dLAN® 500 AV Wireless+

devolo

The Network Innovation

devolo dLAN® 500 AV Wireless+

Contents

1 Preface

1.1 Thank you!

With the dLAN 500 AV Wireless+, you have chosen a HomePlug AV device that combines the advantages of the two network standards dLAN and WLAN. In addition, the dLAN 500 AV Wireless+ has three LAN ports for directly connecting computers or other network components. The dLAN 500 AV Wireless+ enables wireless surfing at transfer rates of up to 500 Mbps via dLAN and of up to 300 Mbps via WLAN in every room of your building—even on the other side of thick concrete walls!

You can have all of your home network's dLAN and WLAN devices available at a glance anywhere and any time using dLAN Cockpit App for smartphones and tablet PCs together with the dLAN 500 AV Wireless+.

1.1.1 About this manual

In addition to a small introduction to the basics of "dLAN" and "WLAN" and a presentation of dLAN 500 AV Wireless+ devolo products and dLAN Cockpit App in **Chapter 2**, in **Chapter 3** you will learn about how to successfully start up the dLAN 500 AV Wireless+ and how you can download

dLAN Cockpit App from the respective store. **Chapter 4** describes configuration options in detail for the built-in configuration interface, including access to the WLAN. What you need to do to integrate your dLAN 500 AV Wireless+ into the dLAN network and how you can monitor it using dLAN Cockpit App and dLAN Cockpit software is covered in **Chapter 5**. Information about product safety and the environmental compatibility of the device and our warranty terms can be found in **Chapter 6** and conclude the manual.

Description of the symbols

Here we briefly describe the meaning of the symbols used in this manual.

> *Very important note. Failure to observe this note may result in damage.*

> *Important note that should be observed.*

> *Additional information, background material and configuration tips for your device.*

If you have any further ideas or suggestions related to our products, we would be delighted to hear from you at support@devolo.com!

devolo on the Internet

For detailed information on our products or "dLAN", visit www.devolo.com. The **Service Centre** area contains downloadable product descriptions and documentation, as well as updates to devolo software and device firmware.

1.2 CE conformity

CE 0680

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 and Switzerland. The product is class A equipment. Class A devices may cause interference when used in residential environments.

> *"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 under* **CE***.*

> *For the permitted voltage range for operating the device and the power consumption, refer to the label on the rear side of the device. Additional technical information is available at www.devolo.com.*

2 Introduction

dLAN is an intelligent, secure technology that lets you set up a home network easily, quickly and economically via your household 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.

2.1 What exactly is dLAN?

dLAN (**d**irect **L**ocal **A**rea **N**etwork) uses the household power grid to transfer data between computers equipped with suitable adapters and other network components. As a result, any power outlet can be used as a network access point. The data is modulated prior to transfer and sent as a signal via household power lines. State-of-the-art technology ensures that the power and data networks do not interfere with one another. Networking via dLAN is fast and secure. The data is encrypted using a key to prevent easy interception by third parties.

2.2 What is WLAN?

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) 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 (from 1 to 140) 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 a dLAN) 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.

2.3 dLAN 500 AV Wireless+

The **dLAN 500 AV Wireless+** unites the technologies of **LAN**, **WLAN** (wireless) and **dLAN** in one case:

- It has three **LAN** ports for **directly** connecting three network components.
- The adapter provides an optimal connection for wireless terminal devices such as laptops, smartphones or tablet PCs (Apple/Android) via **WLAN**.
- Using **dLAN**, **different rooms** can be made accessible via the **mains supply** without any problems and every power outlet becomes a WLAN connection with excellent reception quality.
- Power strips and other devices using up to 16 amps can be connected via the integrated power outlet.
- dLAN 500 AV Wireless+ is the **link** between **dLAN Cockpit App** and the **dLAN network**. It collects all of the dLAN data in the local network and provides it to **dLAN Cockpit App**.

2.3.1 dLAN Cockpit App

dLAN Cockpit App is devolo's **free app**, for checking and configuring WLAN, dLAN and LAN connections for the dLAN 500 AV Wireless+ (via smartphone or tablet PC). The smartphone or tablet PC connects to the dLAN 500 AV Wireless+ at home via **WLAN**.

2.3.2 Sample applications

Fig. 1
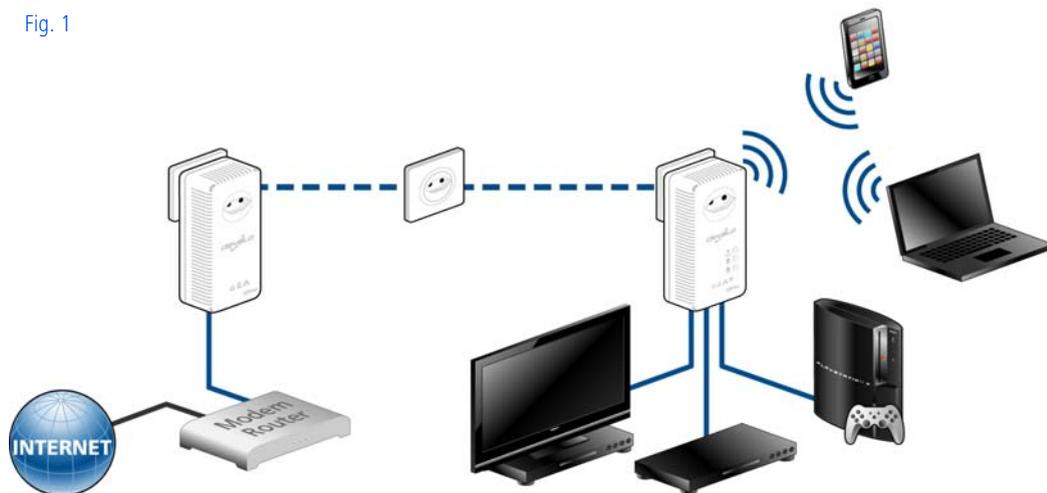
Fig. 2
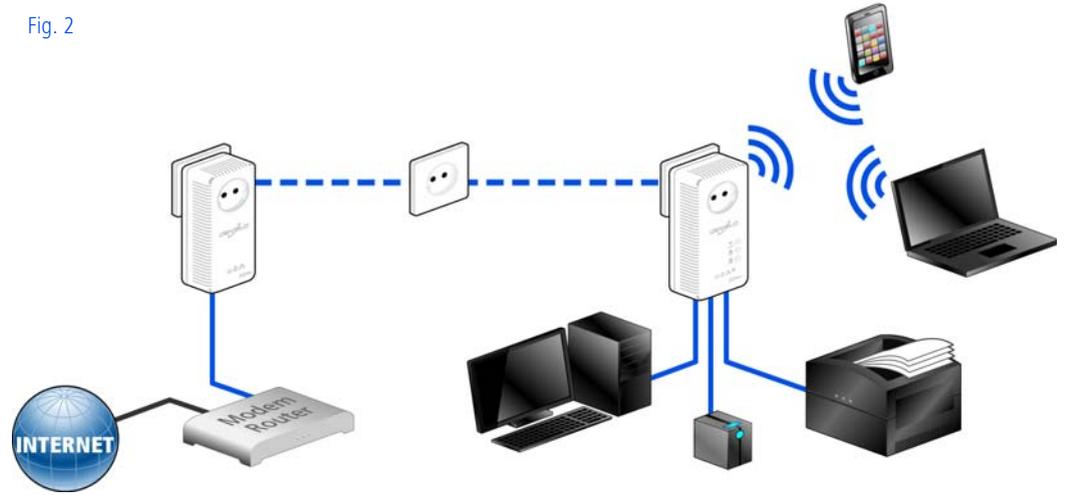
3 Initial use

This chapter covers everything you need to know to set up your dLAN 500 AV Wireless+. It will explain connecting the device and its functions. We will also briefly introduce the included devolo software and then guide you through its installation.

