Renkforce

PL500D WiFi

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. The manufacturer shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from the manufacturer. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks

HomePlug® is a registered trademark of HomePlug Power Alliance.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

Wi-Fi®, Wi-Fi Protected Access™, WPA™, WPA2™ and Wi-Fi Protected Setup™ are registered trademarks of the Wi-Fi Alliance®.

The manufacturer's firmware package contains files which are covered by different licenses, in particular under manufacturer proprietary license and under open source license (GNU General Public License, GNU Lesser General Public License or FreeBSD License). The source code which is available for Open Source distribution can be requested in writing from gpl@gplrequest.com.

Subject to change without notice. No liability for technical errors or omissions.

April 2015

Contents

1 About the manual

Carefully read all instructions before setting up the device and store the manual and/or installation guide for later reference.

After a brief introduction to "PLC" and "WLAN“ basics and the presentation of the PL500D WiFi in Chapter 2, Chapter 3 will cover successfully setting up your adapter and integrate it in your network. Chapter 4 describes configuration options in detail for the built-in configuration interface, including access to the Wi-Fi. How you can manage the PL500D WiFi using the PLC configuration software is covered in Chapter 5. Tips for bandwidth optimization, information of environmental compatibility of the device and our warranty conditions can be found in Chapter 6 and conclude the manual.

1.1 Intended use

Use the adapter as described in these instructions to prevent damage and injuries.

The device is designed for indoor use only.

1.2 CE conformity

This product complies with the technical requirements of the directive 1999/5/EC (R&TTE) and the other relevant provisions of the FTEG, and it is designed for use in the EU, Norway and Switzerland. The product is class A equipment. Class A devices may cause interference when used in residential environments.

CE 0680

"99/05/CE" (R&TTE directive) is a directive similar to the EMC directive. It applies to radio equipment and telecommunication terminal equipment.Observance of these directives is verified by the use of harmonized European norms.

For the CE declaration for this product, refer to the accompanying product CD.

1.3 Safety notes

It is essential to have read and understood all safety and operating instructions before the device is used for the first time; keep them safe for future reference.

DANGER due to electricity

Users should never open devices. Opening the device poses a risk of electric shock!

Users do not need to carry out any maintenance on devices. In the event of damage, disconnect the device from the mains supply by pulling it or its plug out of the power outlet. Then contact qualified specialist personnel (after-sales service) exclusively. **Damage** is deemed to have occurred, for example,

- if the power cable or plug is damaged
- if the device has been showered with liquid (e.g. rain or water).
- if the device is inoperable.
- if the housing of the device is damaged.

Devices may only be operated using a **mains power supply**, as described on the **nameplate**.

To disconnect devices from the mains supply, pull the device itself or its mains plug from the power outlet. **The power outlet and all connected network devices should be easily accessible so that you can pull the mains plug quickly if needed.**

Devices are designed for indoor use only.

Only use devices at a dry location.

Disconnect devices from the mains supply to clean! Avoid solvent cleaning agents since they can cause damage to the housing. Only use a dry towel for cleaning.

DANGER due to overheating

Devices should only be installed at locations that guarantee adequate ventilation. Slots and openings on the housing are used for ventilation:

- Do not **cover** devices when operating.
- Do not place **any objects on** devices.
- Do not insert **any objects** into the **openings** of devices.

- Devices must **not** be placed directly **next to** an open **flame** (such as fire or candles).
- Devices must **not be exposed to direct heat radiation** (e.g. radiator, direct sunlight).

2 Introduction

This chapter gives an overview of the Powerline technology and briefly introduces the adapter. Practical examples are listed at the end of the chapter.

2.1 What does “Inhouse Powerline” stand for?

HomePlug (“Inhouse Powerline”, PLC) is an intelligent, secure technology that lets you set up a home network easily, quickly and economically via your electrical wiring, without the need for complex and expensive dedicated cabling. The available performance and effort required for the installation also compares favourably to traditional methods—Powerline technology now attains speeds you would expect from other LAN technologies.

2.2 What is WLAN?

WLAN (Wireless Local Area Network) refers to the use of radio technology to network computers and other devices. While it is possible to wirelessly connect computers in pairs (peer-to-peer, p2p), a central access point is required to set up a network of multiple devices. Such access points are frequently combined in a single device with modems for Internet access and routers to manage network traffic.

The wireless network established by an access point using a specific channel and name (SSID) has a limited range. The range of the access point, which is also known as a "radio cell", is impeded by building walls. In some cases, stable connections are often only possible between WLAN devices within a single room.

As it is not possible to rely on hardware such as network cables (in a LAN) or household wiring (in Powerline) to control access to a WLAN, wireless networking naturally presents special security challenges. WLANs therefore use a number of security measures, such as a concealed network name, data encryption and access control via the MAC addresses of the network adapters.

2.2.1 Wi-Fi or WLAN?

Wi-Fi is an invented brand name of the Wi-Fi Alliance, a consortium that certifies devices with wireless interfaces. In many countries, Wi-Fi is also used

synonymously with WLAN, which if taken strictly, is incorrect, because Wi-Fi designates the wireless standard and WLAN the wireless network.

