden Sie sich bitte an unseren Vertrieb unter TMO.Sales@magna.com. (Adresse siehe unter Kontakt auf der letzten Seite)

5 Konfiguration

Hinweis:

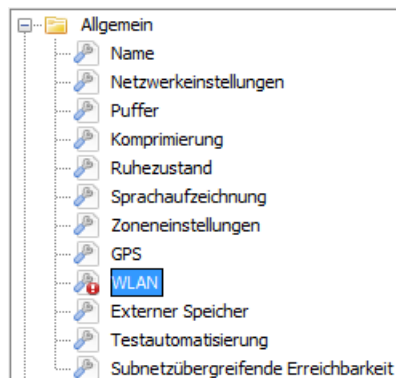
Alle Änderungen die am Logger vorgenommen werden, müssen mit [Zum Logger senden] auf den Logger übertragen werden. Wenn Änderungen erst nach Gerätereustart wirksam werden, meldet es die Client-Software und bietet Ihnen den Neustart an.

Um die WLAN-Funktion (Managed / Master) konfigurieren zu können, ist eine Verbindung des Datenloggers mit dem System Client auf dem PC notwendig. Bitte verbinden Sie den Datenlogger mit dem PC. Wenn Sie den Datenlogger zum ersten Mal für WLAN konfigurieren, ist eine Verbindung über ein LAN-Kabel notwendig. Später können dann Änderungen über eine bestehende WLAN-Verbindung gemacht werden.

Starten Sie den System Client und wählen Sie im Fenster <Netzwerk-Logger> den Datenlogger. Starten Sie die Applikation **[Konfiguration anzeigen] 5**.



Öffnen Sie im Konfigurationsbaum den Ordner **[Allgemein]** und wählen Sie den Unterpunkt **[WLAN]**.



Aktivieren Sie das Kontrollkästchen **WLAN aktiv** auf der rechten Seite.

<input checked="" type="checkbox"/> WLAN aktiv		
Betriebsart:	Master	Zone: Deutschland Gehe zu Zoneinstellungen
Kanal:	1	Kanalbereich: <input checked="" type="radio"/> IEEE 802.11bgn 2.4GHz <input type="radio"/> IEEE 802.11a/n/ac 5GHz
Netzwerk Name (ESSID):	<input type="text"/>	
Authentifizierungs-Modus:	WPA-PSK (WPA oder WPA2)	
Verschlüsselungstyp:	passphrase	
Schlüssel:	<input type="text"/>	<input type="checkbox"/> Schlüssel anzeigen
DHCP-Einstellungen		
DHCP-Modus:	DHCP-Client	
IP-Adresse des Datenloggers:	192 . 168 . 2 . 1	(Default: 192.168.2.1)
Subnetzmaske des Datenloggers:	255 . 255 . 255 . 0	(Default: 255.255.255.0)

Abbildung 5.1: WLAN-Konfiguration

Ist WLAN auf dem Datenlogger aktiv, werden die angeschlossenen Module automatisch vom Gerät erkannt und aktiviert.

5.1 Betriebsarten

Wählen Sie aus dem Dropdown-Menü den Betriebsmodus aus. Es gibt zwei verschiedene Möglichkeiten die WLAN-Funktion des Datenloggers zu verwenden.

5.1.1 Managed

Der Standard ist die Verwendung des Datenloggers im „Infrastructure“ Modus (**[Managed]** Modus). In diesem Modus wird der Datenlogger in die bestehende Netzwerk-Infrastruktur integriert.

