APR222ac

Installation Manual

Legal Notice

Warranty

This publication is subject to change.

Table of Contents

Chapter 1 Introduction

The new generation of access points is manufactured in an environmentally friendly manner and complies with the RoHS directive. They support the latest WLAN technology and are meant to be used in a professional environment.

Safety notices

The *safety precautions* brochure, supplied together with your device, tells you all you need to know when using your access point.

Installation

The *Installation* on page 2 chapter shows you how to connect the device.

Configuration

The *Basic Configuration* on page 6 chapter describes the preliminary actions that need to be carried out for config-uration purposes. Later on, you will find instructions on how to access your device from a Windows PC (using a cur-rent web browser) and how to select basic settings.

Password

If you already know how to configure Teldat devices and you want to get started right away, all you really need to know is the preset user name and password.

User Name: *admin*

Password: *admin*

> ☞ **Note**
>
> Remember to change the password after logging in for the first time. All Teldat devices are supplied with the same one, which means they are not protected against unauthorized access until you change said password. Chapter *Modify system password* on page 10 shows how to change it.

Workshops

Step-by-step instructions for the most important configuration tasks can be found in the separate *Application Work-shop* guide for each application. This can can be downloaded from the *www.bintec-elmeg.com* website (under **Solu-tions)**.

Chapter 2 Installation

> **Note**
>
> Please read the safety notices carefully before installing and starting up your device. These are sup-
> plied together with the device.
>
> Refer to chapter *Technical Data* on page 14.

2.1 Setting up and connecting

> **Note**
>
> The device can be fitted with various antenna systems. External, screw-on standard antennas can be
> used (optional).
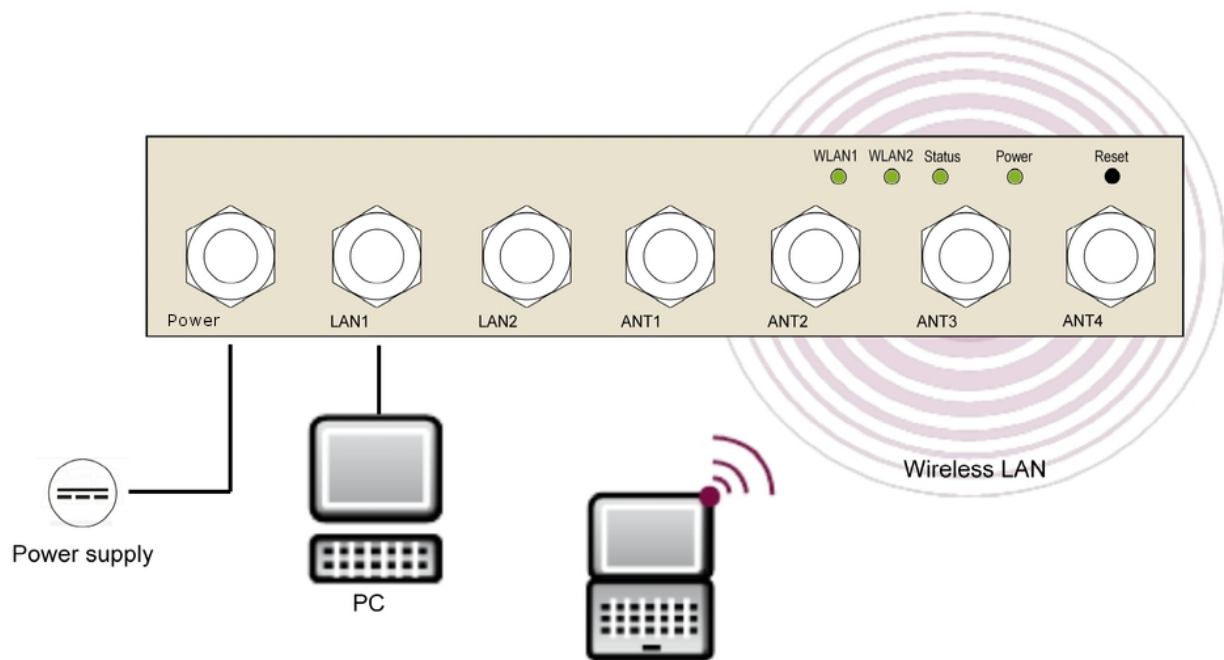
Fig. 1: **APR222ac** *- Connection options*

When setting up and connecting the device, carry out the following steps in order:

(1)   Antennas
        Connect the antenna connectors to the antennas to be used with the device.

(2)   Installation
        Thanks to the brackets in the housing, the access points can be mounted on the wall or ceiling.
        Wall-/Ceiling mounting
        To install the device on the wall/ceiling, the mounting brackets may be readily attached to the housing. They
        are screwed onto the wall/ceiling with six screws.

> ⚠ **Warning**
>
> Before drilling, make sure that there are no building installations nearby. If gas, electricity, water or
> waste water lines are damaged, you may endanger your life or damage property.

• Screw the mount to the wall with the 6 screws.

• Make sure the device connections are accessible.