2.3 The PL500D WiFi

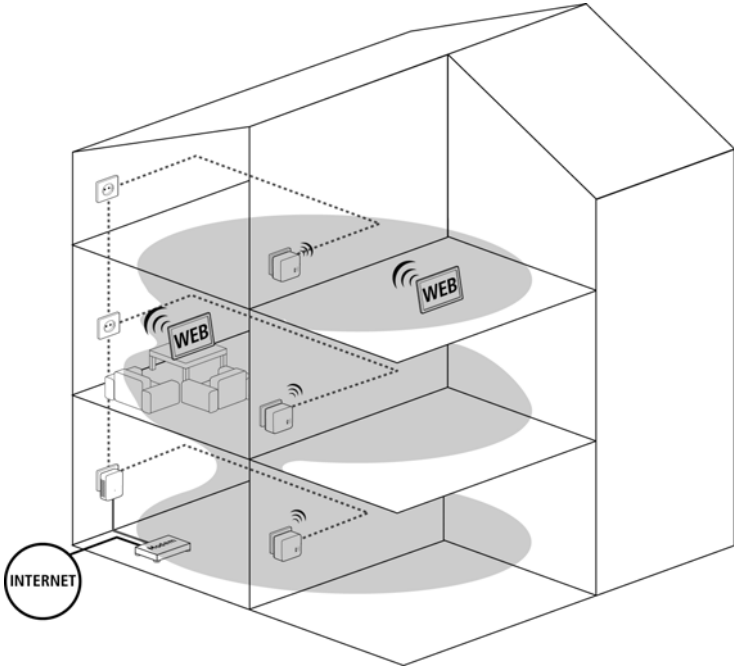
With the PL500D WiFi you can quickly and easily establish connections between WLAN, HomePlug (PLC) and LAN.

- As a WLAN access point, the adapter establishes communication between your WLAN devices and an existing LAN or PLC network. In this way, for example, you can expand your wireless network in no time to rooms that otherwise could not be reached by wireless.
- As a PLC device, the PL500D WiFi has one LAN jack for directly connecting a network device to the power lines.
- By combining the LAN, HomePlug and WLAN standards, you will become totally independent of existing network access points. Instead, you are completely free to connect all your devices either via a power supply socket, LAN or wirelessly. With WiFi Sync, you have optimal Wi-Fi reception for smartphones, laptops and tablets in the entire home—completely automatically (at least two PL500D WiFi required).
- Automatic encryption! Protection from unauthorised access at the touch of a button for HomePlug (AES)
- You can operate up to 8 adapters within one PLC network.

2.3.1 Example applications

PL500D WiFi completes your home network

On the one hand, you connect fixed network devices, such as computers and Internet access devices, by HomePlug. On the other hand, you include devices such as smartphones, laptops and tablets in your home network via Wi-Fi. Each additional PL500D WiFi (e.g. one on every storey) makes it easy for you to enable full Internet access everywhere in the home via Wi-Fi and/or HomePlug.



WiFi Move

Thanks to WiFi Move, an automatic synchronisation of the Wi-Fi settings takes place between all PL500D WiFi adapters, freeing you of the hassle of configuring of each individual PL500D WiFi.

3 Installation

This chapter describes the connection and display elements of the adapter and how to connect it.

3.1 Package contents

- Single:
  - Renkforce PL500D WiFi
  - Hard copy of installation guide
  - CD containing CE conformity, software and online documentation

or

- Kit:
  - Renkforce PL500D WiFi
  - PL500D duo
  - 1 Network cable
  - Hard copy of installation guide
  - CD containing CE conformity, software and online documentation

or

- Network:
  - Two Renkforce PL500D WiFi
  - PL500D duo
  - 1 Network cable
  - Hard copy of installation guide
  - CD containing CE conformity, software and online documentation

The manufacturer reserves the right to change the package contents without prior notice.

3.2 System requirements

- Operating systems: Windows Vista Home Premium (32 bit/64 bit), Windows 7 (32 bit/64 bit), Windows 8 (32 bit/64 bit), Windows 8 Pro (32 bit/64 bit) or any other operating system with network support
- Network connection

3.3 Connection and display elements

The PL500D WiFi has one Wi-Fi and one PLC button with LED status display, a network jack and a reset button.

3.3.1 Wi-Fi button

The Wi-Fi button controls the following Wi-Fi functions:

- **WLAN on/off**:
  - In the factory default settings, Wi-Fi is already enabled and Wi-Fi WPA2 encryption is configured. The default WiFi key for the initial installation of the PL500D WiFi is the adapter's WiFi key.

Before the networking procedure, take note of the WiFi key of the PL500D WiFi from which all Wi-Fi configurations are to be transferred to all other PL500D WiFi adapters. You will find the unique key on the label on the back of the housing.

  - In order to switch Wi-Fi off, press and hold the Wi-Fi button longer than 3 seconds.
  - In order to switch Wi-Fi back on, tap the Wi-Fi button.
- Wi-Fi network with WPS encryption
  - If the device is still on factory defaults, tap the Wi-Fi button in order to activate WPS.
  - If the Wi-Fi connection was switched off and you would like to activate WPS, press the Wi-Fi button twice; once to switch Wi-Fi on, and once to activate WPS.

WPS is one of the encryption standards developed by the Wi-Fi Alliance. The objective of WPS is to make it easier to add devices to an existing network. For more detailed information, refer to Chapter 'Wi-Fi Protected Setup (WPS)'.

- **Indicator lights**:
  The integrated indicator lights (LEDs) show all of the Wi-Fi statuses for the PL500D WiFi by illuminating and/or flashing:
  - When the Wi-Fi connection is switched off, the LED is also off.
  - When the Wi-Fi connection is switched on, the LED lights green.
  - WPS pairing is represented by quick flashing.