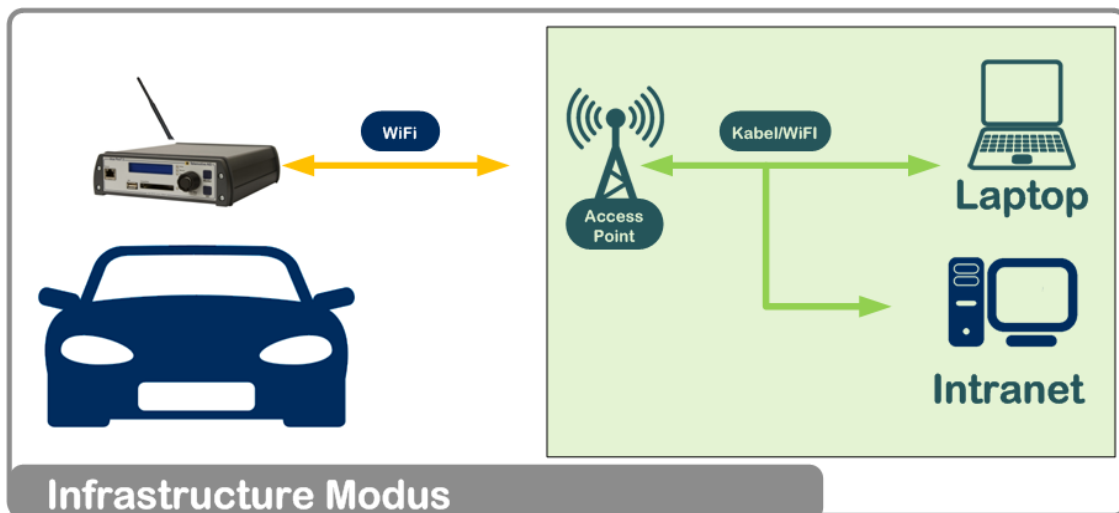


Abbildung 5.2: Managed oder „Infrastructure“ Modus

5.1.2 Master

Im **[Master]** Modus übernimmt der Logger die Rolle des Access Points. Endgeräte (Laptops, Smartphones) können direkt mit dem Logger verbunden werden und dessen DHCP-Dienste verwenden.

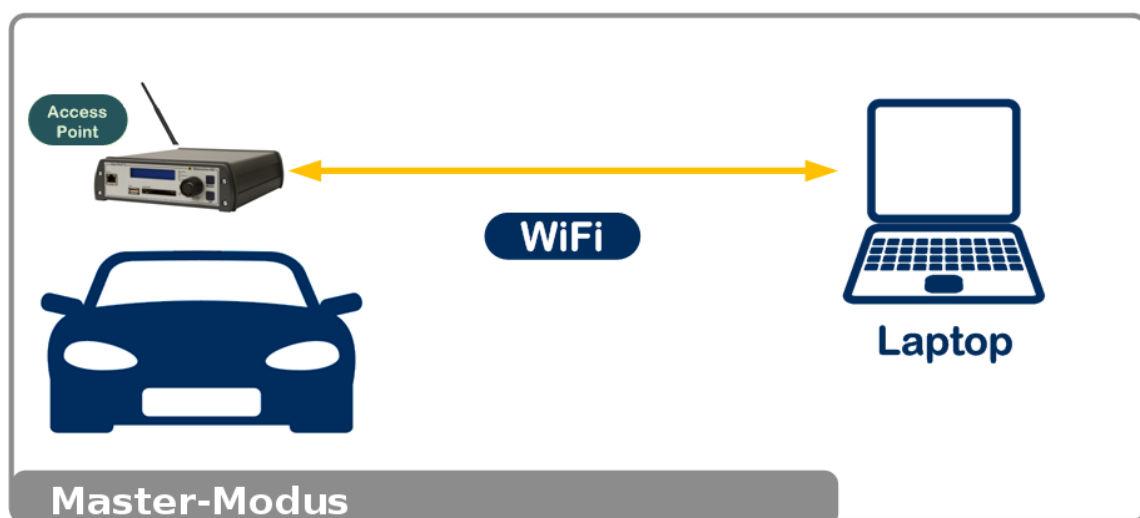


Abbildung 5.3: „Master“ Modus

5.2 Kanal

In der Betriebsart **[Master]** können Sie in einen anderen WLAN-Funkkanal wechseln. Wählen Sie einen Kanal, der möglichst weit von anderen WLAN-Netzen in Ihrer Umgebung entfernt ist.

The screenshot shows a configuration panel for WLAN settings. At the top, there is a checkbox labeled 'WLAN aktiv' which is checked. Below it, there are three dropdown menus: 'Betriebsart' (Operating Mode) set to 'Master', 'Kanal' (Channel) set to '1', and 'Netzwerk Name (ESSID)' (Network Name) set to 'Telemotive'.

Abbildung 5.4: Kanal eingeben

5.2.1.1 WLAN-Standard Auswahl

Ab der Firmware Version 2.4.1 wird in der Betriebsart **[Master]** auch der WLAN-Standard 802.11ac unterstützt.

In den WLAN-Einstellungen können sie nun den entsprechenden Standard, den Ihr WLAN-Modul unterstützt auswählen.

The screenshot shows a configuration panel for WLAN settings. At the top, it says 'Zone: Deutschland' with a link 'Gehe zu Zoneneinstellungen'. Below that, there are two radio button options for 'Kanalbereich' (Channel Range): 'IEEE 802.11bgn 2.4GHz' (which is selected) and 'IEEE 802.11a/n/ac 5GHz'.