Fig. 3

3.1 Package contents

Please ensure that the delivery is complete before beginning with the installation of your dLAN 500 AV Wireless+.

● **Single Kit**:
  ○ dLAN 500 AV Wireless+
  ○ Network cable
  ○ Hard copy of installation guide
  ○ CD containing software and online documentation

or

● **Starter Kit**:
  ○ dLAN 500 AV Wireless+
  ○ dLAN 500 AVplus
  ○ Network cable
  ○ Hard copy of installation guide
  ○ CD containing software and online documentation

devolo AG reserves the right to change the package contents without prior notice.

3.2 System requirements

● **Operating systems:** Windows XP (32-bit), Windows Vista Home Premium (32-bit/64-bit), Windows 7 Home Premium (32-bit/64-bit), Linux (Ubuntu), Mac OS X

● **Network connection**

  Please note that your computer or other device must feature a network adapter with a network port.

  To set up a dLAN network, you need at least two dLAN devices (200 Mbps or 500 Mbps).

3.3 Functions

The dLAN 500 AV Wireless+ has the following elements:

3.3.1 Indicator lights

The indicator lights (LEDs) show all of the statuses for the dLAN 500 AV Wireless+ by illuminating and/or flashing in different ways:

Power

● **Green** flashing and illumination behaviour:
   ○ The LED lights up green when the dLAN 500 AV Wireless+ is operational.
   ○ The LED **flashes briefly**, if the dLAN 500 AV Wireless+ is in **PowerSave mode**.
   ○ The LED **flashes** at **quick, regular intervals,** if the dLAN 500 AV Wireless+ is connecting to the dLAN network (**pairing**).

dLAN

● **Off:** The LED does **not** light up. There is no connection to the dLAN 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 **3.4 Connecting the dLAN 500 AV Wireless+** *and* **4 dLAN network***.*

● **Green**: The network connection is suitable for HD video streaming; flashes when data is being transmitted.
● **Orange**: The network connection is suitable for SD video streaming and online gaming; flashes when data is being transmitted.
● **Red**: The network connection is suitable for simple data transfer and Internet access; flashes when data is being transmitted.

WLAN

- **Off:** The LED does **not** light up. The WLAN connection is disabled.
- **Green** flashing and illumination behaviour:
  - ○ The LED lights up when connected to the WLAN network at **2.4 GHz**.
  - ○ The LED **flashes** at **quick, regular intervals** when data is being transmitted.
  - ○ The LED **flashes briefly** during WPS pairing.
- **Blue** flashing and illumination behaviour
  - ○ The LED lights up when connected to the WLAN network at **5 GHz**.
  - ○ The LED **flashes** at **quick, regular intervals** when data is being transmitted.
  - ○ The LED **flashes briefly** during WPS pairing.

Ethernet

- **Off:** The LED does **not** light up.

  Check all of the cable connections and check if the connected network components are disabled.

- **Green**: Lit steady when a connection to the Ethernet network exists; flashes when data is being transmitted.

3.3.2 Buttons

ON/OFF

Use the ON/OFF button to switch the **WLAN** function on or off.

Make sure that the WLAN function in the factory defaults is enabled and the WLAN encryption is set to WPA2. The default WLAN key is the Wi-Fi key of

the dLAN 500 AV Wireless+. You will find the key on the label on the back of the housing.

🔒 WPS

With the WPS (**W**i-Fi **P**rotected **S**etup) encryption button, you secure your WLAN network at the touch of a button.

> *WPS is one of the encryption standards developed by the Wi-Fi Alliance for increasing security in a WLAN home network. The objective of WPS is to make it easier to add devices to an existing network. For more detailed information, refer to Chapter **5.4.1 Security**.*

🔒 dLAN

Via the dLAN encryption button, you secure your dLAN network at the touch of a button:

● To encrypt your dLAN network individually, press **each encryption button** on the connected devices for approx. **1 second** – within 2 minutes.

● To remove a dLAN device from your network, press the **encryption button** on the corresponding device **for at least 10 seconds** (see **4.1 dLAN network encryption at the touch of a button**).

↺ Reset

The **Reset** button (on the side of the housing) has two different functions:
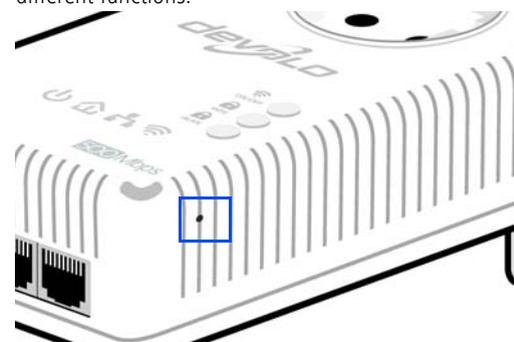
● **The device restarts** if you press the Reset button **for less than 10 seconds**.

● To change the configuration of the dLAN 500 AV Wireless+ 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.

3.3.3 Network jacks

The three LAN ports can be used to connect computers or other network devices to the dLAN 500 AV Wireless+ via commercially available network cables.
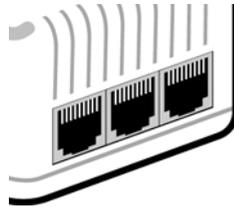
3.3.4 WLAN antennas

The internal WLAN antennas are for connecting to other network devices wirelessly.

3.4 Connecting the dLAN 500 AV Wireless+

This section describes how to connect your dLAN 500 AV Wireless+ to a computer or other network device.

① Use a network cable to connect the dLAN 500 AV Wireless+ to network port of your computer or other network device.

② Plug the dLAN 500 AV Wireless+ into a wall socket.

The power outlet should be in range of the connected network device.
The dLAN 500 AV Wireless+ and the network device should be easily accessible.
To switch off the dLAN 500 AV Wireless+ or disconnect it from the mains supply, pull the power plug out of the power outlet.

