SCHWAIGER®

Inhouse-Powerline

AV 200W

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.

Linux® is a registered trademark of Linus Torvalds.

Ubuntu® is a registered trademark of Canonical Ltd.

Mac® and Mac OS X® are registered trademarks of Apple Computer, Inc.

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.

CE

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.

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

June 2012

Contents

1 Introduction

This chapter gives an overview of the HomePlug technology and briefly introduces the adapter. A practical example is listed at the end of the chapter.

1.1 Was bedeutet “HomePlug”?

HomePlug (“Inhouse Powerline“) 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—HomePlug technology now attains speeds you would expect from other LAN technologies.

1.2 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 (from 1 to 13) 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 HomePlug) 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.

1.3 The AV200W

With the AV200W you can quickly and easily establish connections between WLAN, HomePlug and LAN.

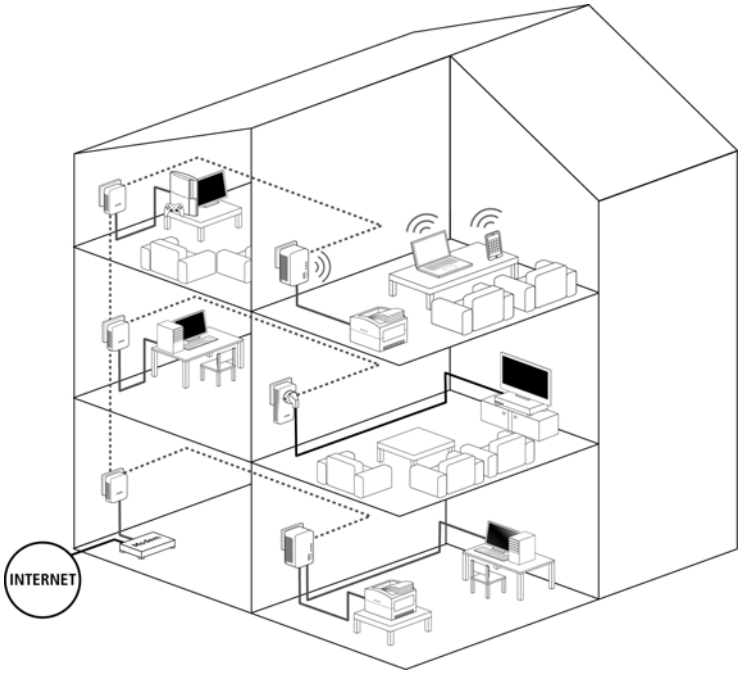
- As a WLAN access point, the adapter establishes communication between your WLAN devices and an existing LAN or HomePlug network. In this way, for example, you can expand your wireless network in no time to rooms that otherwise could not be reached by wireless.
- As a HomePlug device, the AV200W has three LAN jacks for directly connecting three network devices 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. By simply reconnecting your AV200W, you can expand or reconfigure your home network at any time, e.g. simply by taking the adapter along into another room to work.

1.3.1 Example application

The AV200W is a WLAN access point and makes the HomePlug network connected via the mains outlet available wirelessly to other client devices, such as laptops, IP radios or IP telephones.

This is particularly practical if not all client stations are within range of a WLAN access point, for example because concrete walls disrupt the signal. With HomePlug, however, various rooms can be easily connected via the mains supply. And using a AV200W, you can quickly and easily turn every mains outlet into a WLAN connection with excellent reception quality.

The following illustration shows how the AV200W is used to establish a connection to the Internet and within the home network for additional HomePlug devices and a router.



2 Installation

This chapter covers everything you need to know to set up your AV200W. It will explain connecting the device and its functions. We will also briefly introduce the included software and then guide you through its installation.

2.1 System requirements

- Operating systems: Windows XP (32/64 bit), Windows Vista Home Premium (32/64 bit), Windows 7 Home Premium (32/64 bit), Linux (Ubuntu), Mac (OS X) or all operating systems with network support
- Network connection

Please note that your computer or other device must feature a network adapter with a network port. To set up a HomePlug network, you need at least two HomePlug devices (200 Mbps or 500 Mbps).

2.2 Connection and display elements

2.2.1 Control lamps (LEDs)

LEDs		AV200W
Power	green	Lit steady when the adapter is ready for operation.
HomePlug	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	green	Lit steady when a connection to the WLAN network exists; flashes when data is being transmitted.
Ethernet		Lit steady when a connection to the Ethernet network exists; flashes when data is being transmitted.

2.2.2 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 standard WLAN key is the security ID of the AV200W. You will find the 16-character security ID on the label on the back of the housing.

WPS

With the WPS (Wi-Fi Protected Setup) 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 'WiFi Protected Setup (WPS)'.