Abbildung 5.5: WLAN Standard-Auswahl

5.3 Netzwerk Name (ESSID)

Der Netzwerk Name kann individuell vom Benutzer gesetzt werden.

Managed:

Für den Managed Modus muss die ESSID (Netzwerk Name) des Funknetzwerkes eingegeben werden, mit dem der Logger verbunden werden soll.

Master:

Hier kann der Benutzer die ESSID frei konfigurieren, um sich später mit dem Datenlogger manuell zu verbinden.

The screenshot shows a configuration panel for WLAN settings. At the top, there is a checkbox labeled 'WLAN aktiv' which is checked. Below it, there are five dropdown menus: 'Betriebsart' (Operating Mode) set to 'Master', 'Kanal' (Channel) set to '1', 'Netzwerk Name (ESSID)' (Network Name) set to 'Telemotive', 'Authentifizierungs-Modus' (Authentication Mode) set to 'WPA-PSK (WPA oder WPA2)', and 'Verschlüsselungstyp' (Encryption Type) set to 'passphrase'.

Abbildung 5.6: Netzwerk Namen eingeben

5.4 Authentifizierungs-Modus

Wenn Sie die Betriebsart **[Managed]** einstellen, wählen Sie den Authentifizierungs-Modus, welcher von Ihrem Access Point (AP) verwendet wird.

Für die Betriebsarten **[Master]** steht nur der Authentifizierungs-Modus, **WPA-PSK (WPA oder WPA2)** zur Verfügung welcher für die Verbindung zwischen Logger und Endgerät verwendet werden kann.

Folgende Authentifizierungs-Modi können verwendet werden.

5.4.1 Authentifizierung über WPA-PSK

WPA-PSK (WPA oder WPA2): PSK = Pre Shared Key

Der Schlüssel des Benutzers ist im Voraus bekannt. Die Schlüssel werden vor der Kommunikation ausgetauscht. Der gesicherte Schlüssel muss mit dem übertragenen Schlüssel übereinstimmen.

The screenshot shows a configuration form for WLAN. At the top, there is a checkbox labeled 'WLAN aktiv' which is checked. Below it, there are several fields: 'Betriebsart:' with a dropdown menu set to 'Managed'; 'Netzwerk Name (ESSID):' with a text input field containing 'Telemotive'; 'Authentifizierungs-Modus:' with a dropdown menu set to 'WPA-PSK (WPA oder WPA2)'; 'Verschlüsselungstyp:' with a dropdown menu set to 'passphrase'; and 'Schlüssel:' with a text input field that is currently empty and has a red error icon to its left. To the right of the 'Schlüssel:' field is a checkbox labeled 'Schlüssel anzeigen' which is unchecked.

Abbildung 5.7: Authentifizierungs-Modus WPA-PSK

5.4.2 Authentifizierung über WPA-EAP | Nur in Betriebsart [Managed]

WPA-EAP: EAP = Extensible Authentication Protocol
Bei EAP erfolgt die Aushandlung des konkret eingesetzten Authentifizierungs-Mechanismus erst während der Authentifizierungsphase. EAP ist heute weit verbreitet und wird von unterschiedlichen Transportprotokollen unterstützt.

The screenshot shows a configuration form for WLAN. At the top, there is a checkbox labeled 'WLAN aktiv' which is checked. Below it, there are several fields: 'Betriebsart:' with a dropdown menu set to 'Managed'; 'Netzwerk Name (ESSID):' with a text input field containing 'Telemotive'; 'Authentifizierungs-Modus:' with a dropdown menu set to 'WPA-EAP'; 'Verschlüsselungstyp:' with a dropdown menu set to 'passphrase'; 'Benutzername:' with a text input field containing 'defaultUser'; and 'Schlüssel:' with a text input field that has a red error icon to its left and a single dot inside. To the right of the 'Schlüssel:' field is a checkbox labeled 'Schlüssel anzeigen' which is unchecked.

Abbildung 5.8: Authentifizierungs-Modus WPA-EAP


Bei Verwendung von WPA-EAP muss für die Authentifizierung ein Benutzername und ein Schlüssel eingegeben werden. Wird kein Benutzername eingegeben, wird der hostname des Gerätes verwendet.