③ A dLAN network is set up as soon as at least one other dLAN adapter has been connected and plugged into the mains supply. Now you can secure your dLAN network to prevent unauthorised access and you can do so **either**

○ By pressing the **encryption button** on the adapter **or**

○ Using **dLAN Cockpit App** via your smartphone or tablet PC **or**

○ Using the provided devolo **dLAN Cockpit** software – the local monitoring and encryption program **or**

○ By entering the **dLAN password** in the **configuration interface**.

For information on how to proceed in each case, please read further in Chapter **4 dLAN network** *and/or Chapter* **5.4 Device configuration**.

Downloading dLAN Cockpit App

④ Download **dLAN Cockpit App** to your smartphone or tablet PC from the corresponding store.

You can find dLAN Cockpit App quickest by clicking on the magnifying glass in the store and searching directly for **dLAN Cockpit**.

⑤ **dLAN Cockpit App** is placed in your smartphone's or tablet PC's app list as usual. Tapping on the **dLAN Cockpit** icon brings you to the start menu.

You can find more information in Chapter **4.2 dLAN Cockpit App**.

Installation of devolo software

⑥ In order to be able to configure the **WLAN network**, first install the dLAN 500 AV Wireless+ software as described in the following chapter.

3.4.1 Software installation

Software for Windows

The installation wizard installs the adapter's configuration software as well as the **devolo dLAN Cockpit** software on the Windows operating system.

● **dLAN Cockpit** finds all accessible dLAN adapters in your dLAN network, displays information about these devices and encrypts your dLAN network individually.

● You can configure your WLAN network, along with other actions, using the **configuration interface** for your dLAN 500 AV Wireless+.

To install the software, insert the included CD-ROM in the CD drive of your computer.

If AutoPlay is active on your computer, the installation will start automatically. Otherwise, open the directory with the Windows Explorer by right-clicking on **Start** *(or the* **Windows logo***) and selecting* **Explorer** *from the context menu. Then start the installation wizard manually.*

You will be asked for permission to transfer anonymous performance data related to your dLAN adapter to devolo. The data sent to devolo pertains only to the performance values of your dLAN devices. The data is anonymised and will be used exclusively for statistical purposes. By providing it, you can help us improve our products. You can find the installed software applications in the **Start ▷ All Programs ▷ devolo** program group.

Software for Mac (OS X)

The **software ▷ mac** folder contains the dLAN configuration software.

Software for Linux (Ubuntu)

The **Software ▷ Linux** folder contains the dLAN configuration software.

4 dLAN network

Before you can use the dLAN 500 AV Wireless+ in your dLAN network, first you have to connect it to other dLAN AV devices as a home network. Two specific pieces of information are especially important for this:

● Shared use of a dLAN password results in a delimited dLAN network.

● Shared use of the dLAN password serves as access control to the dLAN network as well as the encryption, and thereby the interception protection, of the transmitted data.

The dLAN password can be set in different ways:

● Automatically using the **encryption button** (see **4.1 dLAN network encryption at the touch of a button**)

● Manually using the **dLAN Cockpit** program (see **4.3 dLAN Cockpit**) or **dLAN Cockpit App** program (see **4.2 dLAN Cockpit App)**.

● By entering the **dLAN password** in the **configuration interface** of the adapter (see **5 Network configuration**).

4.1 dLAN network encryption at the touch of a button

To encrypt a dLAN network, in which all associated devices are equipped with an encryption button, simply press the encryption button located on the device. Pressing this button will encrypt your dLAN network with a randomly generated password.
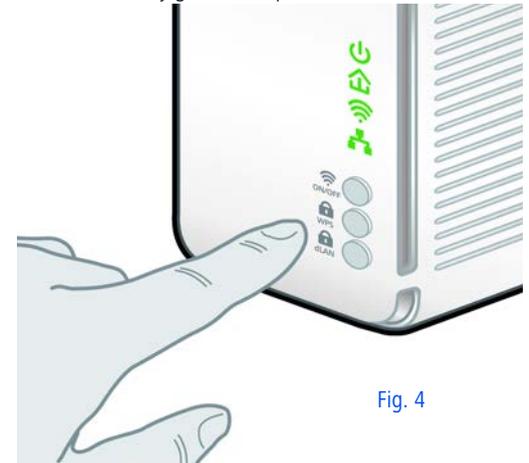
Fig. 4

The following section contains exact instructions on the basis of possible network scenarios:

Encrypting a new dLAN network with a dLAN 500 AV Wireless+ and a dLAN 500 AVplus (Fig. 5)

Once both adapters have been successfully connected, press each encryption button **for approx. one second within two minutes of one another**.

That's it! Your dLAN network is now protected against unauthorised access.
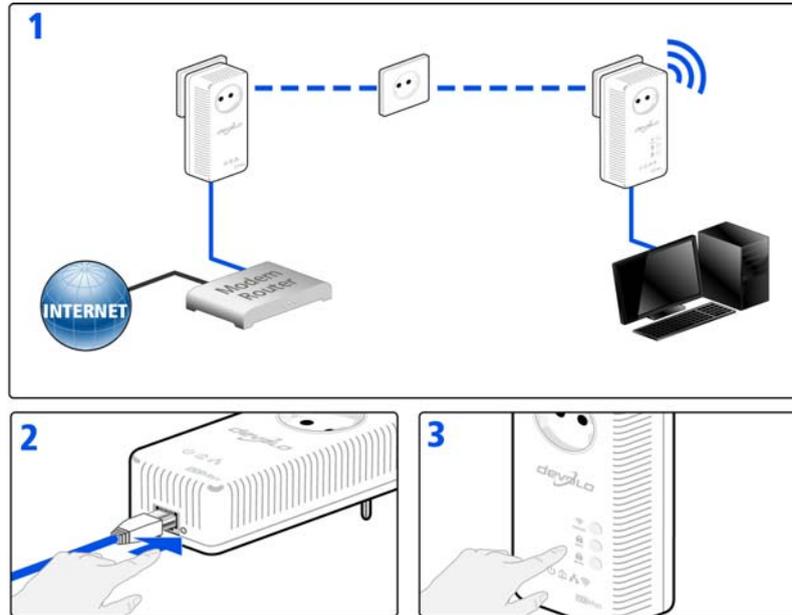
Fig. 5

Expanding an existing dLAN network by adding a new dLAN 500 AV Wireless+ (Fig. 6)

If you have already secured your existing dLAN network using the encryption button, use the same method to integrate further adapters. Once you have successfully connected the new dLAN 500 AV Wireless+, first press the encryption button (approx. **1 second**) of one of your network's existing adapters, then press the encryption button (approx. **1 second**) of your new dLAN 500 AV Wireless+ **within two minutes**.