Fig. 2: Wall/Ceiling mounting

(3)   Protective Earth connection

Protective Earth: In case of error, a terminal can be connected to an external protective conductor to avoid electric shocks.
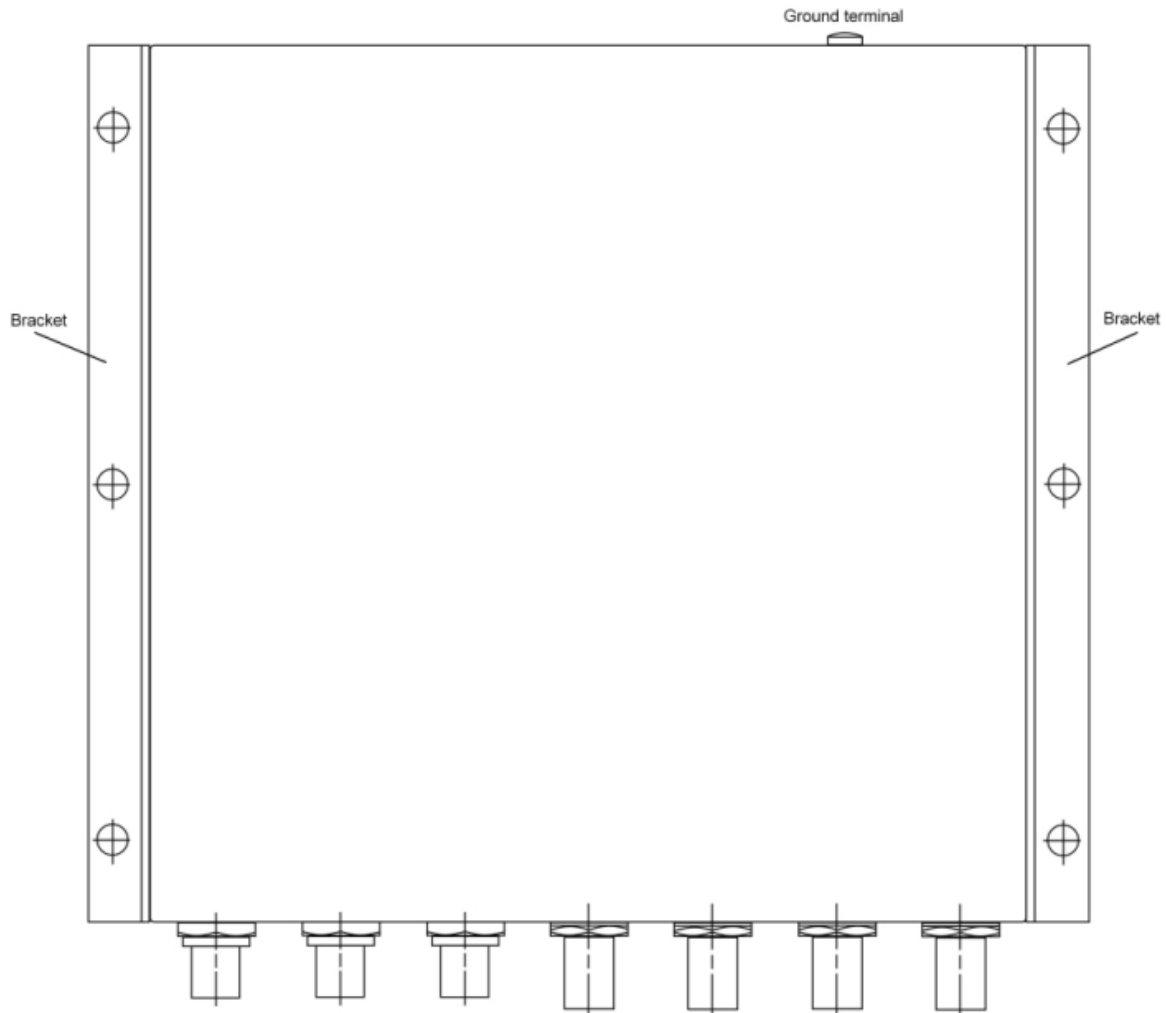
A protective earth cable with a minimum cross-section of 2.5mm^2 and a copper-tinned ring type crimp cable lug (e.g., DIN 46235 or DIN 46234) must be fastened to the rear of the housing (using the M4 bolt close to the IEC 417 Protective Earth Symbol). After installation, check for low ohmic connection between the housing and the protective earth connection.

> ⚠️ **Warning**
>
> This equipment must be grounded. Never unplug the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. When installing or replacing the unit, the ground connection must always be made first and disconnected last.

(4)   LAN

For the standard configuration of your device via Ethernet, connect port **LAN1** or **LAN2** to your LAN using an Ethernet cable. The device automatically detects whether it is connected to a switch or directly to a PC. Use just one of the ports **(LAN1** or **LAN2**). The second port is used to cascade a number of devices. If you use both Ethernet connections on the same switch, loops may form.

(5)   Power connection

The **APR222ac** is powered by a 110 V or 24 V nominal DC power source, depending on the model.