HomePlug

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

- To encrypt your HomePlug network individually, press each encryption button on the connected devices for 1 second—within 2 minutes.
- To remove a HomePlug device from your network, press the encryption button of the corresponding device for at least 10 seconds.

For more details on HomePlug encryption, refer to Chapter 'Configuring the HomePlug network'.

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 1 second.
- To change the configuration of the AV200W back to the factory defaults, press the Reset button for 5 – 10 seconds. Keep in mind that all settings that have already been configured will be lost!

The reset button can be pressed using the tip of a ball-point pen.

2.2.3 Network jacks

The three LAN ports can be used to connect computers or other network devices to the AV200W via commercially available network cables.

2.2.4 WLAN antennas

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

2.3 Connecting the adapter

This section describes how to connect your AV200W to a computer or other network device.

① Use a network cable to connect the AV200W to the network port of your running computer or other network device.

② Plug the AV200W into a wall socket.

The outlet must be within reach of the connected network device.

The AV200W and the network device must be easily accessible.

In order to switch the AV200W off and disconnect it from the power supply, pull the plug out of the power outlet.

③ Once you have connected at least two HomePlug adapters as described above, your HomePlug network has been set up. To secure your network individually, continue with the configuration in the Chapter 'Configuring the HomePlug network'.

④ To install the software, insert the included CD-ROM in the CD drive of your computer.

⑤ The installation wizard will guide you through the software installation by clicking on the button Install AV200W Weblauncher.

⑥ You can find the installed software application under Start -> All Programs -> HomePlug -> HomePlug Wireless Configuration.

3 Network configuration

The AV200W 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. To integrate the AV200W into an existing HomePlug network for the first time only, use the encryption button (see Chapter 'Configuring the HomePlug network').

3.1 Calling up the built-in configuration interface

Call up the built-in online configuration interface under Start -> All Programs -> HomePlug -> HomePlug Wireless Configuration.

By default, you will come directly to the configuration interface. However, if a login password was set up via the option Device configuration -> Security*, you have to enter it first. Read more about this under 'Security'.*

3.2 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.

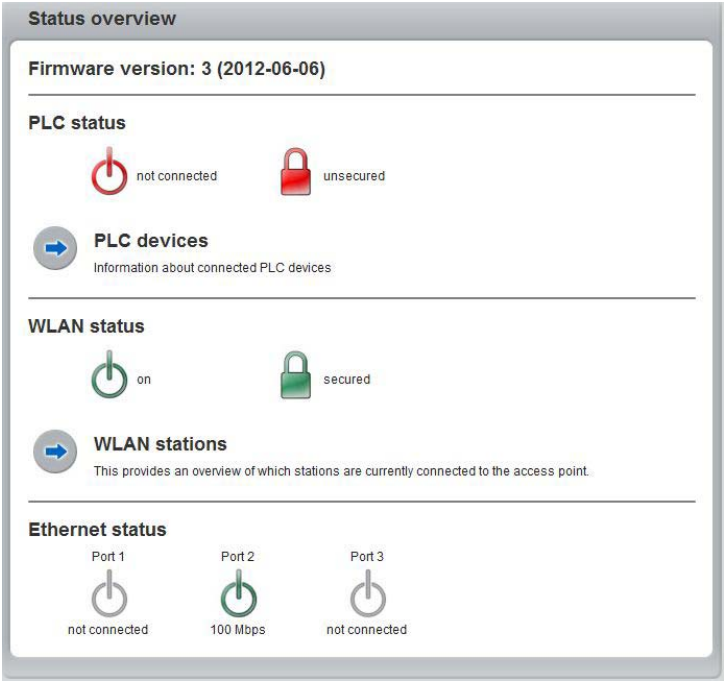
- Click Save to save the settings of the respective area of the configuration interface.
- Click Back to leave the respective area of the configuration interface.
- Select the desired language in the language selection list.

At first, after starting the configuration interface, the four central areas are displayed:

- In the Status overview area, you get general information about all connected HomePlug, WLAN and LAN devices.
- You can change or modify the various settings for your device 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 device here.

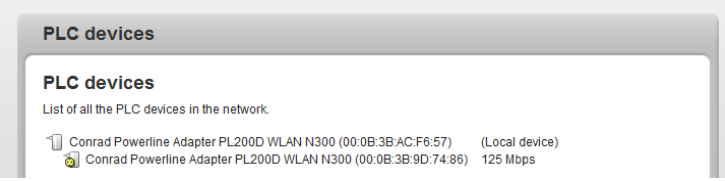
3.3 Status overview

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



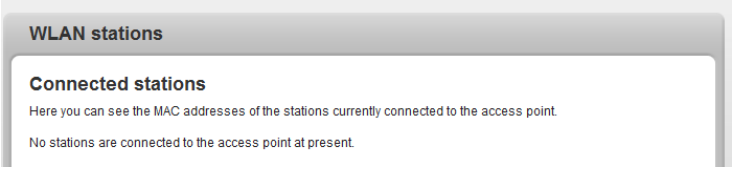
3.3.1 HomePlug status

To display all connected HomePlug devices, click either the Ready to operate icon or the HomePlug devices arrow. Each connected HomePlug device, regardless of whether it is connected locally or in the network, is displayed with its MAC address. Clicking the lock icon brings you directly to the HomePlug settings (see Chapter 'HomePlug settings').