That's it! The new dLAN 500 AV Wireless+ is now integrated in your network. To integrate additional adapters in your network, repeat the above steps.
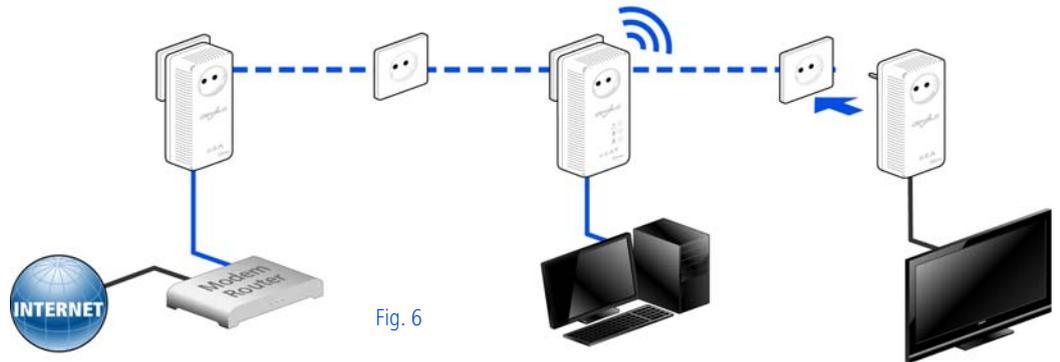
Fig. 6

Removing a dLAN 500 AV Wireless+ from a network (Fig. 7)

To remove a dLAN 500 AV Wireless+ adapter from an existing network, press its 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 device into a different dLAN network, follow the steps described above, depending on whether you are setting up a new network or adding the adapter to an existing one.

Fig. 7
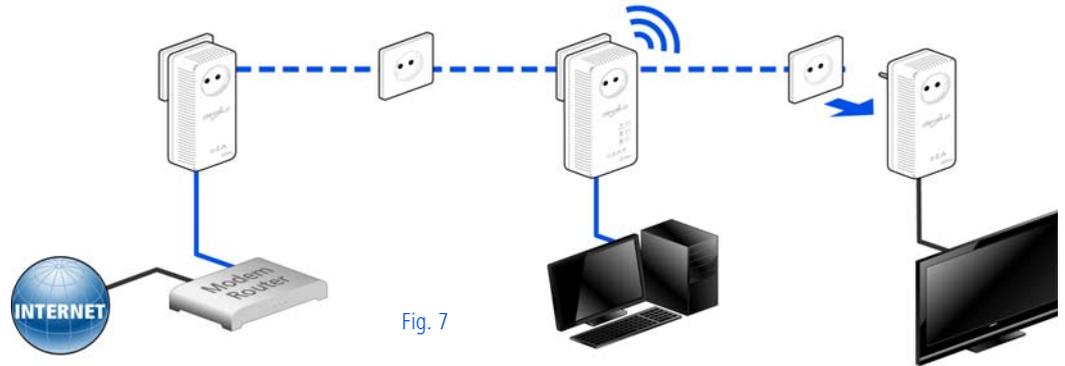
4.2 dLAN Cockpit App

dLAN Cockpit App is an app for monitoring and encryption, which you can use to search out all other accessible dLAN devices in your home network and connect them together into a secure network **using the dLAN 500 AV Wireless+** – this could be considered the counterpart to the **local** devolo dLAN Cockpit **software** (see **4.3 dLAN Cockpit**).

In addition, you can also use **dLAN Cockpit App** to access the **configuration interface** for the dLAN 500 AV Wireless+ and to change settings in the WLAN and dLAN network (see **5 Network configuration**).

① After you have integrated the dLAN 500 AV Wireless+ into your home network as described in Chapter **3.4 Connecting the dLAN 500 AV Wireless+** and have downloaded dLAN Cockpit App, you can get to start menu just by tapping on **dLAN Cockpit**.

② In order to connect the dLAN 500 AV Wireless+ to your smartphone or tablet PC, select **My dLAN**.

③ As soon as your smartphone or tablet PC is connected to the dLAN 500 AV Wireless+, all of the adapters found in the network appear with a picture and corresponding name.

The menu in dLAN Cockpit App automatically adjusts to the orientation (horizontal/vertical) of the smartphone or tablet PC.

If your smartphone or tablet PC switches to power saving mode, the previously displayed view is shown again when you activate the screen again.

4.2.1 Overview page

You can page through the list of adapters by **swiping** across the screen (left/right or up/down).

The **house** icon displays the connection over dLAN.

The **WLAN** icon displays the connection over WLAN.

The **bar graph** reflects the connection quality. The data rate is displayed in **Mbps**. Tapping on a respective adapter allows you to read the transfer rate for another device from the selected adapter's point of view.

Tapping on the **gear/arrow** brings you to the configuration interface for the dLAN 500 AV Wireless+. For more detailed information on the interface refer to Chapter **5 Network configuration**.

Tapping on the **recycle bin** removes the connected adapters.

4.2.2 Settings menu

Tapping on the two **gears** brings you to the settings menu for the respective adapter.

Here you have the option of assigning a unique **new name** for yourself and to reset the respective device to the **factory default settings**. In addition, you can learn about device information such as the firmware version in use and the individual MAC address.

4.2.3 Menu on the bottom edge of the screen

The functions of the menu on the bottom edge of the screen are self-explanatory and can be operated intuitively. Depending on which submenu you are in, the following functions appear:

- ● **Start**: **dLAN Cockpit** start menu
- ● You can always use the **Refresh** option to display the current status of devices that have been found (if this hasn't happened automatically).
- ● During the initial installation of the adapter, select the **Add adapter** option.
- ● The **Troubleshooting guide** contains additional installation aids.

● **Security**: Tapping on the **key** icon allows you to change the dLAN password for either the entire dLAN network or just for the respective adapter or to reset it to the factory defaults.

> *The factory default password is **HomePlugAV**. For security reasons, we recommend setting an individualised dLAN password.*