Beim Wechsel auf den Authentifizierungs-Modus WPA-EAP erscheinen in der Konfiguration weitere Einstellungsmöglichkeiten:

Zusätzlich kann im WPA-EAP Modus der EAP-Authentifizierungsmodus gewählt werden. Die verfügbaren Einstellungen sind:

5.4.2.1 EAP-Authentifizierungsmodus: TLS

Beim EAP-Authentifizierungsmodus TLS kann der Verschlüsselungstyp [passphrase] oder [Hexadezimal] für den benötigten Schlüssel verwendet werden. Außerdem kann ein TLS-Zertifikat auf den Logger geladen werden. Diese Option ist nur bei Onlinekonfigurationen verfügbar!



The screenshot shows the 'EAP-Einstellungen' (EAP Settings) window. At the top, 'EAP-Authentifizierungsmodus' (EAP Authentication Mode) is set to 'TLS'. Below this, there is a section for 'TLS-Zertifikat' (TLS Certificate) with three rows: 'CA-Zertifikat (Server):', 'Client-Zertifikat:', and 'Client-Keyfile:'. Each row has a text input field and two buttons: 'Öffnen' (Open) and 'Entfernen' (Remove). Below the certificate section, 'Verschlüsselungstyp' (Encryption Type) is set to 'passphrase'. At the bottom, there is a 'Schlüssel:' (Key) text input field and a checkbox labeled 'Schlüssel anzeigen' (Show Key).

Abbildung 5.9: EAP-Authentifizierungsmodus TLS

5.4.2.1.1 Zertifikatstypen

CA-Zertifikat (Server)

Firmen internes Zertifikat (CA = Certificate Authority = Zertifizierungsstelle)

Client-Zertifikat

Geräte Zertifikat (kann für ein oder mehrere Geräte gültig sein)

Client-Key / Public-Key

Verschlüsselter Schlüssel fürs Client-Zertifikat

Schlüssel / Client-Key Passwort / Public-Key Passwort

Passwort zum Entschlüsseln des Client-Key / Public-Key

5.4.2.1.2 Anwendungsarten der Zertifikate

Wenn gerätespezifische Zertifikate im Radius Server definiert wurden:

- CA- und Client-Zertifikat, Client-Key und Client-Key Passwort
- Client-Zertifikat, Client-Key und Client-Key Passwort

Wenn keine gerätespezifischen Zertifikate definiert wurden:

- CA-Zertifikat

Wenn keine Zertifikate vom Radius Server definiert wurden, dann braucht man auch keine.

5.4.2.2 EAP-Authentifizierungsmodus Tunnel TTLS

Abbildung 5.10: EAP-Authentifizierungsmodus Tunnel TTLS

Für Tunnel TTLS kann die Authentifizierung über ein TLS-Zertifikat oder ein Token realisiert werden, bei dem zusätzlich die Art des Authentifizierungstokens angegeben werden kann.

Abbildung 5.11: Tunnel TLS mit Token und Zertifikat

Wird als Authentifizierung TSL-Zertifikat ausgewählt, kann dieses zusätzlich auf den Logger übertragen werden.

Über die Schaltfläche [Entfernen] können die Zertifikate auch wieder gelöscht werden.

Abbildung 5.12: Tunnel TLS mit Token, Zertifikat und TLS-Zertifikat

5.4.2.3 EAP-Authentifizierungsmodus Tunnel PEAP

The screenshot shows the 'EAP-Einstellungen' (EAP Settings) window. The 'EAP-Authentifizierungsmodus' (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 'Authentifizierung' (Authentication), the 'Token' radio button is selected. The 'Authentifizierungstoken' (Authentication Token) is set to 'NONE'.

Abbildung 5.13: EAP-Authentifizierungsmodus Tunnel PEAP

Im Modus Tunnel PEAP kann zusätzlich zur Art des Authentifizierungstokens noch die PEAP Version sowie das PEAP Label angegeben werden:

The screenshot shows the 'EAP-Einstellungen' window with the 'PEAP Version' dropdown menu open. The menu options are 'DEFAULT', 'PEAPv0', and 'PEAPv1'. The 'Authentifizierungsmodus' is 'Tunnel PEAP' and the 'Authentifizierungstoken' is 'NONE'.

Abbildung 5.14: Tunnel PEAP | PEAP Version

DEFAULT:

deaktiviert Benutzung der PEAP Version.

PEAPv0:

default: Wird am häufigsten benutzt

PEAPv1:

The screenshot shows the 'EAP-Einstellungen' window with the 'PEAP Label' dropdown menu open. The menu options are 'DEFAULT', 'CLIENT_EAP_ENCRYPTION', and 'CLIENT_PEAP_ENCRYPTION'. The 'Authentifizierungsmodus' is 'Tunnel PEAP' and the 'Authentifizierungstoken' is 'NONE'.