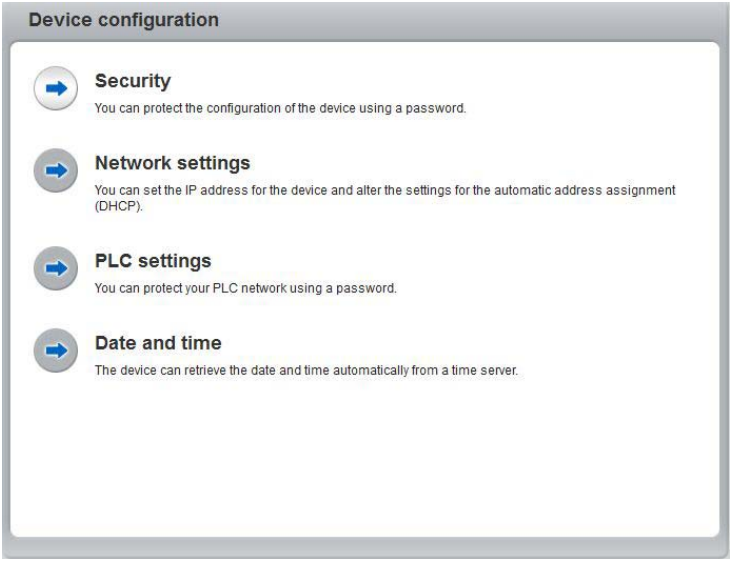
3.3.2 WLAN status

To display all connected WLAN devices, click either the Ready to operate icon or the WLAN stations arrow. Each connected WLAN client is displayed with its MAC address. Clicking the lock icon brings you directly to the WLAN filters area (see Chapter 'WLAN filters'), where you can configure settings for network security.



3.4 Device configuration

In the configuration area you can modify settings for security, network, HomePlug, date and time.

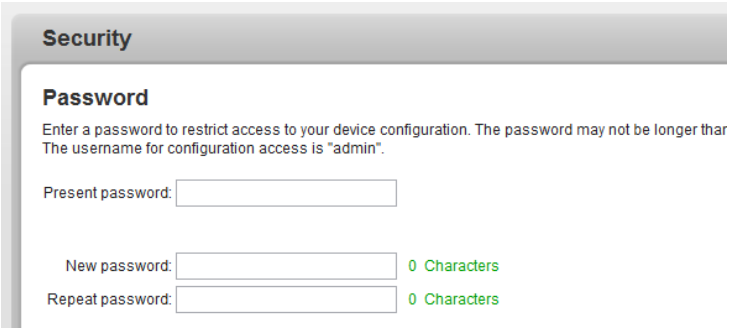


3.4.1 Security

In this area you can set a login password for access to the configuration interface of the AV200W.

By default, the built-in configuration interface of the AV200W is not protected with a password. After installing the AV200W, however, you should enable this protection by assigning a password to prevent access by a third party.

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!



If the configuration interface is called up again later, the following window appears first:

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

The admin user name cannot be changed.

3.4.2 Netzwork settings

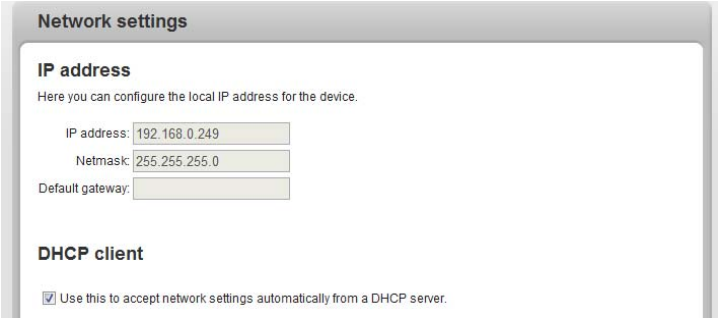
The AV200W also communicates via the TCP/IP protocol as a component of your home network. The IP address required for this can either be entered

manually as a static address 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 AV200W automatically receives an address from it.