> **Note**
>
> Please verify device power input is valid for your power feeding.

There is no on/off switch or fuse. A label on the rear of the equipment contains the power supply information. Connect the device to a mains socket.

Use a power cord that matches the type of connector on your device and insert it in the appropriate socket. Now plug the power cord into a power socket. The power LED signals that your device is correctly connected to the power supply.

> **Warning**
>
> This equipment requires an external overcurrent protection device. To comply with safety regulations, either a 5.0 A time-lag fuse or a previously approved 1-amp thermo-magnetic circuit breaker (ABB-S281-UC-K-1 or equivalent) must be installed in the power line.

Observe the correct polarity of the DC connection, wrong polarity may destroy the external line fuse.

The device is now ready for configuration.

2.2 Anticorrosion measures to protect the metal parts of the device during transportation, storing or at its final location

As far as the metal housing is concerned, the **APR222ac** was designed to be placed in an enclosed location, protected from bad weather; never to be exposed or subject to these or any other extreme environmental conditions.

The housing is made out of electrogalvanized iron and has an external powder paint coating based on epoxy and polyester resins, added for aesthetic and anti-corrosion purposes. These characteristics give the housing the ability to withstand the effects of external corrosive agents (oxidation) to which the device might be exposed during transportation, storage or at its final location. As previously mentioned, these locations must always be indoors, sheltered, and not exposed to extreme environmental or meteorological conditions.

External paint's resistance to corrosion.

Humidity cabinet	DIN 50017	No change after 500 hours
Salt fog chamber	ASTM B117-97	500 hours

However, there are various considerations and measures that need to be taken into account during the transportation, storage and final deployment of devices to prevent the metal parts from rusting.

- Devices should be stored indoors or in places that are dry, clean and away from chemicals.
- Do not subject the devices to sudden rapid changes in temperature that could lead to condensation (which, in turn, will cause the metal parts in the devices to rust). Try to maintain the devices at as constant a temperature as possible.
- During transportation and storage, place the device on a wooden or plastic pallet in order to avoid direct contact with the ground.

Never store the device outdoors. If this is unavoidable, take the following steps and make sure the situation lasts as little as possible.

- Protect the devices with a waterproof cover (made out of plastic, canvas or a similar material).
- Try to leave some space between the devices and the waterproof cover to allow some air circulation.
- Keep the devices on wooden or plastic pallets and never in direct contact with the ground. Try to set the pallet at a slight angle to allow any water that might occasionally collect on the waterproof cover to drain off.

- Check the storage area regularly to make sure there is no moisture or con-
densation build-up on or around the stored devices.

As mentioned above, keep the device outdoors for as short a period as possible, especially in seasons with extreme temperatures that can accelerate the oxidization of metal parts.

2.3 Cleaning

You can clean your device easily. Use a damp or anti-static cloth. Do not use solvents. Never use a dry cloth since the electrostatic charge could cause electronic failure. Make sure that no moisture can enter the device and cause damage.

2.4 Support information

Teldat, S.A. offers a technical support service. The device software can be regularly updated for maintenance purposes and to add new features.

Contact information:

Web: www.teldat.com

Tel.: +34 918 076 565

Fax: +34 918 076 566

Email: support@teldat.com

Chapter 3 Basic Configuration

To configure the basic settings in your device, use **Dime Manager** (IP address assignment) and **GUI** (other configuration steps).

A step-by-step explanation is included below. A detailed online help system gives you extra support.

This user guide assumes you have the following:

* Basic knowledge regarding network structures.
* Knowledge of basic network terminology, such as server, client and IP address.
* Basic knowledge on how to use Microsoft Windows operating systems.

3.1 Presettings

3.1.1 Preconfigured data

There are three ways in which you can access the device to perform configuration tasks:

(a) Dynamic IP address

In ex works state, your device is set to DHCP client mode. This means that, when connected to your network, an IP address will automatically be assigned whenever a DHCP server is run. You may use this IP address (assigned by the DHCP server) to access your device for configuration purposes. For information on how to determine the dynamically assigned IP address, please see your DHCP server documentation.

(b) Fallback IP address

If you do not run a DHCP server, you can connect your device directly to your configuration PC and access it using the following fallback IP configuration (already predefined):

* **IP Address**: *192.168.0.252*
* **Netmask**: *255.255.255.0*

Make sure that the PC has a suitable IP configuration (see *Configuring a PC* on page 8).

(c) Assigning a fixed IP address

You can use **Dime Manager** to assign a new IP address and the required password to your device.

> ☞ **Note**
>
> Please note:
>
> If, to set the basic configuration, your device has obtained a dynamic IP address from a DHCP server, the fallback IP address (192.168.0.252) will be automatically deleted.
>
> On the other hand, if you set up a device connection over the fallback IP address (192.168.0.252) or use **Dime Manager** to assign an IP address, you will only be able to access your device over this IP address. This means that the device will no longer obtain a dynamic IP configuration over DHCP.