Abbildung 5.15: Tunnel PEAP | PEAP Label

DEFAULT:

deaktiviert Benutzung des PEAP Labels.

CLIENT_EAP_ENCRYPTION

default: altes Label: Wird am häufigsten benutzt

CLIENT_PEAP_ENCRYPTION

neue Label

Auch im Modus Tunnel PEAP kann für die Authentifizierung sowohl ein Token als auch ein TLS-Zertifikat genutzt werden.

EAP-Einstellungen

EAP-Authentifizierungsmodus: Tunnel PEAP

PEAP Version: PEAPv0

PEAP Label: CLIENT_EAP_ENCRYPTION

Authentifizierung: Token TLS-Zertifikat

Authentifizierungstoken: NONE

Abbildung 5.16: Tunnel PEAP | Token oder TLS-Zertifikat

Bei Verwendung des Tokens kann ebenfalls die Art des Authentifizierungstoken angegeben werden. Zur Auswahl stehen folgende Optionen:

EAP-Einstellungen

EAP-Authentifizierungsmodus: Tunnel PEAP

PEAP Version: PEAPv0

PEAP Label: DEFAULT

Authentifizierung: Token TLS-Zertifikat

Authentifizierungstoken: NONE

Zertifikat

CA-Zertifikat (Server):

Authentifizierungstoken-Dropdown: NONE, MSCHAP_V2, PAP

Abbildung 5.17: Tunnel PEAP | Token | Authentifizierungstoken

NONE

Keine Verschlüsselung.

Zertifikate sind hier optional.

MSCHAP_V2

Microsoft Challenge Handshake Authentication Protocol Version 2.

Zertifikate sind hier optional.

PAP

Password Authentication Protocol.

Zertifikate sind hier optional.

5.5 Verschlüsselungstyp

Wählen Sie einen der folgenden Verschlüsselungstypen.

Passphrase:

Sicherheitsschlüssel wird aus einem Passwort generiert. Die Zeichenlänge des Schlüssels muss zwischen 8 und 64 liegen.

Hexadecimal:

Sicherheitsschlüssel muss eingestellt werden und wird in Hexadezimal-Zeichen angezeigt.

The screenshot shows a configuration window for WLAN. The 'WLAN aktiv' checkbox is checked. The 'Betriebsart' is set to 'Master', 'Kanal' to '1', and 'Netzwerk Name (ESSID)' to 'Telemotive'. The 'Authentifizierungs-Modus' is 'WPA-EAP'. The 'Verschlüsselungstyp' dropdown menu is open, showing 'passphrase' selected and 'hexadecimal' as an alternative option. The 'Benutzername' field is empty.

Abbildung 5.18: Verschlüsselungstyp wählen

5.6 Schlüssel

Der Schlüssel wird durch den Benutzer gesetzt. Rote Symbole mit Ausrufezeichen und eine Hinweismeldung zeigen an, wenn ein falscher Schlüssel gesetzt wurde.

Die Eingabe eines Schlüssels ist optional und nicht zwingend nötig.

The screenshot shows the same configuration window as in 5.18, but with the 'Schlüssel' field containing a single character. A red warning icon is present next to the field. Below the field, a message reads: 'Die Zeichenlänge des Schlüssels muss zwischen 8 und 64 liegen. Aktuell: 1'. The 'Schlüssel anzeigen' checkbox is unchecked. The 'DHCP-Einstellungen' section is expanded, showing 'DHCP-Modus' set to 'DHCP-Client', 'IP-Adresse des Datenloggers' as '192.168.2.1', and 'Subnetzmaske des Datenloggers' as '255.255.255.0'.

Abbildung 5.19: Warnung bei ungültigem Schlüssel

5.7 DHCP-Einstellungen

Der DHCP Modus für die WLAN Verbindung kann im unteren Bereich eingestellt werden.

DHCP-Einstellungen

DHCP-Modus: DHCP-Client

IP-Adresse des Datenloggers: 192 . 168 . 2 . 1 (Default: 192.168.2.1)

Subnetzmaske des Datenloggers: 255 . 255 . 255 . 0 (Default: 255.255.255.0)

Abbildung 5.20: DHCP Einstellungen für die WLAN Verbindung

Als DHCP Modus werden folgende Möglichkeiten angeboten:

DHCP-Client

DHCP deaktiviert

DHCP-Client

DHCP-Server

Abbildung 5.21: DHCP-Modus

DHCP Master kann nur in der Betriebsart [Master] verwendet werden.