The LED status display can be deactivated on the configuration interface of the PL500D WiFi (see 'LED settings').

3.3.2 PLC button

The PLC button controls the following PLC functions:

- Encrypting the PLC network
  - To encrypt your PLC network individually, press each PLC encryption button on the connected devices for approx. 1 second within 2 minutes (see 'Connecting the adapter').
  - To remove a PLC device from your network, press the PLC encryption button on the corresponding device for at least 10 seconds (see 'Connecting the adapter').
- **Indicator lights**:
  The integrated indicator lights (LEDs) show all of the PLC statuses for the PL500D WiFi by illuminating and/or flashing:
  - The LED flashes slowly. There is no connection to the PLC network.

Check whether the adapter is connected to the mains supply correctly and whether the encryption process has been carried out successfully. For more information, refer to 'Connecting the adapter' and 'Network configuration'.

  - The LED lights green. The network connection is suitable for HD video streaming.
  - The LED lights orange. The network connection is suitable for SD video streaming and online gaming.
  - The LED lights red. The network connection is suitable for simple data transfer and Internet access.

The LED status display can be deactivated on the configuration interface of the PL500D WiFi (see 'LED settings').

• WiFi Move

WiFi Move is a function for synchronising the Wi-Fi settings of all PL500D WiFi adapters connected to your home network.

- Within 2 minutes first press the PLC button of the existing PL500D WiFi (approx. 1 second) and finish by pressing the PLC button of the new PL500D WiFi (approx. 1 second).
- The existing PL500D WiFi transmits its entire Wi-Fi configuration to the new PL500D WiFi adapter. The existing and the new PL500D WiFi adapters are now continuously connected with each other, and from now on exchange changes to the Wi-Fi configuration automatically with each other.

For more information on the WiFi Move, refer to Chapter 'WiFi Move'

3.3.3 Reset

The **Reset** button (next to the network jack) has two different functions:

- The device restarts if you press the Reset button for less than 10 seconds.
- To change the configuration of the PL500D WiFi back to the factory defaults, press the Reset button for more than 10 seconds. Keep in mind that all settings that have already been configured will be lost!

You can use the tip of a drawing pin to press the reset button.

3.3.4 Network connection

Via the LAN port, a computer or another network device can be connected to the PL500D WiFi via a commercially available network cable.

3.3.5 Wi-Fi antennas

The internal Wi-Fi antennas are for connecting to other network devices wirelessly.

3.4 Connecting the adapter

The device is designed for indoor use only.

Note the WiFi key of the PL500D WiFi before the networking procedure. You will find the unique adapter key on the label on the back of the housing.

In order to connect the PL500D WiFi to your laptop, tablet or smartphone later via WiFi, enter the noted WiFi key as the network security key.

In the following sections we describe how to connect the PL500D WiFi and integrate it into the network. We clarify the exact procedures based on potential network scenarios:

3.4.1 Single—Expanding an existing network

❶ Plug the PL500D WiFi into a wall socket. As soon as the indicator light of the PLC button lights green (after approx. 45 seconds), the adapter is ready to operate.

Note: The power outlet should be in range of the connected network device. The PL500D WiFi with the cable-based network device should be easy to access.
To switch off the PL500D WiFi or disconnect it from the mains supply, pull the power plug out of the power outlet.

Integrating the PL500D WiFi into an existing PLC network

❷ Before you can use the PL500D WiFi in your PLC network, first you have to connect it to your existing PLC devices as a network. This is accomplished by using a shared PLC password. This forms a delimited PLC network. Shared use of the PLC password is used both for access control for the PLC network and for encryption (and thus interception protection) of the transmitted data. The PLC password can be set in different ways:

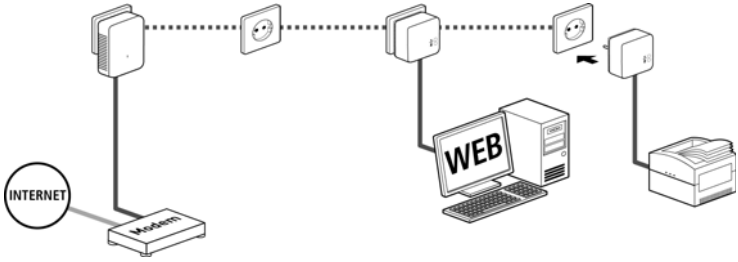
PLC network encryption at the touch of a button
First press the PLC encryption button (for about 1 second) on an adapter in your existing network and then, within 2 minutes, press the PLC encryption button (for about 1 second) on the new PL500D WiFi. The new PL500D WiFi is now integrated into your existing PLC network.

or

PLC network encryption using PLC configuration software. More information can be found in Chapter 'Encrypting the PLC network via the configuration software'.

or

PLC network encryption by entering the PLC password in the configuration interface. More information can be found in Chapter 'Device configuration'. .



Integrating the PL500D WiFi into an existing WiFi network

3. Establish the WiFi connection with your laptop, tablet or smartphone by entering the previously noted WiFi key as the network security key.

4. For the PL500D WiFi to show the same WiFi configuration as your WiFi router, you can apply the WiFi access data at the touch of a button. The WiFi Clone function can be enabled in different ways:

   Enabling WiFi Clone at the touch of a button
   First press the PLC encryption button on the front side of the PL500D WiFi and then press the WPS button on the WiFi router with the access data you want to apply.

   or

   Enabling WiFi Clone via the configuration interface. For more information about this function, refer to Chapter 'WiFi Clone'.