Use the following access data to configure your device in an ex works state:

* **User Name**: *admin*
* **Password**: *admin*

> **Note**
>
> All Teldat devices are delivered with the same username and password. This means they are not pro-
> tected against unauthorized use as long as the password remains unchanged. Make sure you change
> said password to stop your device from being unduly accessed!
>
> Section *Modify system password* on page 10 describes how to change your password.

3.1.2 Software update

Your device contains the system software version that was available at the time of production. Since then, more re-
cent versions may have been released. You can easily update your device using **GUI** through the *Maintenance-
>Software &Configuration* menu.

Section *Software update* on page 11 describes the updating process.

3.2 System requirements

Your PC must meet the following system requirements for configuration purposes:

• Internet Explorer or Mozilla Firefox.

• Installed network card (Ethernet).

• TCP/IP protocol installed (see *Configuring a PC* on page 8).

3.3 Preparation

To get ready for configuration, you need to...

• Obtain the data required for the basic configuration.

• Check whether the PC you need to use for configuration purposes meets the necessary requirements.

• Install the **Dime Manager** software, which gives you more tools to work with your device.

3.3.1 Gathering data

The main data for the basic configuration can be gathered quickly, as no information is required that needs in-depth
network knowledge. If applicable, you can use the example values.

Before starting the configuration process, you should gather data for the following purposes:

• IP configuration (mandatory if your device is in the ex works state).

• Configuration of a wireless network connection in Access Point mode (optional).

The following table gives examples of possible values for the necessary data. You can enter your personal data in
the "Your values" column, for future consideration.

If you configure a new network, you can use the values for IP addresses and netmasks that appear in the example.
When in doubt, ask your system administrator.

Basic configuration

To configure basic settings in your gateway, you need information on your network environment:

IP configuration of the access point

Access data	Example value	Your values
IP address of your access point	*192.168.0.252*	
Netmask of your access point	*255.255.255.0*	

Access Point mode

If you run your device in Access Point mode, you can set up the required wireless networks. To do this, you need the following data:

Configuration of a wireless network

Access data	Example value	Your values
Network Name (SSID)	*default*	
Security mode	*WPA-PSK*	
Preshared key	*supersecret*	

3.3.2 Configuring a PC

To access your device via the network and configure it, the PC used needs to meet some previous requirements.

- Make sure that the TCP/IP protocol is installed on the PC.
- Select the IP configuration that suits your configuration PC.

  The PC via which you want to configure the IP address for your device must be in the same network as your device.

Checking the Windows TCP/IP protocol

Follow these steps to check whether you have installed the protocol:

(1)   Click the Windows Start button and then **Settings** -> **Control Panel** -> **Network Connections** (Windows XP) or **Control Panel** -> **Network and Sharing Center** -> **Change Adapter Settings** (Windows 7).

(2)   Click on **LAN Connection**.

(3)   Click on **Properties** in the status window.

(4)   Look for the **Internet Protocol (TCP/IP)** entry in the list of network components.

Installing the Windows TCP/IP protocol

If you cannot find the **Internet Protocol (TCP/IP)** entry, install the TCP/IP protocol as follows:

(1)   First click on **Properties**, then on **Install** in the status window of the **LAN Connection**.

(2)   Select the **Protocol** entry.

(3)   Click **Add**.

(4)   Select **Internet Protocol (TCP/IP)** and click on **OK**.

(5)   Follow the on-screen instructions and restart your PC when you have finished.

Allocating an IP address to the PC

Allocate an IP address to your PC as follows:

(1)   Select **Internet Protocol (TCP/IP)** and click on **Properties**.

(2)   Choose **Use following IP address** and enter a suitable IP address, its matching netmask, your default gateway and your preferred DNS server.

If you run a DHCP server in your network, you can click on the default Windows settings **Obtain IP address automatically** and **Obtain DNS server address automatically**.

Your PC should now meet all the requirements needed in order to configure your device.

3.4 IP configuration

In the ex works state, your device is configured in DHCP Client mode and dynamically receives an IP address if you run a DHCP server in your network. Otherwise, connect your device directly to the configuration PC and use fallback IP address *192.168.0.252*.

Alternatively, you can use **Dime Manager** to assign a required fixed IP address.

To do this, install the program on your configuration PC.

After installation, carry out the following steps to configure an IP address on your device:

(1) Start the **Dime Manager** from the Windows Start menu: **Start -> Programs ->Dime Manager**.
The **Dime Manager** initial screen appears:
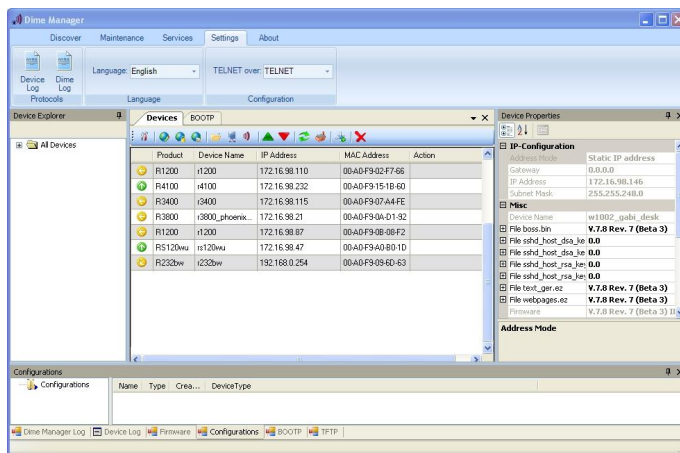
Fig. 3: **Dime Manager** - *initial screen*
The **Dime Manager** detects the devices installed in the network.