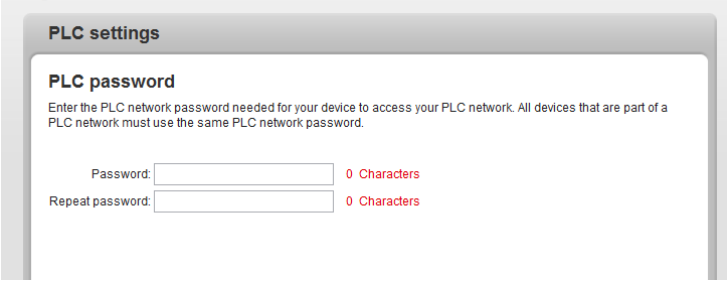
You can also assign a static IP address by making entries under **IP address** (e.g. '192.168.0.250') and **Netmask** (e.g. 255.255.255.0).



3.4.3 HomePlug settings

In a HomePlug network, all connected components must use the same password. The HomePlug password is normally defined once at the installation of your AV200W using the HomePlug encryption button (see Chapter 'Configuring the HomePlug network') or is taken over from the existing network.

The HomePlug standard password is **HomePlugAV**.

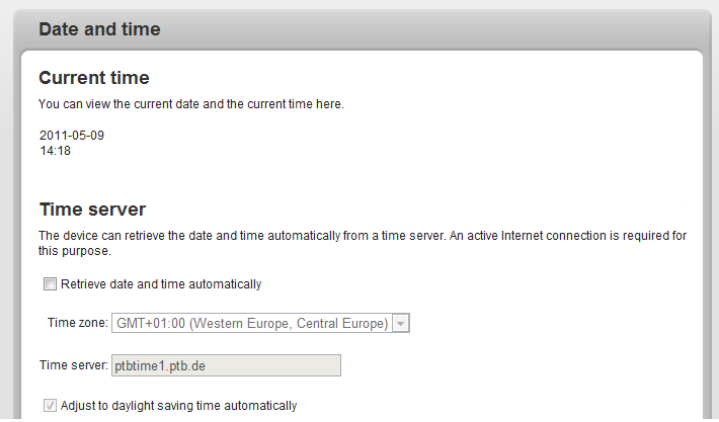


3.4.4 Time server

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.

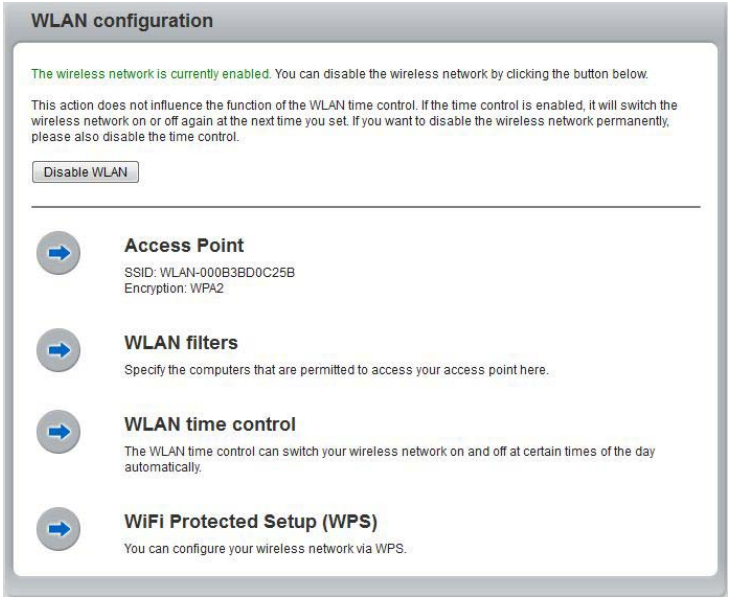
To see which Internet time server your computer uses to communicate, simply click the clock in the lower right corner of the screen and select the Internet time tab.

Enable the option **Retrieve date and time automatically**, so that the AV200W 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 AV200W automatically adjusts to daylight saving time.



3.5 WLAN configuration

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



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 'WLAN time control'.

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

3.5.1 Access point

Since the AV200W acts as an access point, you have to configure various parameters for your wireless network. If you would like, you can completely shut off the WLAN part of your AV200W, e.g. if you want to operate it exclusively as a simple HomePlug device via the built-in Ethernet connections. To do so, switch off the Enable WLAN option under Status overview -> WLAN stations, or simply press the WLAN ON/OFF button on the housing.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the AV200W. In this case, configure the device via Ethernet or HomePlug.

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 AV200W, 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.

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 AV200W 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.

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.

Without encryption, not only are all data transmitted from client computers to the AV200W 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.