3.4.2 Kit and Network—Setting up a new PLC network

1. Connect the PL500D duo to your Internet access device's network jack.

2. Plug the PL500D WiFi into a wall socket. The adapter is ready to operate once the indicator light of the PLC encryption button turns white (after approx. 45 seconds).

To disconnect the adapter from the mains supply, unplug the device. The power outlet and all connected network devices should be easily accessible so that you can pull the mains plug quickly if needed.

Connecting a PL500D duo and a PL500D WiFi as a PLC network

❸ The factory default password of the adapters is HomePlugAV. For security reasons, we re-commend overwriting it and assigning a password of your own. The PLC password can be set in different ways:

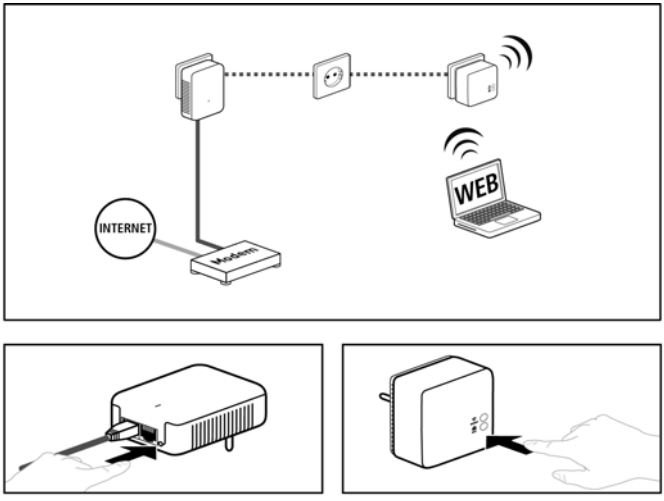
PLC network encryption at the touch of a button
First press the PLC encryption button (for about 1 second) of PL500D duo and then, within 2 minutes, press the PLC encryption button (for about 1 second) of PL500D WiFi. Your PLC network is now set up and protected against unauthorised access.

or

PLC network encryption using the configuration software. For more information, refer to Chapters 'Encrypting the PLC network via the configuration software'.

or

PLC network encryption by entering the PLC password in the configuration interface. More information can be found in Chapter 'Device configuration'.



Integrating additional PL500D WiFi adapters into a WiFi network

4. Establish the WiFi connection with your laptop, tablet or smartphone by entering the previously noted WiFi key as the network security key.

5. For the PL500D WiFi to show the same WiFi configuration as your WiFi router, you can apply the WiFi access data at the touch of a button. The WiFi Clone function can be enabled in different ways:

   Enabling WiFi Clone at the touch of a button
   First press the PLC encryption button on the front side of PL500D WiFi and then press the WPS button of the WiFi router with the access data you want to apply.

   or

   Enabling WiFi Clone via the configuration interface. For more information about this function, refer to Chapter 'WiFi Clone'.

6. First press the PLC encryption button (for about 1 second) on the existing WiFi adapter that has the entire WiFi configuration which is to be transferred to the new PL500D WiFi adapter now, and then press the PLC encryption button on the new PL500D WiFi (for about 1 second). The existing WiFi adapter transmits both the PLC as well as the entire WiFi configuration to the new PL500D WiFi adapter.

7. To integrate additional PL500D WiFi adapters into your WiFi-ac, repeat this step.

The WiFi adapters are now continuously connected to each other and, from now on, share changes to the WiFi configuration with each other automatically.

To customise your WiFi network security, install the configuration software and proceed with configuring your network. To do so, read Chapters 'Installing the software' and 'Network configuration'.

3.5 Installing the software

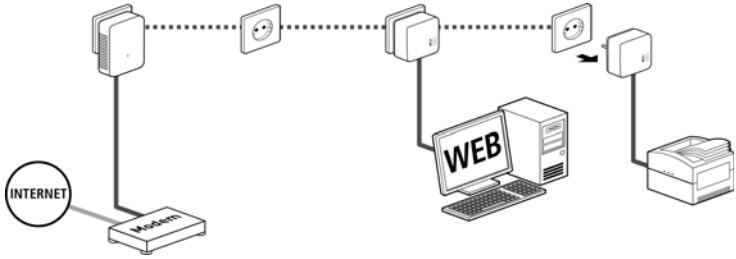
1. To install the software, insert the included CD-ROM in the CD drive of your computer. The installation wizard will guide you through the software installation.

❷ You can find the installed software applications in the Start -> All Programs -> PLC -> Access Manager.

❸ The Access Manager starts the integrated configuration interface of your PL500D WiFi. For more information on the configuration interface, please refer to Chapter 'Network configuration'.

3.6 Excluding the adapter from your network

To exclude an adapter from an existing network, press its PLC encryption button for at least ten seconds. The device will be assigned a new randomly generated password and will thus no longer be able to access the network. To integrate the adapter in a different PLC network, follow the steps described above, depending on whether you are setting up a new network or adding the adapter to an existing one.



4 Network configuration

The PL500D WiFi has a built-in configuration interface that can be called up using a standard web browser. Most settings for operating the device can be modified here.

4.1 Calling up the built-in configuration interface

Call up the built-in online configuration interface under Start -> All Programs -> PLC -> Access Manager.