(2) Double click on the device you want to configure from the list.
The following dialog box appears:

Fig. 4: IP address allocation using **Dime Manager**

(3) Enter the network parameters (**Device name**, **IP address**, **Netmask** and **Gateway**) and click on **OK**.

> **Note**
>
> The maximum length of the Device name parameter is 32 characters.
>
> The Device name parameter may only contain letters "a"-"z", "A"-"Z", digits "0"-"9", a dash "-" and a dot ".". The first character must be a letter, and the last character cannot be a dot (".") or dash ("-"). A single character cannot be used as name.

Your device can now be reached over the Ethernet with its IP address using a web browser. It may now be configured.
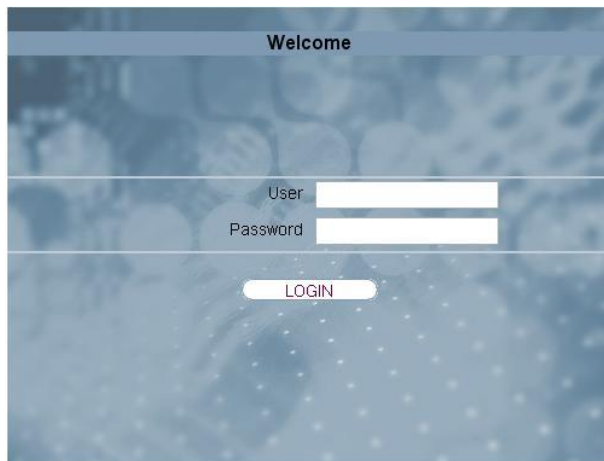
GUI Call up

Fig. 5: **GUI** *Login*

Start the configuration interface as follows:

(a)   Enter the IP address of your device in the address line of your web browser.

   With a DHCP server:
   • The IP address that the DHCP server assigned to your device.

   Without a DHCP server:
   • With direct connection to the configuration PC: fallback IP address *192.168.0.252*.
   • The fixed IP address assigned via **Dime Manager**.

   Press the **Enter** (**Return**) key.

(b)   Enter **admin** in the User field and **admin** in the Password field.

3.5 Modify system password

All Teldat devices are delivered with the same username and password. As a result, and for as long as said password remains unchanged, they are not protected against unauthorized use. Make sure you change the password to prevent your device from being unduly accessed!

Proceed as follows:

(a)   Go to the System Management ->Global Settings Settings->Passwords menu.

(b)   Enter a new password under System Admin Password.

(c)   Enter the new password again under Confirm Admin Password.

(d)   Click on **OK**.

(e)   Store the configuration using the **Save configuration** button on top of the navigation menu.

Note the following rules on password use:

• The password should not be easily guessed. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.

• The password should contain at least one character that is not a letter (special character or number).

• The password should be at least 8 characters long.

• Change your password regularly, e.g., every 90 days.

3.6 Setting up a wireless network

Follow these steps to use your device as an access point:

(1) In **GUI**, select the **Assistants**->**Wireless LAN** menu.

(2) Follow the steps shown by the wizard. The wizard has its own online help service, offering all the information you may require.

(3) Store the configuration using the **Save configuration** button (on top of the navigation menu).

Configuring the WLAN Adapter under Windows XP

After installing the drivers for your WLAN card, Windows XP sets up a new connection in the network environment. Follow these steps to configure the Wireless LAN connection:

(1) Click on **Start** -> **Settings** and double-click on **Network Connections** -> **Wireless Network Connection**.

(2) On the left-hand side, select **Change Advanced Settings**.

(3) Go to the **Wireless networks** tab.

(4) Click on **Add**.

Proceed as follows:

(1) Enter a **Network Name**, e.g. *Client-1*.

(2) Set **Network Authentication** to *WPA2-PSK*.

(3) Set **Data Encryption** to *AES*.

(4) Under **Network Key** and **Confirm Network Key**, enter the configured pre-shared key.

(5) Exit each menu with **OK**.

> ☞ **Note**
>
> Windows XP allows several menus to be modified. Depending on the configuration, the path to the wireless network connection you want to configure may be different to that described above.

Configuring the WLAN Adapter using Windows 7

A pop-up window informs you about all wireless networks within reach. All you have to do is to configure your connection.

(1) First, click on the WLAN icon in the system tray of the task bar. Windows 7 then displays all wireless networks within your reach.

(2) Select the VSS of your device and click on **Connect**.

(3) In the opening window, enter the pre-shared key you have configured for your VSS and click on **OK**.