4.3 dLAN Cockpit

devolo **dLAN Cockpit** is a monitoring and encryption program that detects all reachable dLAN AV devices in your home network and combines them in a secure network. Due to its logical graphic design, the dLAN Cockpit is easy and intuitive to operate. After installing the devolo software, it can be found in the **Start** ▷ **Programs** ▷ **devolo** program group.
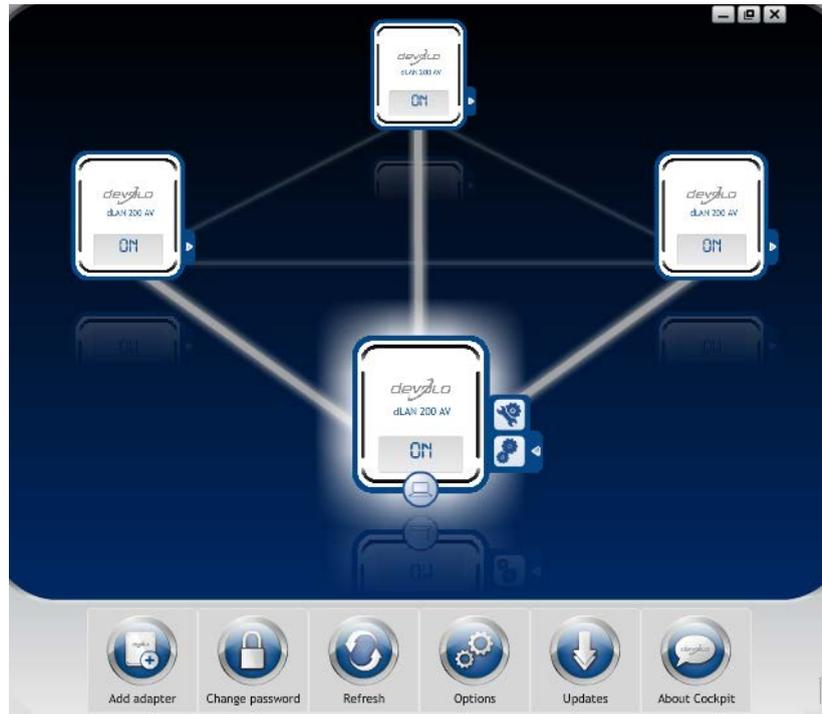
After starting the dLAN Cockpit, all reachable dLAN devices in your home network will appear. This may take a moment.

All adapters found in the network appear with as adapter icon with a corresponding product name. The adapter in the middle of the dLAN network identified with the symbol shown here symbolises your locally connected device. If you have multiple dLAN devices connected locally, you can jump back and forth between them. Clicking an adapter icon with the mouse enables the corresponding dLAN AV device and highlights it.

The coloured connecting lines of the adapters illustrate the current transmission quality:

● **Green**: the network connection is suitable for HD video streaming.

● **Orange**: the network connection is suitable for SD video streaming and online gaming.

● **Red**: the network connection is suitable for simple data transfer and Internet access.

If data transmission from one device to another is actually taking place, the data rate is displayed on the respectively highlighted adapter.

Settings and functions

You can configure settings for the respectively highlighted device or for the network

● via the buttons at the bottom edge of the screen

● or via tabs arranged at the side of each adapter.

You can always use the **Refresh** button to display the current status of devices that have been found (if this hasn't happened automatically).

By means of the **Options** button or the corresponding tabs of the respective adapter, you can learn device information such as the firmware version used and the individual MAC address.

Options are given like assigning an **additional name**, resetting the respective device to the **factory default settings** or **removing** a **device** from the existing dLAN network.

The above-mentioned setting options vary depending on the function and features of your device.

You can also specify whether information on the performance of your dLAN adapters will be transferred to devolo.

The data sent to devolo pertains only to the performance values of your dLAN devices. The data is anonymised and will be used exclusively for statistical purposes. By providing it, you can help us improve our products.

The **Troubleshooting Guide** includes installation instructions and information about how to connect your devices optimally with one another.

4.3.1 Encrypting a network with dLAN Cockpit

If you use dLAN AV devices **without an encryption button**, data can be encrypted only via **dLAN Cockpit**.

Before the networking procedure, note the security IDs of all dLAN AV adapters. This unique identifier of each dLAN 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 dLAN adapters are connected to the power grid and computers or other network components as appropriate.

Scan for local adapter

After dLAN Cockpit is started, it searches for the dLAN adapter connected directly to your computer first.

Adding an adapter

Add all the dLAN devices you want to your dLAN network by selecting the **Add adapter** button. You will need the **16**-character security IDs of the adapters from the label on the housing. Enter it now in the **Security ID** field and confirm with **OK**. If a security ID is correct and the device can be reached in the dLAN network, it will be added to your network of configured adapters and also displayed in the program.

Entering a network password

After you have added all the dLAN devices you want to your dLAN network, select the **Change password** button to assign a shared network password that will apply for all registered adapters in your personal home network.

You can choose between your own password, a random password and the default password. To define your own password with a length of at least eight characters, enter this into the **Network password** text field. Alternatively, you can have a randomly selected, highly secure password assigned using the **Generate secure password** button. Use the **Factory default password** button to reset the dLAN adapter to the default password. Normally, the display of the password is hidden for security reasons. If you enable the option **Show characters**, the current password is displayed in legible form in the text field.

The factory default password is **HomePlugAV***. Assigning a specific password to a single adapter will exclude it from the remaining dLAN network.*

If **dLAN Cockpit** is called up again later after a successful initial installation, for example to **integrate** a **new adapter** into a network, the application remembers the devices that were entered earlier. Enter the new device as described in the **Adding an adapter** section. The **current network password** is assigned **automatically** to the newly added device.

5 Network configuration

The dLAN 500 AV Wireless+ has a built-in configuration interface that can be called up using a standard web browser. All settings for operating the device can be modified here.

5.1 Calling up the built-in configuration interface

You can access the built-in online configuration interface for the dLAN 500 AV Wireless+ in different ways:

● Using **dLAN Cockpit App** on your smartphone or tablet PC, you can access the device's configuration interface by going to the **overview page** of dLAN Cockpit App and tapping on the **gear/arrow**.

*You can find more information on dLAN Cockpit App in Chapter **4.2 dLAN Cockpit App**.*

● Using **dLAN Cockpit** software under **Start ⇨ All Programs ⇨ devolo ⇨ dLAN Cockpit**, you can get to the device's configuration interface by click-

ing on the tab for the dLAN 500 AV Wireless+.

Then the program determines the current IP address and starts the configuration in the web browser.

● In addition, you can call up the device's configuration interface by entering the host name **dlanwireless.local** into your web browser's address line.

By default, you will come directly to the configuration interface. However, if a login password was set via the option **Device configuration ⇨ Security**, you have to enter this first (see **5.4.1 Security**).

5.2 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 dLAN, WLAN and LAN devices.

● You can change or modify the various device settings for security, network, dLAN and time under **Device configuration**.

● You can change or modify WLAN 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 dLAN 500 AV Wireless+ here.

5.3 Status overview

In the **Status overview** area you can track the status of your connected dLAN, WLAN and LAN devices.

5.3.1 dLAN status

To display all connected dLAN devices, click either the **house** icon or the **dLAN devices** arrow. Each connected dLAN device, regardless of whether it is connected locally or remotely in the network, is displayed with its MAC address, name and type. Clicking or tapping the **lock** icon brings you directly to the **dLAN settings** (see **5.4.3 dLAN settings**).

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

Add dLAN® device

Add dLAN® device

Here you can add a new dLAN® device to your network. First, enter the security ID printed on the rear side, plug the device into a power outlet, and then confirm by clicking Save.

The security ID consists of four groups, each with four capital letters, separated by hyphens.

Security ID: [   ] - [   ] - [   ] - [   ]

Before the networking procedure, note the security IDs of all dLAN adapters. This unique identifier of each dLAN 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 dLAN adapters are connected to the power grid and computers or other network components as appropriate.