4.2 Menu description

All menu functions are described in the corresponding interface as well as in the associated chapter in the manual. The sequence of the description in the manual follows the structure of the menu.

- Click Save to save the settings of the respective area of the configuration interface.
- Click Back to leave the respective area of the configuration interface.
- Select the desired language in the language selection list.

The four central areas of the configuration interface are displayed on the left edge. Click the button of an area to move directly into it.

- In the Status overview area, you get general information about all connected HomePlug, Wi-Fi and LAN devices.
- You can change or modify the various device settings for security, network, HomePlug and time under Device configuration.
- You can change or modify Wi-Fi settings in the WLAN configuration area.
- The Management section is for resetting, securing and restoring your individual configurations. In addition, you can update the firmware of your PL500D WiFi here.

4.3 Status overview

In the Status overview area you can track the status of your connected PLC, Wi-Fi and LAN devices.

4.3.1 PLC status

Here, you can see whether your devices are connected to a PLC network. To display all connected PLC devices, click either the house icon or the PLC devices arrow. Each connected PLC device, regardless of whether it is connected locally or remotely in the network, is displayed with its MAC address, name and type. Clicking the lock icon brings you directly to the PLC settings (see 'PLC settings').

You can add additional PLC devices to your PLC network by tapping on Add device. To do this, enter the security ID for the respective PLC adapter in the Security ID field and confirm with Save.

Before the networking procedure, note the security IDs of all PLC adapters. This unique identifier of each PLC device is located on the label on the housing. It consists of 4 x 4 letters separated by dashes (e.g. ANJR-KMOR-KSHT-QRUV). Ensure that all PLC adapters are connected to the power grid and computers or other network components as appropriate.

4.3.2 WLAN status

Here, you can see whether the Wi-Fi connection is switched on or switched off and whether Wi-Fi Move Technology is activated (see 'WiFi Move'). Clicking the Wi-Fi icon brings you directly to the WLAN configuration (see 'WLAN configuration'). Click on the WLAN monitor arrow to have all of the known Wi-Fi devices displayed. Each Wi-Fi station known since the last system start is displayed together with its name, MAC and IP address and the last login date, along with the speed if possible if there is an Internet connection and a time server was found.

Clicking the lock icon of the access point brings you directly to the Wi-Fi configuration area (see 'Access point'), where you can configure settings for Wi-Fi network security.

4.3.3 Ethernet status

The status of the network connection is displayed in this area.

4.4 Device configuration

In the device configuration area, you can modify settings for device security, network, HomePlug (PLC), date and time and LED.

4.4.1 Device security

In this area you can control the access to the configuration interface as well as enable and disable the functions of the interfaces and buttons on the PL500D WiFi.

Password

You can set a login password for access to the configuration interface.

By default, the built-in configuration interface of the PL500D WiFi is not protected with a password. However, we recommend assigning a password when the installation of the PL500D WiFi is complete to protect it against tampering by third parties.

1. To do so, first enter (if present) the current password and then enter the desired new password twice. Now the configuration interface is protected against unauthorised access with your individual password!
2. Call up the configuration interface again later.
3. Enter admin in the User name field and your individual password in the Password field.

The admin user name cannot be changed*.*

4.4.2 Network settings

The PL500D WiFi also communicates via the TCP/IP protocol as a component of your home network. The IP address required for this can either be entered manually or obtained automatically from a DHCP server.

The option Use this to accept network settings automatically from a DHCP server is enabled in the factory defaults.

If a DHCP server is already present in the network for giving out IP addresses, have the option Use this to accept network settings automatically from a DHCP server enabled so that the PL500D WiFi automatically receives an address from it.

You can also assign a static IP address by making entries under IP address (e.g. '192.168.0.249') and Netmask (e.g. 255.255.255.0).

If you happen to forget the IP address of your PL500D WiFi, proceed as described under 'Calling up the built-in configuration interface'.

4.4.3 PLC settings

In a PLC network, all connected components must use the same password. The PLC password can be defined with the PLC encryption button (see 'Configuring the PLC network'), by using the configuration software or at this location in the configuration interface. You can choose to configure the password locally or for the entire ("Total") network.

If you only change the password for a local device, you exclude it from your complete PLC network.

The PLC default password is HomePlugAV*.*

4.4.4 Time server

A time server is a server on the Internet whose task consists of providing the exact time.

The option Retrieve date and time automatically *is activated by default so that the PL500D WiFi can automatically synchronise the date and time.*

Select your Time zone and the Time server. If you have enabled the option Adjust to daylight saving time automatically, the PL500D WiFi automatically adjusts to daylight saving time.

Synchronisation with an Internet time server has to be ensured in order to use the Wi-Fi time control, for example (see 'WLAN time control'). In addition, the time server has to be activated, and an active Internet connection is also required.

4.4.5 LED settings

The LED status display can be deactivated by activating the function Disable all LEDs permantly in order to prevent unwanted lighting, for example, in the master bedroom.

The LED status display is activated in the factory default state.

4.5 WLAN configuration

In the WLAN configuration area, you can configure settings for the Wi-Fi network and its security.

If you would like, you can completely shut off the Wi-Fi part of your PL500D WiFi, e.g. if you want to operate it exclusively as a simple PLC device via the built-in Ethernet connections. There are three different methods for switching the Wi-Fi function on and off:

- Press the ON/OFF button on the front panel of the device.
- Use the Enable WLAN or Disable WLAN button on the configuration interface under WLAN configuration.
- Enable the Wi-Fi time control. For more information, refer to Chapter 'WLAN time control'.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the PL500D WiFi. In this case, configure the device via Ethernet or PLC.