5.8 Zoneneinstellungen

Über die Auswahl der betreffenden <Länderzone> können die Funkfrequenzen und die Sendeleistung eingestellt werden, die im jeweiligen Land eingehalten werden müssen.

Allgemein

- Name
- Netzwerkeinstellungen
- Puffer
- Komprimierung
- Ruhezustand
- Sprachaufzeichnung
- Zoneneinstellungen**
- GPS
- WLAN
- Externer Speicher
- Testautomatisierung
- Subnetzübergreifende Erreichbarkeit

Zoneneinstellungen

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

Automatisch auf Sommerzeit umstellen

Länderzone: Deutschland - DE

Abbildung 5.22: Konfiguration – Allgemein – Zoneneinstellungen

5.8.1 Beispiel: Verbindung eines Smartphones mit dem Logger

<input checked="" type="checkbox"/> WLAN aktiv		
Betriebsart:	<input type="text" value="Master"/>	Zone: Deutschland Gehe zu Zoneinstellungen
Kanal:	<input type="text" value="1"/>	Kanalbereich: <input checked="" type="radio"/> IEEE 802.11bgn 2.4GHz <input type="radio"/> IEEE 802.11a/n/ac 5GHz <input type="radio"/> IEEE 802.11a/n/ac 5.5GHz
Netzwerk Name (ESSID):	<input type="text" value="Telemotive"/>	
Authentifizierungs-Modus:	<input type="text" value="WPA-PSK (WPA oder WPA2)"/>	
Verschlüsselungstyp:	<input type="text" value="passphrase"/>	
Schlüssel:	<input type="text" value=""/>	<input type="checkbox"/> Schlüssel anzeigen
DHCP-Einstellungen		
DHCP-Modus:	<input type="text" value="DHCP-Client"/>	
IP-Adresse des Datenloggers:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="1"/>	(Default: 192.168.2.1)
Subnetzmaske des Datenloggers:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	(Default: 255.255.255.0)

Abbildung 5.23: Beispiel WLAN-Konfiguration

[Index](#)

6 Weitere Informationen und Einstellungen am Laptop/PC

Wenn die IP-Adresse/Subnetzmaske manuell gesetzt werden muss (z. B. wenn bei Nutzung der Betriebsart **[Ad-hoc]** oder kein DHCP-Service im Infrastruktur-Netzwerk verfügbar ist), öffnen Sie bitte den „Status von Drahtlosnetzwerkverbindung“ der WLAN-Netzwerkarte.

Die Einstellungen der WLAN-Karte können dann über die Schaltfläche **[Eigenschaften]** erreicht werden.

Hinweis: Für Änderungen sind Administrations-Rechte notwendig.

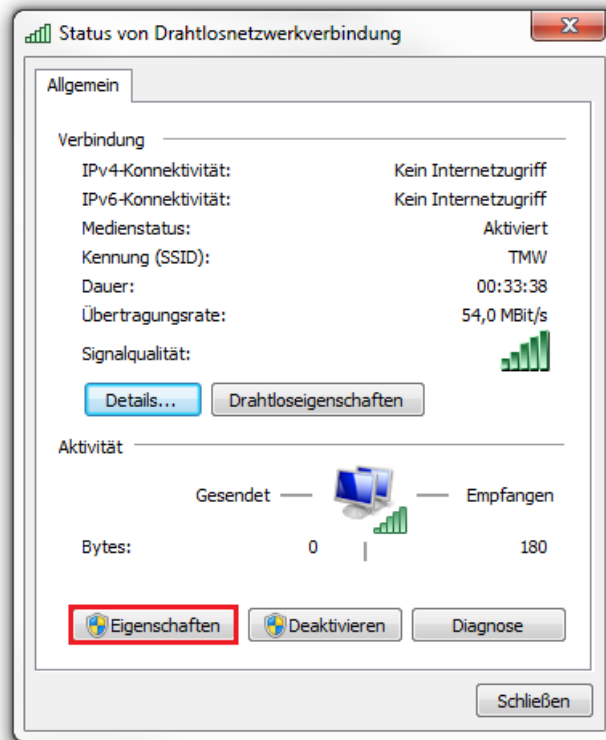


Abbildung 6.1: Status von Drahtlosnetzwerkverbindung

Jetzt können Sie Ihr TCP/IP-Protokoll wählen. Bitte stellen Sie sicher, dass Sie das richtige Kommunikationsprotokoll verwenden. **(TCP/IPv4)** Bei Bedarf kontaktieren Sie Ihren Netzwerk-Administrator.