5.3.2 WLAN monitor

Click on either the **WLAN** icon or the **WLAN monitor** arrow to have all of the known WLAN devices displayed. Each WLAN 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. Clicking or tapping the **lock** icon brings you directly to the **WLAN configuration** area (see **5.5 WLAN configuration**), where you can configure settings for WLAN network security.

WLAN monitor

Known stations

Here you see a list of stations and their connection status.

No stations have been connected to the access point since it was last restarted.

5.3.3 Ethernet status

The status and connection speed for the three network jacks are shown in this area.

Ethernet status

Port 1	Port 2	Port 3
not connected	100 Mbps	not connected
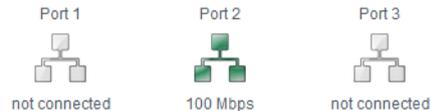
5.4 Device configuration

In the configuration area of the device you can modify settings for security, network, dLAN, date and time.
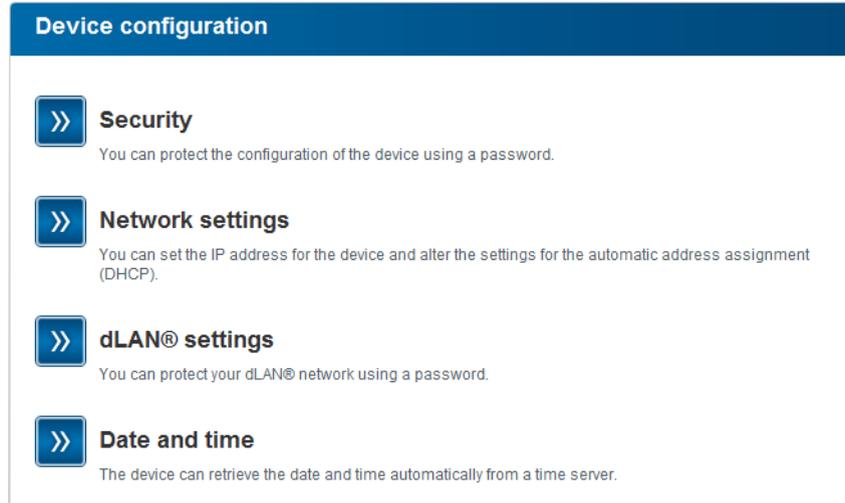
Device configuration

» **Security**
You can protect the configuration of the device using a password.

» **Network settings**
You can set the IP address for the device and alter the settings for the automatic address assignment (DHCP).

» **dLAN® settings**
You can protect your dLAN® network using a password.

» **Date and time**
The device can retrieve the date and time automatically from a time server.

5.4.1 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 dLAN 500 AV Wireless+.

Password

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

By default, the built-in configuration interface of the dLAN 500 AV Wireless+ is not protected with a password. However, we recommend assigning a password when the installation of the dLAN 500 AV Wireless+ 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!

Security

Password

Enter a password to restrict access to your device configuration. The password may not be longer than 24 characters. The username for configuration access is "admin".

Present password: [   ]

New password: [   ] 0 Characters
Repeat password: [   ] 0 Characters

② Call up the configuration interface again later; the following window appears first:

③ Enter **admin** in the **User name** field and your individual password in the **Password** field.

The **admin** *user name cannot be changed.*

5.4.2 Network settings

The dLAN 500 AV Wireless+ 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 dLAN 500 AV Wireless+ 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 dLAN 500 AV Wireless+, proceed as described under **5.1 Calling up the built-in configuration interface***.*

Network settings

IP address

Here you can configure the local IP address for the device.

IP address: 192.168.0.249
Netmask: 255.255.255.0
Default gateway:

DHCP client

☑ Use network settings provided by a DHCP server

5.4.3 dLAN settings

In a dLAN network, all connected components must use the same password. The dLAN password can be defined in **dLAN Cockpit App** or **dLAN Cockpit**, via the **dLAN encryption button** (see Chapter **4 dLAN network**) or at this spot 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 **Total** dLAN **network**.

*The dLAN default password is **HomePlugAV.***

dLAN® settings

dLAN® password

Enter the dLAN® network password needed for your device to access your dLAN® network. All devices that are part of a dLAN® network must use the same dLAN® network password.

Define password for: ○ Local device
                       ● Total network
Password: [   ] 0 Characters
Repeat password: [   ] 0 Characters

5.4.4 Time server

A time server is a server on the Internet whose task consists of providing the exact time. Most time servers are coupled with a radio clock.

The option **Retrieve date and time automatically** is activated by default so that the dLAN 500 AV Wireless+ 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 dLAN 500 AV Wireless+ automatically adjusts to daylight saving time.

Date and time

Current time

You can view the current date and the current time here.

Not possible to retrieve time information from the time server. Please check the device configuration and your Internet connection.

Time server

The device can retrieve the date and time automatically from a time server. An active Internet connection is required for this purpose.

☑ Retrieve date and time automatically

Time zone: GMT+01:00 (Western Europe, Central Europe) ▾

Time server: ptbtime1.ptb.de

☑ Adjust to daylight saving time automatically

5.5 WLAN configuration

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

Access Point
SSID: devolo-bc:f2:af:69:11:f8
Encryption: WPA2

Guest account
Disabled

WLAN filters
Specify the computers that are permitted to access your access point here.

Parental controls
You can establish a time limit for individual computer access via the access point.

WLAN time control
The WLAN time control can switch your wireless network on and off at certain times of the day automatically.

WiFi Protected Setup (WPS)
You can configure your wireless network via WPS.

If you would like, you can completely shut off the WLAN part of your dLAN 500 AV Wireless+, e.g. if you want to operate it exclusively as a simple dLAN device via the built-in Ethernet connections. There are three different methods for switching the **WLAN function** on and off:

● Simply 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 WLAN time control. For more information, refer to Chapter **5.5.5 WLAN time control**.

The operating state of the device is displayed under **5.3 Status overview**.

WLAN configuration

The wireless network is currently enabled. You can disable the wireless network by clicking the button below.

This action does not influence the function of the WLAN time control. If the time control is enabled, it will switch the wireless network on or off again at the next time you set. If you want to disable the wireless network permanently, please also disable the time control.

Disable WLAN

5.5.1 Access point

Since the dLAN 500 AV Wireless+ acts as an access point, you have to configure various parameters for your wireless network.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the dLAN 500 AV Wireless+. In this case, configure the device via Ethernet or dLAN.

Settings

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.

Access Point

Settings

Please select the settings to be used by your access point.

SSID *: devolo-bc:f2:af:69:11:f8   Hide SSID: ☐

Frequency band: ⦿ 2.4 GHz ○ 5 GHz Channel: Auto ▾ Use 40-MHz channels: ☐ **

Please check whether all wireless connected devices support 5 GHz operating mode before enabling it!