The operating state of the device is displayed under 'Status overview'.

4.5.1 Access point

Since the PL500D WiFi acts as an access point, you have to configure various parameters for your wireless network.

When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.

In the factory defaults of the PL500D WiFi, the WLAN function is enabled and the WPA2 WLAN encryption is set with the security ID as the standard WLAN key. You will find the 16-character security ID on the label on the back of the housing.

The SSID specifies the name of your wireless network. You can see this name when logging onto the WLAN and thereby identify the correct subnet. If you enable the Hide SSID option, your wireless network remains hidden. In this case, potential network users must know the exact SSID and enter it manually to be able to set up a connection.

Some WLAN adapters have difficulty connecting to such hidden wireless networks. If the connection to a hidden SSID poses problems, first try to set up the connection with a visible SSID and only then try to hide it.

For operation as an access point, a (transmission) channel must be specified. There are 13 channels available. We recommend keeping the default setting Auto, since in this setting the PL500D WiFi selects the channel regularly and independently. In other words, if the last connected station logs out, a search for a suitable channel is carried out immediately. If no stations are connected, the device automatically selects a channel every 15 minutes.

Without encryption, not only are all data transmitted from client computers to the PL500D WiFi in your wireless network without protection, but there is also no password prompt to establish the connection. If no other security measures were set up, such as a WLAN filter (see Chapter 'WLAN filters'), third parties can gain access to your network at any time and, for example, share your Internet connection. Usually this happens without you noticing it.

To secure the data transmission in your wireless network there are two security standards available.

- The older and weaker WEP standard can protect communication with the help of a key having either 10 or 26 characters. To do so, enter a series of hexadecimal characters with the corresponding number of characters into the Key field.
- The state-of-the-art WPA and WPA2 (Wi-Fi Protected Access) methods allow individualised keys consisting of letters and numbers **and the displayed special characters** with a length of up to 63 characters. You can simply enter this using the keyboard, without having to convert it into hexadecimal format first (as with WEP). Under Mode, you can limit access of clients to the PL500D WiFi to the method you have selected.

Save all modified settings before leaving this configuration area again.

You should always encrypt the connections in your WLAN. Otherwise anyone within range could penetrate into your home network and, for example, share your Internet connection. Always select the better WPA2 encryption method if possible. Use WEP only if one of your wireless terminal devices does not operate with a better standard

4.5.2 Guest account

If you have friends or acquaintances visiting and you want to provide them with Internet access but without giving away the password for your Wi-Fi, you can set up a separate guest account in addition to the main Internet connection. The guest account can have its own SSID, time limit and Wi-Fi pass-

word. This way your visitors can surf the Internet without having access to your local network.

To set up a guest account, enable the Activate guest account option.

Define the name of the guest network in the SSID field (Service Set Identifier).

Automatic shutoff

If you would like to set a time limit for the guest account, enable the option Automatically shut off guest account after ... and enter the desired time limit.

Note that guest access is subordinated to the actual Wi-Fi configuration, and with it, is subject to the settings of the Wi-Fi time control. This means that guest access can only be used within the times that are defined for the PL500D WiFi under 'WLAN time control'.

Security

You should also encrypt the guest account to prevent anyone in signal range from intruding into your home network and sharing your Internet connection. WPA and WPA2 (Wi-Fi Protected Access) security standards are available for this.

WPA and WPA2 (Wi-Fi Protected Access) methods allow individualised keys consisting of letters and numbers **and the displayed special characters** with a length of up to 63 characters*. You can simply enter this using the keyboard, without having to convert it into hexadecimal format first. Under* Mode*, you can limit access to the PL500D WiFi to the method you have selected.*

4.5.3 WLAN filters

In addition to encryption (see Chapter 'Access point'), you can secure your wireless network even more by using a WLAN filter to limit access via WLAN to the PL500D WiFi for selected devices. Even if the encryption is switched off, the device will not establish a connection.

The WLAN filter should be used only as an additional option. By using it you could limit access to your wireless network, but without encryption it would be relatively easy for third parties to eavesdrop on all of your data transmissions.

To use the WLAN filter, enable the option Enable filters. Now you can enter various network devices by means of what is known as your MAC address for access to your PL500D WiFi. Confirm each entry with Add.

Approved Wi-Fi stations

Network devices or stations connected to your PL500D WiFi are automatically listed, that is, to enable an already connected station for the PL500D WiFi, simply select the MAC address of the respective device and confirm it with Add. This then appears under Approved WLAN stations. To remove an enabled station, select its MAC address and confirm it with Delete.

The Wi-Fi filter can only be set for stations connected directly to the access point (not the guest account).

The MAC address designates the hardware interface of each individual network device uniquely (e.g. the WLAN adapter of a computer or the Ethernet port of a printer). It consists of six double-digit hexadecimal numbers, each separated by a colon (e.g. 00:0B:3B:37:9D:C4). The MAC address is on the housing of the device..

You can easily determine the MAC address of a Windows computer by opening the window with the command prompt under Start -> All Programs -> Accessories -> Command Prompt. Enter the command IPCONFIG /ALL here. The MAC address is displayed under the designation Physical address.

After entering the MAC addresses, do not forget to click the Save button. If the entered values are incorrect (e.g. because the colons are missing), a corresponding error message is displayed.