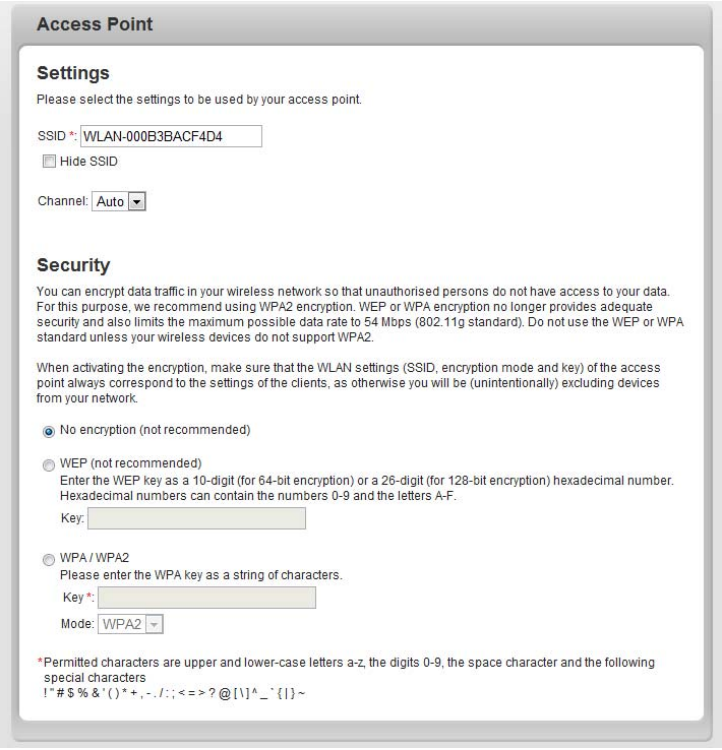
To secure the data transmission in your wireless network there are two security standards available.

- 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 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 AV200W 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

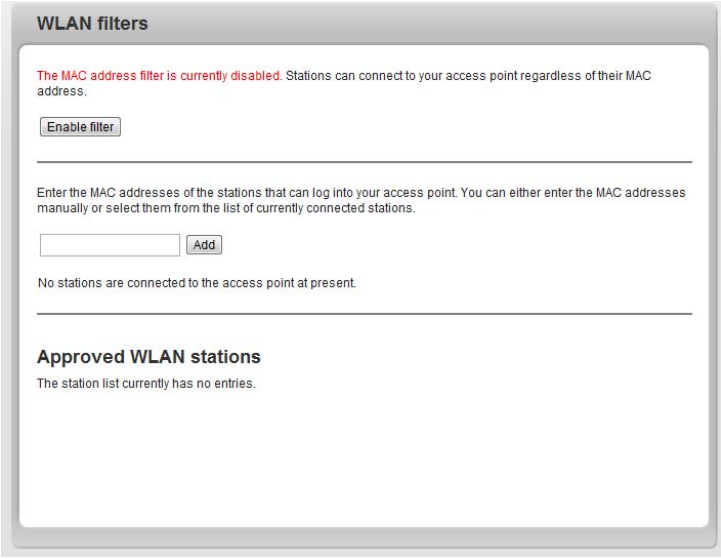
if possible. Use WEP only if one of your wireless terminal devices does not operate with a better standard.



3.5.2 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 AV200W 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 AV200W. Confirm each entry with Add. Network devices or stations connected to your AV200W are automatically listed, that is, to enable an already connected station for the AV200W, 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 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 AV200W 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!

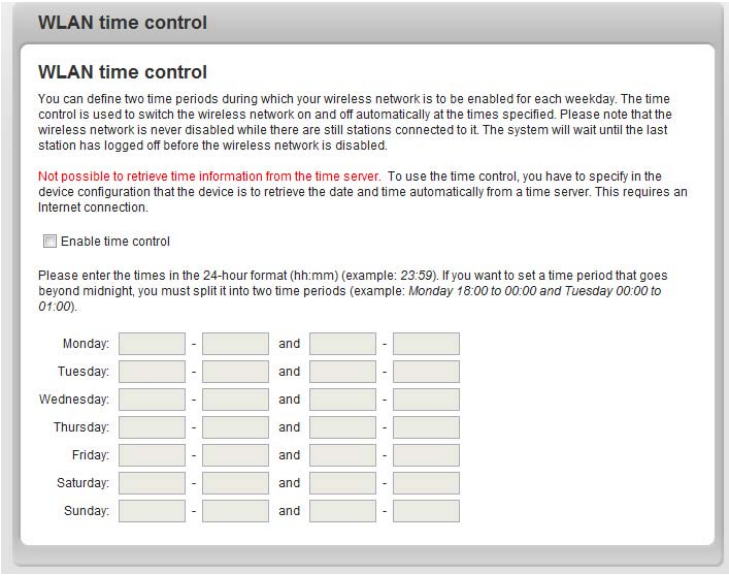
3.5.3 WLAN time control

To be able to use the WLAN time control, the option Retrieve date and time automatically *must be enabled under* Device configuration -> Date and time*. An active Internet connection is also required. (see Chapter 'Time server')*

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 AV200W registers connected stations, the wireless network remains enabled. The wireless network is not switched off until the last station has logged off.