Note: In 2.4 GHz mode the WLAN LED is green, in 5 GHz mode it is blue.

In the factory default setting *of the dLAN 500 AV Wireless+, the* WLAN function is enabled *and WLAN* WPA2 *encryption is configured. The default WLAN key is the Wi-Fi key for the dLAN 500 AV Wireless+. You will find the key 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 in a particular frequency range.

● Thirteen channels are available at the **standard 2.4 GHz** frequency.

● If you select the higher **5 GHz** frequency range, it is important to ensure that all of your connected devices also support this frequency band. **From channel 52 onward** you go into the **radar range**. When **accessing the device for the first time**, a **radar detection phase** starts automatically, during which the dLAN 500 AV Wireless+ cannot be accessed.

In both cases, we recommend keeping the default setting **Auto** since the dLAN 500 AV Wireless+ selects the channel regularly and independently in this setting. 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.

Pay attention to the various LED colours of the WLAN LED. For more information, refer to Chapter 3.3.1 **Indicator lights***.*

Keep the following in mind if you would like to use doubled channel width (utilising 40 MHz channels): The potential transfer rate is 300 Mbps instead of 150 Mbps when using wireless channels with doubled channel width, but increased interference can occur due to neighbouring access points.

Security

Without encryption, not only are all data transmitted from client computers to the dLAN 500 AV Wireless+ 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 **5.5.3 WLAN filters**), third parties could gain access to your network at any time and, for example, share your Internet connection. Each instance of access is visible to you in the WLAN monitor (see Chapter **5.3.2 WLAN monitor**).

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 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 dLAN 500 AV Wireless+ 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. If possible, always select the better WPA2 encryption method. Only use WEP if one of your wireless terminal devices does not operate with a better standard.

Security

You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WEP or WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11a/g standard). Do not use the WEP or WPA standard unless your wireless devices do not support WPA2.

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

○ No encryption (not recommended)

○ WEP (not recommended)
   Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
   Key:

● WPA / WPA2
   Please enter the WPA key as a string of characters.
   Key *: JFRINMQHHNUJGFXO
   Mode: WPA2 ▼

* Permitted characters are upper and lower-case letters a-z, the digits 0-9, the space character and the following special characters
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

**When using wireless channels with double bandwidth (40 instead of 20 MHz), the potential connection speed is up to 300 Mbps (otherwise it is 150 Mbps); at the same time, neighbouring access points may receive increased interference.

5.5.2 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 WLAN, 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 WLAN password. 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. You can also enable or disable the guest account in **dLAN Cockpit App** using the **Activate guest account** button.

Define the name of the guest network in the **SSID** field.

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 the guest account depends on the dLAN 500 AV Wireless+ and can only be active just as long.*

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 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 to the dLAN 500 AV Wireless+ to the method you have selected.

Guest account

Settings

Please select the settings to be used by the guest account.

☐ Activate guest account

SSID *: devolo-guest-bc:f2:af:69:11:f8

Automatic shutoff

You can define whether the guest account is to be shut off after a certain period of time. However, at most, guest account is active only for as long as the general access point is.

☐ Automatically shut off guest account after [   ] [▼]

Security

You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11a/g standard). Do not use the WPA standard unless your wireless devices do not support WPA2.

○ No encryption (not recommended)

◉ WPA / WPA2
　　Please enter the WPA key as a string of characters.
　　Key *: JFRINMQHHNUJGFXO
　　Mode: WPA2 [▼]

*Permitted characters are upper and lower-case letters a-z, the digits 0-9, the space character and the following special characters
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

5.5.3 WLAN filters

In addition to encryption (see **5.5.1 Access point**), you can secure your wireless network even more by us-ing a WLAN filter to limit access to WLAN devices. Even if the encryption is switched off, the device will not establish a connection.

WLAN filters

The MAC address filter is currently disabled. Stations can connect to your access point regardless of their MAC address.

[Enable filter]

Enter the MAC addresses of the stations that can log into your access point. You can either enter the MAC addresses manually or select them from the list of currently known stations.

[   ] [Add]

No stations have connected to the access point yet.

Approved WLAN stations

The station list currently has no entries.

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 manually enter different network devices to provide access to your dLAN 500 AV Wireless+ using what is known as their MAC address or you can select take them from a list of known devices (see **5.3.2 WLAN monitor** ⟡ **WLAN monitor**). Confirm each entry with **Add**.

Approved WLAN stations

Network devices or stations connected to your dLAN 500 AV Wireless+ are automatically listed, that is, to enable an already connected station for the dLAN 500 AV Wireless+, 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 selected**.

The WLAN 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).

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 dLAN 500 AV Wireless+ 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!

5.5.4 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 dLAN 500 AV Wireless+ has to be enabled and an active Internet connection is also required (see **5.4.4 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 (see **5.3.2 WLAN monitor** ⇨ **WLAN monitor**). Confirm each entry with **Add**.

WLAN stations with time limit

Here you can find a list all of the WLAN 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 or tapping 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 configured time limit will be monitored**.

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

Station setting

WLAN station time limit

Define and activate a time limit.

WLAN station

MAC address: 00:0b:3b:3f:c7:97
Name:

You can define whether the time limit is to be monitored for this station.

☐ The configured time limit will be monitored

Set the daily time quota for this station:

Hours Minutes
24 ▾ 00 ▾

A **time quota** can only be used if it matches the **time periods** defined in the **WLAN time control** and if the **dLAN 500 AV Wireless+ is enabled** and there is an Internet connection. (see **5.5.5 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.

5.5.5 WLAN time control

Synchronisation with an Internet time server has to be ensured in order to use WLAN time control. In this case, the time server (Device configuration ▷ Date and time ▷ Obtain date and time automatically) for the dLAN 500 AV Wireless+ has to be enabled and an active Internet connection is also required 5.4.4 Time server). The time server is enabled by default.

To be able to use the WLAN 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 dLAN 500 AV Wireless+ 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.

WLAN time control

WLAN time control

You can define two time periods during which your wireless network is to be enabled for each weekday. The time control is used to switch the wireless network on and off automatically at the times specified. Please note that the wireless network is never disabled while there are still stations connected to it. The system will wait until the last station has logged off before the wireless network is disabled.

Not possible to retrieve time information from the time server. To use the time control, you have to specify in the device configuration that the device is to retrieve the date and time automatically from a time server. This requires an Internet connection.

☐ Enable time control

Please enter the times in the 24-hour format (hh:mm) (example: 23:59). If you want to set a time period that goes beyond midnight, you must split it into two time periods (example: Monday 18:00 to 00:00 and Tuesday 00:00 to 01:00).