Wählen Sie Ihr verwendetes WLAN-Protokoll an und klicken Sie auf die Schaltfläche **[Eigenschaften]**.

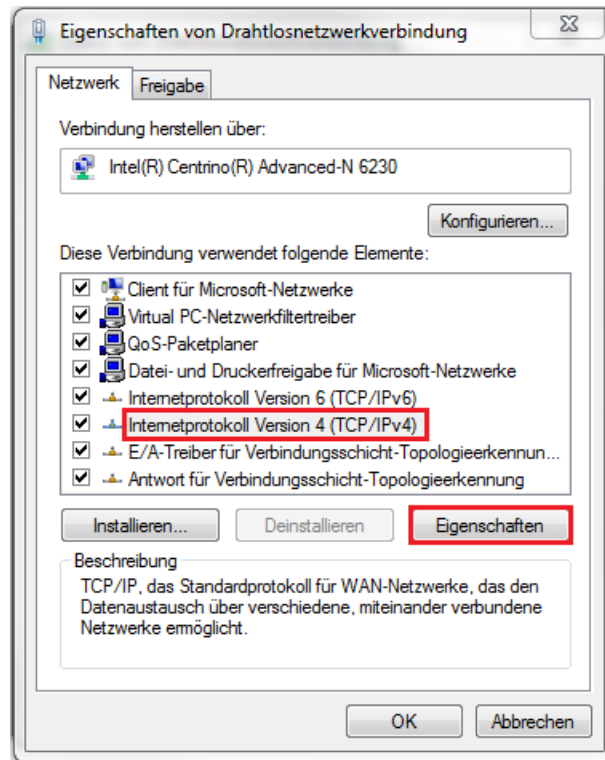


Abbildung 6.2: Eigenschaften von Drahtlosnetzwerkverbindung

Markieren Sie das Kontrollkästchen **Folgende IP-Adresse verwenden:**, um die IP-Adresse zu ändern. Erhöhen Sie die letzte Ziffer der IP-Adresse um 1 und geben Sie die Standard-Subnetz-Maske ein. Die Einstellungen für [Standardgateway] und [DNS] werden nicht verändert.

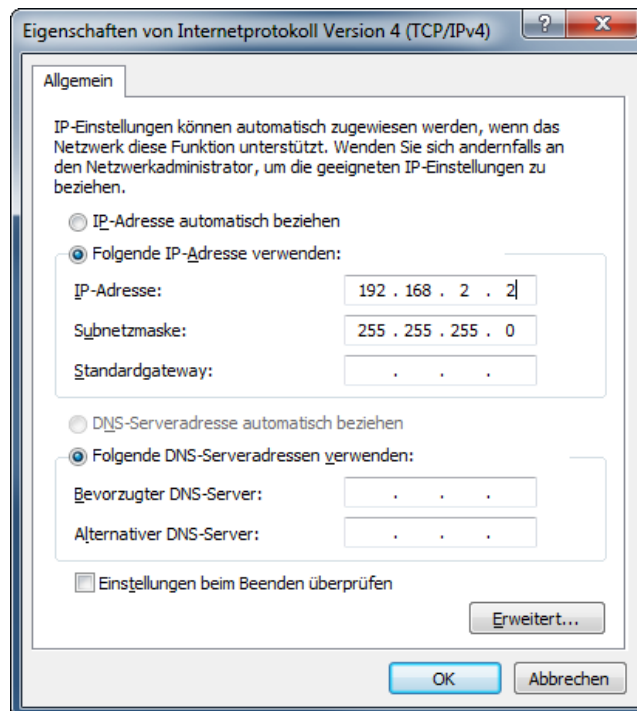



Abbildung 6.3: Eigenschaften von Internetprotokoll

7 Verbindung mit dem Datenlogger über WLAN

Schritt 1:

Verbinden Sie den PC/Laptop mit dem vorher konfigurierten Netz.

Schritt 2:

Öffnen Sie den System Client und schauen Sie in die Netzwerk-Logger-Liste. Bei erfolgreicher Verbindung zum Datenlogger oder TSL-Verbund über WLAN, erscheint der Logger in der Liste mit  Symbol.