Keep in mind that you also have to enter the MAC address of your own computer if you are connected to the PL500D WiFi not via the Ethernet port, but via WLAN. Otherwise you will block your own access to the device via WLAN by activating the WLAN filter!!

4.5.4 Parental controls

You can regulate Internet access for specific stations based on time using this function. For instance, to protect your children from excessive Internet use, you can define how long they may use the Internet per day.

Synchronisation with an Internet time server is necessary to be able to use the parental controls. In this case, the time server (Device configuration -> Date and time -> Obtain date and time automatically) for the PL500D WiFi has to be enabled and an active Internet connection is also required (see 'Time server'). The time server is enabled by default.

If you would like to set up a daily time quota, enable the option Turn on parental controls. Now enter the MAC addresses for the stations for which you would like to set up a time quota. You can enter the MAC addresses manually or select them from the list of currently known stations (WLAN status -> WLAN monitor). Confirm each entry with Add.

WLAN stations with time limit

Here you can find a list all of the Wi-Fi stations for which the Internet access time is limited.

Each station is displayed with its MAC address, name, time remaining and the specified time quota.

If you would like to delete a station from this list, highlight the station and confirm with Delete selected.

Clicking on Edit brings you to the settings menu for the time quota. If you would like the time quota to be monitored, enable the option The time limit will be monitored.

The daily time quota can be specified in hours and minutes.

A time quota can only be used if it matches the time periods defined in the WLAN time control and if the PL500D WiFi is enabled and there is an Internet connection. (see 'WLAN time control').

The time quotas for the parental controls are defined per day and the time periods for WLAN time control are defined per weekday.

If you expand an ongoing time quota, the change takes effect immediately; if you reduce an ongoing time quota, the change takes effect on the following day.

4.5.5 WLAN time control

*Synchronisation with an Internet time server has to be ensured in order to use Wi-Fi time control. In this case, the time server (*Device configuration -> Date and time -> Obtain date and time automatically*) for the PL500D WiFi*

has to be enabled and an active Internet connection is also required (see 'Time server'). The time server is enabled by default.

To be able to use the Wi-Fi time control, enable the option Enable time control. The time control automatically switches your wireless network on and off at certain times of the day.

You can define two time periods during which your wireless network is to be enabled for each weekday. Then the time control automatically switches the wireless network on or off.

Keep in mind that, as long as the PL500D WiFi registers connected stations, the wireless network remains enabled. The wireless network is not switched off until the last station has logged off.

Manually switching the access point on or off (i.e. using a button) always has priority over automatic time control. The configured time control would take effect automatically during the next defined time period.

4.5.6 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is one of the international encryption standards developed by the Wi-Fi Alliance for easily and quickly setting up a secure wireless network. The encryption keys of the respective WLAN client are transmitted automatically and continuously to the other WLAN client(s) of the wireless network. The PL500D WiFi offers two different variants for transmitting these encryption keys:

WPS via PBC (Push Button Configuration):

① Start the encryption process on the PL500D WiFi

- ○ either by pressing the WPS button on the front panel of the device or
- ○ by pressing the Start setup button on the user interface under WLAN configuration -> Wi-Fi Protected Setup (WPS).

② Then press either the WPS key of the WLAN client you are adding or the WPS button on the configuration interface. Now the devices exchange their encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

WPS via PIN:

① To interconnect WLAN clients securely in your wireless network via PIN variants, enter an individualised key in the configuration interface under WLAN configuration -> Wi-Fi Protected Setup (WPS) -> PIN and start the encryption process by pressing the Start setup button.

② Open the configuration interface of the WLAN client to be added and transmit the PIN selected on the PL500D WiFi. Confirm the encryption process as described there. Now the devices exchange their encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

The client can also create the PIN; this must then be entered onto the configuration interface of the PL500D WiFi.

Use of the WPS process implies either WPA or WPA2. For that reason, keep in mind the following automatic settings depending on the encryption standard (also refer to Chapter 'Access point'), i.e.

- if under WLAN configuration -> Access Point No encryption or WEP is selected in advance, WPA2 is set automatically. The newly generated password is displayed under WLAN configuration -> Access Point in the Key field.
- if under WLAN configuration -> Access Point WEP is selected in advance, WPA2 is set automatically. The newly generated password is displayed under WLAN configuration -> Access Point in the Key field.
- if under WLAN configuration -> Access Point WPA is selected in advance, this setting remains with the previously assigned password.
- if under WLAN configuration -> Access Point WPA2 is selected in advance, this setting remains with the previously assigned password.

4.5.7 WiFi Move

Wi-Fi Move Technology is a function for synchronising the Wi-Fi settings of all PL500D WiFi adapters connected to your home network.

WiFi Move support enabled

You can enable synchronisation of the WiFi settings either by using the functions in this menu or by pressing the respective PLC button on the corresponding adapters.

To learn how to synchronise the WiFi settings at the touch of a button, refer to Chapters 'Connecting the adapter'.

Switch on WiFi Move Technology (if necessary) by clicking/tapping under WLAN configuration d WiFi Move. All WiFi adapters are now continuously connected to each other and, from now on, share changes to the WiFi configuration with each other automatically.

In addition, you can see when the last synchronisation took place and which devices are connected via WiFi Move Technology.

4.5.8 WiFi Clone

WiFi Clone lets you apply the WiFi access data of an existing WiFi access point (such as your WiFi router) at the touch of a button. Start the procedure with the Start setup option and then press the WPS button of the device with the WiFi access data (SSID and WiFi password) to be applied.