3.7 Software update

The range of functions of Teldat devices is continuously being extended. Teldat SA makes them available to you free of charge. Checking for new software versions and the installation of updates can be carried out easily via **GUI**. An Internet connection is necessary to perform an automatic update.

Proceed as follows:

(1) Go to the **Maintenance -<Software &Configuration** menu.

(2) Under **Action**, select **Update System Software** and, under **Source Location**, **Latest Software from Update Server**.

(3) Confirm by clicking on **Go**.

The device will now connect to the Teldat SA download server and check whether an updated version of the system software is available. If so, your device will be updated automatically. When installation of the new software is complete, you will be invited to restart the device.

> **Caution**
>
> After clicking on **Go** to confirm, the update cannot be aborted. If an error occurs during the update, do not re-start the device: contact support instead.

Chapter 4 Reset

If the configuration is incorrect or your device cannot be accessed, you may use the **Reset** button to reset the device to the ex works standard settings.

All existing configuration data will be erased!

To do this, follow these steps:

(1)   Keep the **Reset** button pressed for approximately 30 seconds.

(2)   Look at the LEDs:
       - While the Status LED is permanently lit, the device runs through the reset and boot sequence.
       - As soon as the Status LED signals normal operation again (blinking), the reset is complete. Release the **Reset** button.

You can now configure your device again, as described in *Basic Configuration* on page 6.

> **Note**
>
> If you delete the boot configuration using **GUI**, all passwords will also be reset and the current boot configuration deleted. Next time, the device will boot with the standard ex works settings.

Chapter 5 Technical Data

This chapter summarizes all the hardware properties of the **APR222ac** device.

5.1 General product features

General product features cover performance aspects and the technical prerequisites for the installation and operation of your device. The following table summarizes these features:

General Product Features

Property	Value
Dimensions and weights:	
Equipment dimensions without cable (W x L x H)	ca. 212 x 212 x 40 mm plus 30 mm mounting kit (2x15mm).
Weight	Approx. 2,600 g.
Material	Paint-coated galvanized iron sheet.
LEDs	4 (1x Power, 1x Status, 2x WLAN).
Power consumption of the device	Max. 20 W.
Voltage supply	Integrated power supply. Galvanic isolation, 110 V DC or 24 V DC (depending on the model) -30 % + 25 % (power supply according to EN 50 155, except for 10 ms power interruption at full operation).
Environmental requirements:	
Ingress Protection Rating	IP 30 (Solid particle protection >2.5mm).
Storage temperature	-40 °C to +85 °C.
Room temperature	EN 50155 Class T3: -25...+70°C / +85°C 10 min.
Relative atmospheric humidity	EN 50155: annual average value <= 75 %, at 30 days per year 95 %.
Available interfaces:	
WLAN	2 x radio modules for 802.11 ac, 2.4GHz or 5GHz, 2x2 MIMO.
Ethernet IEEE 802.3 LAN	10/100/1000BaseT(X) M12 (8-pin).
Available sockets:	
Ethernet interface	2 x 8-pole female M12 socket.
Antenna sockets	Each radio has two female N-type antenna sockets (a total of four antenna sockets). ANT1 is internally connected to CH1 and ANT 2 is internally connected to CH0 at radio module 1. ANT3 is internally connected to CH1 and ANT 4 is internally connected to CH0 at radio module 2.
Power supply socket	4-pole male M12 socket.
Buttons	Reset.

To ensure safe operation, **APR222ac** devices have a protective earth connection. The minimum cross-section of the earth lead should be 2.5 mm⊡ The distance between the device and the earth connection should be as short as possible.

5.2 LEDs

The LEDs show the radio status, radio activity and LED states of your device. The LED states are made up of LED combinations, further explained in detail in this chapter.

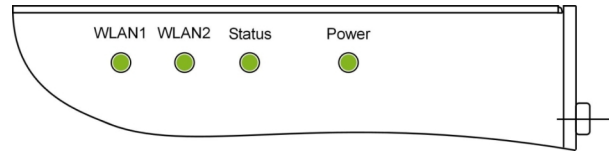The LEDs on the **APR222ac** device are arranged as follows:

Fig. 6: **APR222ac** *LEDs*

In operation mode, the LEDs display the following status information:

LED status display APR222ac

LED	Status	Information
Power (green)	on	The power supply is connected.
	off	No power supply.
Status (green)	off	The power supply is not connected. If other LEDs are on, also Error.
	on (static)	Error.
	on (blinking)	Ready.
WLAN 1/2 (green)	on (blinking slowly)	Free.
	on (static)	At least one client is registered.
	on (flickering)	At least one client is registered and there is data traffic.
	on (blinking fast)	BLD (Broken Link Detection) active.
	on (blinking fast)	5 GHz scan active.