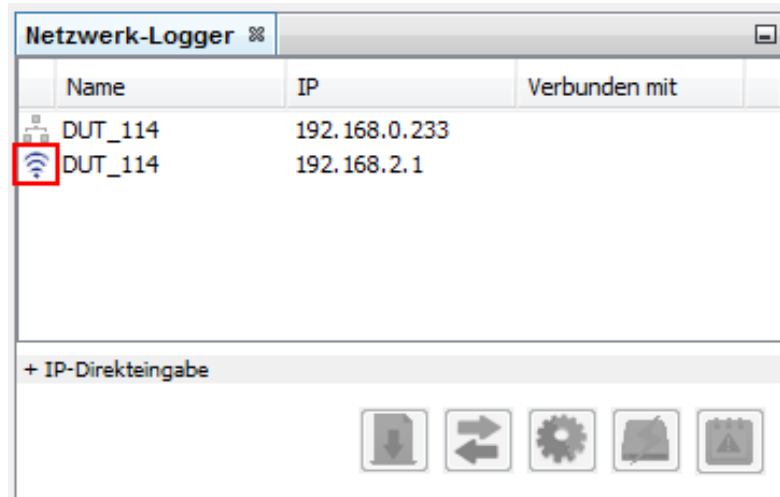


Abbildung 7.1: Reiter „Netzwerk-Logger“

8 Anhang | Technische Informationen zu den Adaptern

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.

Abbildung 8.1: Anhang | Technische Informationen zu den Adaptern

Hinweis: Der Netgear N300 wird aufgrund von Verbindungsabbrüchen nicht mehr empfohlen, und auch von uns nicht mehr vertrieben!

9 Abkürzungen

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 (www.mostnet.de)
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

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

Tabelle 9.1: Abkürzungen[Index](#)

10 Abbildungsverzeichnis

Abbildung 4.1: Verlinkung der Handbücher im Client.....	9
Abbildung 5.1: WLAN-Konfiguration	12
Abbildung 5.2: Managed oder „Infrastructure“ Modus	13
Abbildung 5.3: „Master“ Modus.....	13
Abbildung 5.4: Kanal eingeben.....	14
Abbildung 5.5: WLAN Standard-Auswahl	14
Abbildung 5.6: Netzwerk Namen eingeben.....	14
Abbildung 5.7: Authentifizierungs-Modus WPA-PSK	16
Abbildung 5.8: Authentifizierungs-Modus WPA-EAP	16
Abbildung 5.9: EAP-Authentifizierungsmodus TLS	17
Abbildung 5.10: EAP-Authentifizierungsmodus Tunnel TTLS	19
Abbildung 5.11: Tunnel TLS mit Token und Zertifikat	19
Abbildung 5.12: Tunnel TLS mit Token, Zertifikat und TLS-Zertifikat	19
Abbildung 5.13: EAP-Authentifizierungsmodus Tunnel PEAP	20
Abbildung 5.14: Tunnel PEAP PEAP Version	20
Abbildung 5.15: Tunnel PEAP PEAP Label	20
Abbildung 5.16: Tunnel PEAP Token oder TLS-Zertifikat	21
Abbildung 5.17: Tunnel PEAP Token Authentifizierungstoken	21
Abbildung 5.18: Verschlüsselungstyp wählen	22
Abbildung 5.19: Warnung bei ungültigem Schlüssel	22
Abbildung 5.20: DHCP Einstellungen für die WLAN Verbindung	23
Abbildung 5.21: DHCP-Modus.....	23
Abbildung 5.22: Konfiguration – Allgemein – Zoneneinstellungen	23
Abbildung 5.23: Beispiel WLAN-Konfiguration	24
Abbildung 6.1: Status von Drahtlosnetzwerkverbindung	25
Abbildung 6.2: Eigenschaften von Drahtlosnetzwerkverbindung.....	26
Abbildung 6.3: Eigenschaften von Internetprotokoll	26
Abbildung 7.1: Reiter „Netzwerk-Logger“	27
Abbildung 8.1: Anhang Technische Informationen zu den Adaptern	28

[Index](#)

11 Tabellenverzeichnis

Tabelle 4.1: Zusätzliche Funktionen über optionale Lizenzen.....	10
Tabelle 9.1: Abkürzungen.....	30
Tabelle 12.1: Versionshistorie	33

[Index](#)

12 Versionshistorie

Version	Änderung	Datum

Tabelle 12.1: Versionshistorie

13 Kontakt



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

MAGNA Telemotive GmbH

Büro München
Frankfurter Ring 115a
80807 München

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

Vertrieb
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.Produktsupport@magna.com
ServiceCenter: <https://sc.telemotive.de/bluepirat>