3.5.4 WiFi 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 AV200W offers two different variants for transmitting these encryption keys:

WPS via PBC (Push Button Configuration):

① Start the encryption process on the AV200W

- ○ 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).

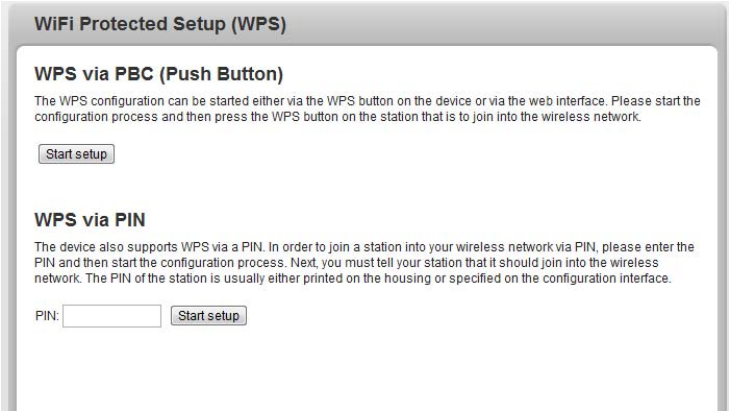
② Then press either the WPS key of the WLAN client you are adding or the WPS button on the configuration interface. Now the devices exchange

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 AV200W. 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.



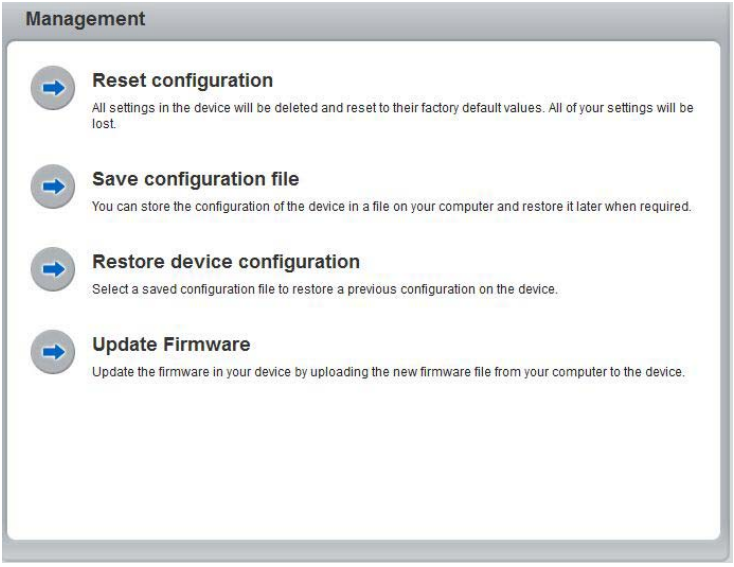
Use of the WPS process implies either WPA or WPA2. For that reason, keep in mind the following automatic settings depending on the encryption standard (also refer to Chapter 'Access point'), i.e.

- 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.

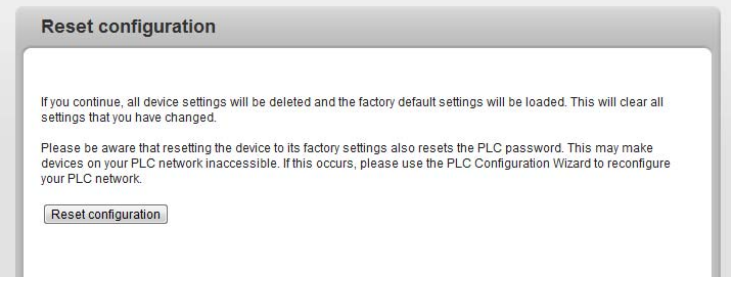
3.6 Management

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 AV200W.



3.6.1 Resetting the configuration

With the Management -> Reset configuration command, the AV200W is reset to the original factory defaults. In doing so, you lose your personal settings. The last-assigned HomePlug password for the AV200W is also reset to the HomePlug standard password HomePlugAV. To secure your HomePlug network individually again, reconfigure it by using the encryption button (see Chapter 'Configuring the HomePlug network').