4.6 Management

In the Management area you can reset the current configuration to the factory defaults, save it to your computer as a file or restore it from there and update the firmware of the PL500D WiFi.

4.6.1 Resetting the configuration

With the Management -> Reset configuration command, the PL500D WiFi is reset to the original factory defaults. In doing so, you lose your personal settings. The last-assigned PLC password for the PL500D WiFi is also reset to the PLC standard password HomePlugAV. To secure your PLC network individually again, reconfigure it by using either the encryption button (see Chapter 'Configuring the PLC network').

You can change the PLC password by using the configuration software under Device configuration -> PLC settings *or by using the* encryption button*.*

For backup purposes, all active configuration settings can be transmitted to your computer, stored there as a file and reloaded into the PL500D WiFi. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

4.6.2 Saving a configuration file

To save the active configuration to your computer as a file, select the corresponding button in the area Management -> Save configuration file. Then enter a storage location and name for the settings file.

4.6.3 Restoring a configuration

An existing configuration file can be sent to the PL500D WiFi in the area Management -> Restore device configuration and enabled there. Select a suitable file via the Browse... button and start the operation by clicking the Restore device configuration button.

4.6.4 Refresh firmware

The firmware of the PL500D WiFi includes the software for operating the device. If necessary, the manufacturer offers new versions on the Internet as a file download, for example to modify existing functions.

① To bring the firmware up to the latest version, first go to the website www.renkforce.com, and download the appropriate file for the PL500D WiFi to your computer.

② Then in the configuration dialogue, go to the area Management -> Update Firmware. Click Browse... and select the downloaded file.

③ Then start the update procedure with the Update Firmware button. After a successful update, the PL500D WiFi restarts.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the PL500D WiFi via PLC or LAN rather than WLAN.

5 Encrypting the PLC network via the configuration software

Upon successful installation, the configuration software can be found under Start --> All programs --> PLC --> Access Manager (see Chapter 'Installing the software').

- Scan for local adapter
  After launching the wizard, it initially scans for the local adapter connected directly to your computer.

Please note: You must connect every PLC device that you intend to integrate securely in your network directly to your computer for configuration.

- Assign a network password
  In this step, select a network password that will apply to all adapters in your home network. The password must be used by all devices.

The factory default password is HomePlugAV. For security reasons, we recommend overwriting it and assigning a password of your own.

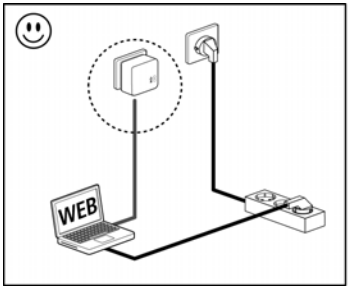
- Add further adapters
  To add a new adapter to your network, first connect it directly to your computer and launch the wizard again. Then assign the password that will apply to all adapters in your home network.

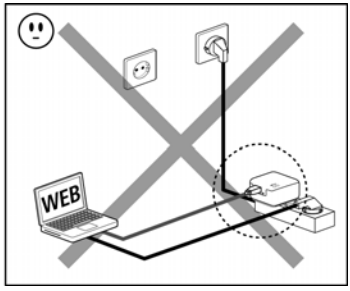
6 Appendix

6.1 Bandwith optimisation

To significantly improve the transmission capacity of the network, we recommend that you comply with the following "connection rules":

• Plug the device directly into a wall socket. Avoid extension strips.





• Plug the devices into different outlets and avoid using the same extension strip.

6.2 Disposal of old devices

The icon with crossed-out wastebasket on the device means that this adapter is an electrical or electronic device that falls within the scope of application of the German Electrical and Electronic Equipment Act. Since 24 March 2006, these types of devices may no longer be disposed of with household waste. Rather, in Germany, they can be given to a municipal collection point free of charge. Contact your municipal government to find out the address and hours of the nearest collection point.

6.3 Warranty conditions

The warranty is given to purchasers of the manufacturer's products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at the manufacturer's sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Alternatively, the manufacturer reserves the right to replace the defective product with a comparable product with the same specifications and features. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by the manufacturer, but not shipping and handling costs involved in transport from the buyer to the service station and/or to the manufacturer.

c) Replaced parts become property of the manufacturer.

d) The manufacturer is authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for this product is two years. This period begins at the day of delivery from the manufacturer's dealer. Warranty services carried out by the manufacturer do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the person carrying out the transportation and the sender should be informed immediately. On discovery of damage which is not externally visible, the transport company and the sender are to be immediately informed in writing, at the latest within 3 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if a copy of the original purchase receipt is returned with the device. The manufacturer reserves the right to require the submission of the original purchase receipt.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the label with the serial number has been removed from the device,

b) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

c) if the device was stored or operated under conditions not in compliance with the technical specifications,

d) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

e) if the device was opened, repaired or modified by persons not contracted by the manufacturer,

f) if the device shows any kind of mechanical damage, or

g) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable hardware, software, installation or operation, the manufacturer reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

a) The above conditions define the complete scope of the manufacturer's legal liability.

b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

d) The manufacturer is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

e) In the case that the intentional or culpable negligence of the manufacturer's employees has caused a loss of data, the manufacturer will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

f) The warranty is valid only for the first purchaser and is not transferable.

g) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, the manufacturer's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

h) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between the manufacturer and the purchaser.