Monday:		-		and		-	
Tuesday:		-		and		-	
Wednesday:		-		and		-	
Thursday:		-		and		-	
Friday:		-		and		-	
Saturday:		-		and		-	
Sunday:		-		and		-	

5.5.6 Wi-Fi Protected Setup

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 sta-

tion are transmitted automatically and continuously to the other WLAN station(s) of the wireless network. The dLAN 500 AV Wireless+ offers two different variants for transmitting these encryption keys:

WiFi Protected Setup (WPS)

Using WPS you can integrate WLAN stations into your wireless network by entering a PIN or by pressing the WPS button on the device.

Note: If WPS is enabled, any configured WLAN filter will be temporarily disabled!

☑ WPS active

WPS via PBC (Push Button)

The WPS configuration can be started either by using the WPS button on the device or via the web interface. Please start the configuration process and then press the WPS button on the device that is to join the wireless network.

Start setup

WPS via PIN

The device also supports WPS via a PIN. In order to join a station to your wireless network via PIN please enter the PIN and then start the configuration process. Next, you must tell your station that it should join the wireless network. The PIN of the station is usually either printed on the housing or specified on the configuration interface.

PIN: [ ]   Start setup

Note: WPS cannot be used to integrate WLAN stations into your wireless network via guest account!

WPS via PBC (Push Button Configuration):

① Start the encryption process on the dLAN 500 AV Wireless+

- ○ 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 station 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 stations 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 station to be added and transmit the PIN selected on the dLAN 500 AV Wireless+. Confirm the encryp-

tion 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.

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 **5.4.1 Security**), 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.

5.6 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 dLAN 500 AV Wireless+.

Management

» Reset configuration
All settings in the device will be deleted and reset to their factory default values. All of your settings will be lost.

» Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.

» Restore device configuration
Select a saved configuration file to restore a previous configuration on the device.

» Update Firmware
Update the firmware in your device by uploading the new firmware file from your computer to the device.

5.6.1 Resetting the configuration

With the **Management ⟫ Reset configuration** command, the dLAN 500 AV Wireless+ is reset to the original factory defaults. In doing so, you lose your personal settings.

The last-assigned dLAN password for the dLAN 500 AV Wireless+ is also reset. To re-secure your dLAN network individually, read further at **5.4.3 dLAN settings**.

For backup purposes, all active configuration settings can be transmitted to your computer, stored there as a file and reloaded into the dLAN 500 AV Wireless+. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

5.6.2 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.
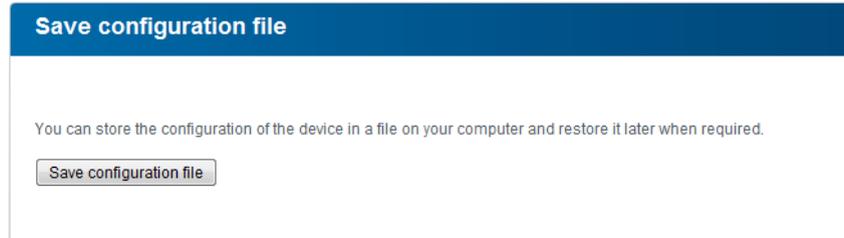
5.6.3 Restoring a configuration

An existing configuration file can be sent to the dLAN 500 AV Wireless+ 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.

Restore device configuration

Please select the configuration file to be loaded onto the device.

File name: [   ] [Browse...]

[Restore device configuration]

5.6.4 Update firmware

The firmware of the dLAN 500 AV Wireless+ includes the software for operating the device. If necessary, de-volo offers new versions on the Internet as a file down-load, for example to modify existing functions.

Update Firmware

Current firmware version: 1 (2012-08-21)

Please select the firmware file to be loaded onto the device.

File name: [_____] [Browse...]

[Update Firmware]

① To bring the firmware up to the latest version, first go to the devolo website, www.devolo.com, and download the appropriate file for the dLAN 500 AV Wireless+ 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 dLAN 500 AV Wireless+ restarts automatically.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the dLAN 500 AV Wireless+ via dLAN or LAN rather than WLAN.

6 Appendix

6.1 Important safety instructions

All safety and operating instructions should be read and understood before using the device, and should be kept for future reference.

● Never open the device. There are no user-serviceable parts inside the device.

> ***Do not try to service this product yourself! Contact qualified technicians each and every time your device needs maintenance. There is a risk of electric shock!***

● Use the device in a dry location only.

● Always use the included network cable to connect the device.

> ***The outlet must be within reach of the connected network devices. The adapter and the network devices must be easily accessible.***

● To switch the device off, pull the power plug.

● To disconnect the device from the power supply grid, pull the power plug.

● Do not insert any objects into the openings of the device.

● Do not keep the device in direct sunlight.

● Slots and openings on the case serve as ventilation. Never block or cover them.

● Never set up the device near a heater or radiator.

● The device should be located only where sufficient ventilation can be ensured.

● Disconnect the device from the power supply grid before cleaning. Use a moist towel to clean the device. Never use water, paint thinner, benzene, alcohol or other strong cleaning agents when cleaning the device, as these could damage the case.

● Never use the device with a power supply that does not meet the specifications provided on the rating plate. If you do not know what type of power supply you have at home, contact your dealer or energy supplier.

● In the event of damage, disconnect the device from the power supply grid and contact customer service. This applies, for example, if

  ○ the power cable or plug is damaged.

  ○ liquid has been spilled on the device or objects have fallen into the device.

  ○ the device has been exposed to rain or water.

○ the device does not work, even though the operating instructions have been followed properly.

○ the device's case is damaged.

6.2 Disposal of old devices

To be used in the countries of the European Union and other European countries with a separate collecting system:

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 ("Elektrogesetz"). 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 devolo AG warranty is given to purchasers of devolo 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 devolo'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, devolo 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 devolo, but not shipping and handling costs involved in transport from the buyer to the service station and/or to devolo.

c)   Replaced parts become property of devolo.

d)   devolo 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 devolo product is three years. This period begins at the day of delivery from the devolo dealer. Warranty services carried out by devolo 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. devolo 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 devolo,

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, devolo reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

The above conditions define the complete scope of devolo's legal liability.

a) 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.

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

c) devolo is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

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

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

f) 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, devolo's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

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

Index

B
Bar graph 23

C
CE 6

D
Default WLAN key 14, 47
DHCP server 40
Disposal of old devices 68
dLAN encryption 42
dLAN house symbol 23
dLAN password 42

F
Factory default password 28

G
Gear/arrow 24
Generate secure password 28

I
Important safety instructions 6
Indicator lights 13
Integrating the new adapter into the network 29
IP address 40

K
Key icon 25

L
LAN (Network connection) 16

Linux 18

M
Mac (OS X) 18
MAC address 53

N
Network password 28

P
Package contents 12

R
Recycle bin 24
Reset 15

S
Security ID 28, 36
Software installation 17
SSID 47
System requirements 12

T
Time server 43
Troubleshooting guide 24

W
Warranty 68
WEP 48
Wi-Fi key 14, 47
Wi-Fi Protected Setup (WPS) 15, 59
WLAN antenna 16
WLAN filter 52
WLAN icon 23