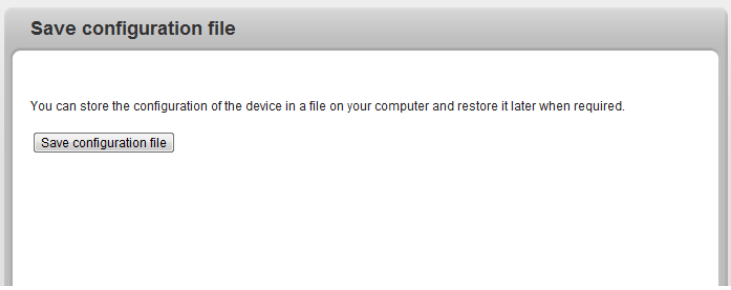


You can change the HomePlug password by using the configuration software in the Windows program group Start -> All Programs -> HomePlug -> HomePlug Wireless Configuration *or by using the* encryption button*.*

For backup purposes, all active configuration settings can be transmitted to your computer, stored there as a file and reloaded into the AV200W. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

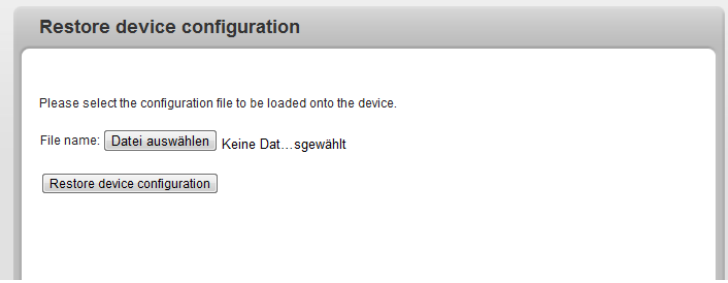
3.6.2 Saving a configuration file

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.



3.6.3 Restoring a configuration

An existing configuration file can be sent to the AV200W 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.



3.6.4 Refresh firmware

The firmware of the AV200W includes the software for operating the device. If necessary, Schwaiger 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.schwaiger.de, and download the appropriate file for the AV200W 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 AV200W restarts.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the AV200W via HomePlug or LAN rather than WLAN.

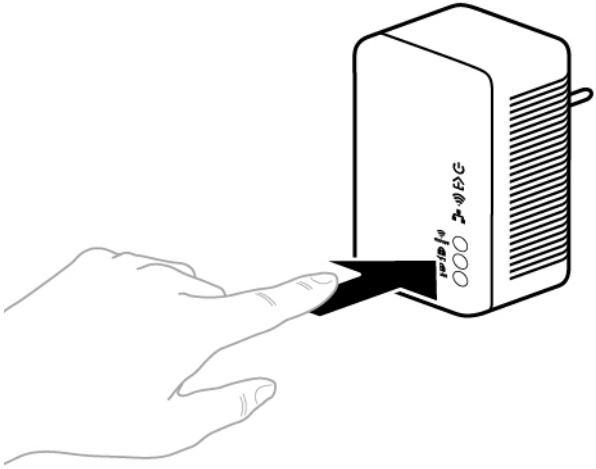
4 Configuring the HomePlug network

To set up custom encryption for your network—either using the **encryption button** or the **HomePlug Configuration Wizard**. Please note the following basic principle when choosing your encryption method:

- In PLC networks, data encryption is as simple as touching a button, since all corresponding PLC devices are equipped with an encryption button.
- For PLC networks that **include devices with and without encryption buttons**, data encryption must be set up using the **HomePlug Configuration Wizard**.

4.1 Encrypting the PLC network at the touch of a button

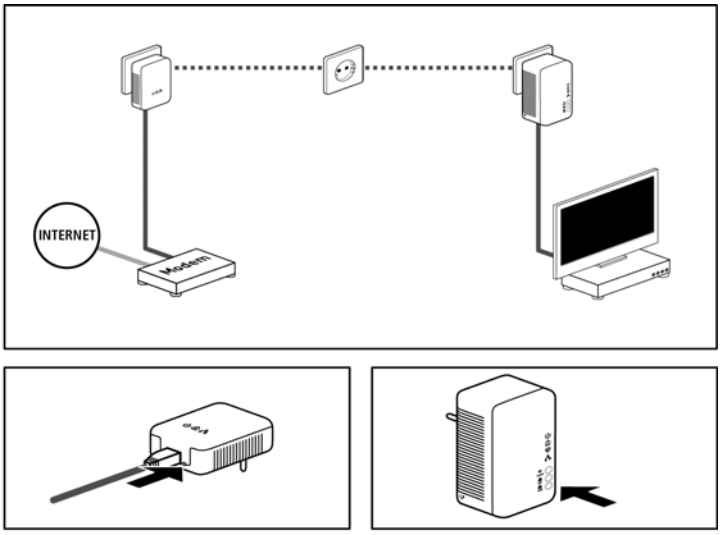
To encrypt a PLC network simply press the PLC button that is located on the device. Pressing this button will encrypt your network with a randomly generated password.



Adapters cannot be configured while in Standby mode.