5.3 Connectors

All the connections are located on the underside of the device.
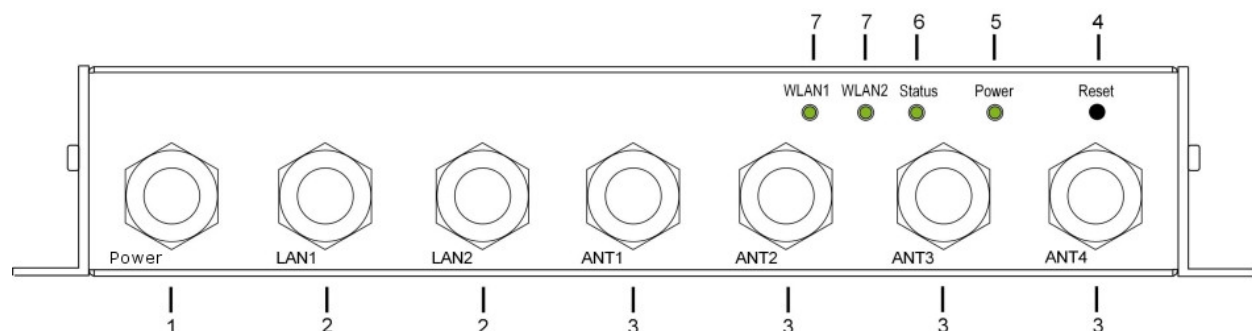
Fig. 7: Connectors

Underside of APR222ac

1	Power	Socket for 110V DC or 24V DC power supply, depending on the model.
2	LAN1 / LAN2	10/100/1000BaseT (X) M12 (8-pin) Port.
3	ANT1 - ANT4	Connections to screw in the external antennas.
4	Reset	Reset button performs restart (base plate of the device).
5	Power	LED (green).

6	Status	LED (green).
7	WLAN1 / WLAN2	LED (green).

5.4 Pin assignments

5.4.1 Ethernet interface

Your device has two Ethernet interfaces. These are used to connect individual PCs or other switches.

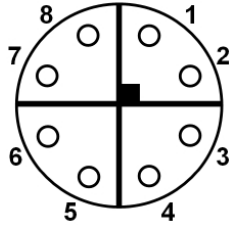The connection is made via an 8-pole female M12 socket.

Fig. 8: Ethernet 10/100/1000BaseT(X) M12 (8-pin) Port

The pin assignment is as follows:

Pinouts for the M12 (8-pin) Port

Pin	Connection
1	TRD 1+
2	TRD 1-
3	TRD 2+
4	TRD 2-
5	TRD 4+
6	TRD 4-
7	TRD 3-
8	TRD 3+

☞ **Note**

To install the LAN cable using the M12 Male cable connector, the maximum tightening torque allowed is 0,4Nm. Higher values may damage the M12 router connector. After its initial connection, frequent checkups must be carried out to ensure its correct fitting.

5.4.2 Power supply socket

The power supply socket is a 4-pole male M12 socket.
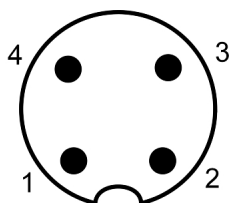
Fig. 9: 4-pole male M12 socket

Pinouts for the 4-pole M12 socket

Pin	Connection
1	+ VIN DC
2	+ VIN DC
3	0 V
4	0 V

> **Note**
>
> To install the power cable using the M12 cable connector, the maximum tightening torque allowed is 0,4Nm. Higher values may damage the router connector. After its initial connection, frequent checkups must be carried out to ensure its correct fitting.

5.5 Frequencies and channels

Different certification regulations apply around the world. ETSI standards (predominantly used in Europe) are the most common. For operation in Europe, please read the notes under R&TTE Compliance Information.

> **Note**
>
> National restrictions and requirements for the authorization and operation of wireless networks may apply. You must ensure that your network complies with these restrictions and requirements.
>
> The requirements for any country may change.Teldat SA recommends that you check with local authorities for the latest status of national regulations for both 2.4 and 5 GHz wireless LANs.
>
> The operating frequency is determined by the access point that the client is associated with. The client's operating frequency cannot be set manually. The access point must be properly configured to meet local regulations.

5.6 WEEE information

The waste container symbol with the »X« through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life.

Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist.

Le symbole se trouvant sur l'appareil et qui représente un conteneur à ordures barré signifie que l'appareil, une fois que sa durée d'utilisation a expiré, doit être éliminé dans des poubelles spéciales prévues à cet effet, de manière séparée des ordures ménagères courantes.

Il simbolo raffigurante il bidone della spazzatura barrato riportato sull'apparecchiatura significa che alla fine della durata in vita dell'apparecchiatura questa dovrà essere smaltita separatamente dai rifiuti domestici nei punti di raccolta previsti a tale scopo.

El símbolo del contenedor con la cruz, que se encuentra en el aparato, significa que cuando el equipo haya llegado al final de su vida útil, deberá ser llevado a los centros de recogida previstos, y que su tratamiento debe estar separado del de los residuos urbanos.

Symbolen som sitter på apparaten med den korsade avfallstunnan betyder att apparaten när den tjänat ut ska kasseras och lämnas till de förutsedda sortergårdarna och skiljas från normalt hushållsavfall.