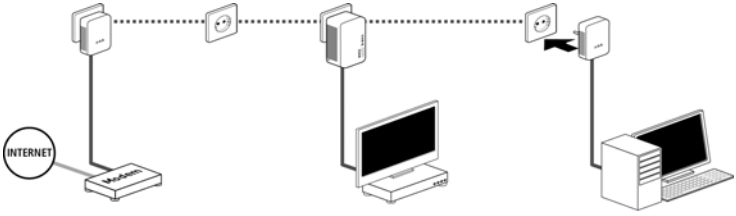
The following section contains exact instructions on the basis of possible network scenarios:

Encrypting a new PLC network consisting of two PLC adapters



Once both adapters have been successfully connected, press each encryption button for one second within two minutes of one another. That's it! Your PLC network is now protected against unauthorized access.

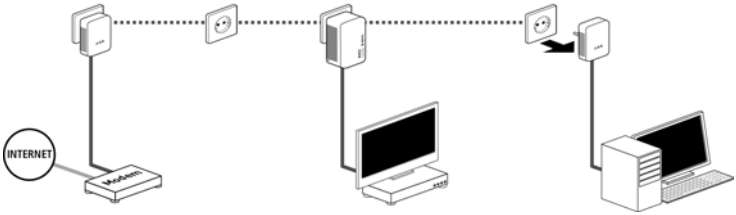
Expanding an existing PLC network with a new AV200W



If you have already secured your existing PLC network using the encryption button, use the same method to integrate other adapters. Once you have successfully connected the new AV200W, first press the encryption button of one of your network's existing adapters (one second), then press the encryption button of your new AV200W (one second) within two minutes. That's it! The new AV200W is now integrated in your network.

To integrate additional adapters in your network, repeat the above steps.

Excluding a AV200W from your network



To exclude a AV200W 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 adapter in a different AV200W network, follow the steps described above, depending on whether you are setting up a new network or adding the adapter to an existing one.

5 Appendix

5.1 Technical data

Standards	Wireless spezification IEEE 802.11b,g,n (2.4 GHz Single Band) HomePlug standard AV Ethernet standard IEEE 802.3/x/u, Auto MDI /MDI-X
Media access	Wireless 802.11: CSMA/CA, EDCA Ethernet 802.3: CSMA/CD HomePlug AV: CSMA/CA
Protocols	DHCP (Client), APIPA, Auto IP, ARP, ICMP, TCP/IP, UDP (IP), WMM 802.11e, Ethernet Bridge 802.1D
Modes	Access point with WEP, WPA (TKIP), WPA2 (AES)
Transmission speed	200 Mbps over the power supply grid 300 Mbps over wireless
Transmission method	Asynchronous
Modulation	OFDM - 1155 carriers, 1024/256/64-QAM, QPSK, BPSK via power grid Wireless: 802.11b: DSSS (Direct Sequence Spread Spectrum) 802.11g: OFDM (Orthogonal Frequency Division Multiple-xing) 802.11n: OFDM (Orthogonal Frequency Division Multiple-xing)
Range	300 m over the power supply grid up to 300 m over wireless
Security	128Bit AES encryption over the power supply grid WEP, WPA (PSK), WPA2 (PSK), TKIP over wireless
LEDs	4 LEDs: Power Powerline Link/Act WLAN On/Act ETH Link/Act
LAN ports	HomePlug: EURO mains plug WLAN: internal 2.4 GHz antennas Ethernet: three RJ45 (IEEE 802.3u/ 10/100 Mbps)
Power consumption	Maximum 0.13A with: Maximum: 7W Typical: 5.6W
Power supply	AC 230 V, 50 Hz

Environment	Humidity (non-condensing): 10-90% Storage: -25°C to 70°C Operation: 0°C to 40°C
System requirements	Ethernet interface Windows XP (32/64 bit), Windows Vista (32/64 bit), Windows 7 (32/64 bit), Linux (Ubuntu), Mac (OS X)
Warranty	2 years

5.2 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 device. The adapter and the network device must be easily accessible.

- To switch off the device, pull the power plug.
- To disconnect the device from the power supply grid, pull the power plug.
- Do not keep the device in direct sunlight.
- Do not insert any objects into the openings of the device.
- 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.

5.3 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.

5.4 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.

MANUFACTURER INFORMATION

Dear customer,
should you require technical assistance and your dealer or installer was not able to help, please contact our technical support.

Schwaiger GmbH
Wuerzburger Straße 17
90579 Langenzenn
Hotline: +49 (0) 9101 702-299
www.schwaiger.de
info@schwaiger.de

Business hours:

Monday to Thursday:	08:00 am - 05:00 pm
Friday:	08:00 am - 02:30 pm

SCHWAIGER®