Tegnet på apparatet som viser en avfallcontainer med et kyss over, betyr at apparatet må kastet på hertil egnet avfallssted og ikke sammen med vanlig avfall fra husholdningen.

Το σύμβολο που βρίσκεται στην συσκευή με το σταυρωμένο κοντέϊνερ απορριμμάτων σημαίνει, ότι η συσκευή στο τέλος της διάρκειας χρήσης της πρέπει να διατεθεί ξεχωριστά από τα κανονικά απορρίμματα στα γι' αυτό τον σκοπό προβλεπόμενα σημεία διάθεσης.

Symbolet med gennemkrydset affaldsbeholder på apparatet betyder, at apparatet, når det ikke kan bruges længere, skal bortskaffes adskilt fra normalt husholdningsaffald på et af de dertil beregnede bortskaffelsessteder.

Znajdujący się na urządzeniu symbol przekreślonego pojemnika na śmieci oznacza, że po upływie żywotności urządzenia należy go oddać do odpowiedniej placówki utylizacyjnej i nie wyrzucać go do normalnych śmieci domowych.

Het doorgehaalde symbool van de afvalcontainer op het apparaat betekent dat het apparaat op het einde van zijn levensduur niet bij het normale huisvuil mag worden verwijderd. Het moet bij een erkend inzamelpunt worden ingeleverd.

O símbolo com um caixote de lixo riscado, que se encontra no aparelho, significa, que o aparelho no fim da sua vida útil deve ser eliminado separadamente do lixo doméstico nos centros de recolha adequados.

Chapter 6 Access and Configuration

This chapter describes the access and configuration options.

6.1 Access options

• Via your LAN.

6.1.1 Access via LAN

Accessing via one of the Ethernet interfaces allows you to open **GUI** in a web browser (for configuration purposes) and to access your device via Telnet or SSH.

> ⚠️ **Caution**
>
> If you use **GUI** to carry out your initial configuration, using other configuration options to install addition-al settings may cause inconsistencies or malfunctions. Therefore, we recommend using **GUI** until the configuration process is completed. If you use SNMP shell commands, carry on using this configuration method.

6.1.1.1 HTTP/HTTPS

With a current web browser, you can use the HTML interfaces to configure your device.

The configuration can be set up using **GUI**. To do this, enter your device's IP address in the web browser's address field.

With a DHCP server:

• The IP address that the DHCP server assigned to your device.

Without a DHCP server:

• With direct connection to the configuration PC: fallback IP address *192.168.0.252*.
• The fixed IP address assigned via **Dime Manager**.

Press the **Enter (Return) key**.

6.1.1.2 Telnet

A Telnet connection allows you to access the SNMP shell and use other configuration options.

You do not need any additional software on your PC to set up a Telnet connection. Telnet is available for all operat-ing systems.

Proceed as follows:

Windows
(1)   Click on **Run…** in the Windows Start menu.
(2)   Enter **telnet <IP address of your device>.**
(3)   Click on **OK**. A window with the login prompt appears. You are now in the SNMP shell of your device.
(4)   Follow the steps in *Logging in for configuration* on page 21.

Unix

You can also set up a trouble-free Telnet connection on UNIX and Linux:
(1)   Enter **telnet <IP address of your device>** in a terminal. A window with the login prompt appears. You are now

in the SNMP shell of your device.

(2)   Follow the provisions set forth in *Logging in for configuration* on page 21.

6.1.1.3 SSH

In addition to the unencrypted and potentially viewable Telnet session, you can also connect to your device via an SSH connection. This is encrypted, so all the remote maintenance options can be carried out securely.

The following preconditions must be met in order to connect via SSH:

• The encryption keys needed must be available on the device.

• An SSH client must be installed on your PC.

Encryption keys

First of all, make sure the keys to encrypt the connection are available on your device:

(1)   Log in to one of the types already available (e.g., via Telnet - for login see *Login* on page 21).

(2)   Enter **update -i** for the input prompt. You are now in the Flash Management shell.

(3)   Call up a list of all the files saved on the device: **ls -al**.

If you see a display like the one shown below, the keys needed are already there and you can connect to the device via SSH:

```
Flash-Sh > ls -al

Flags Version Length Date Name ...

Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860

Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub

Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key

Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub

Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```

> **Note**
>
> The device generates a key pair for each of the algorithms (RSA and DSA), i.e., two files that, for each algorithm, must be stored in the flash (see example above).

If no keys are available, you have to generate these first. Follow these steps:

(1)   Leave the Flash Management shell by pressing **exit**.

(2)   Launch **GUI** and log on to your device (see *Calling up GUI* on page 23).

(3)   Make sure that *English* is the language selected.

(4)   Check the key status in the **System Management**->**Administrative Access**->**SSH** menu. If both keys are available, you'll see the *Generated* value under **RSA Key Status** and **DSA Key Status**.

(5)   If one or both of these fields contains the *Not Generated* value, you must generate the relevant key. To have the device generate the key, click on **Generate**.
       The device generates the key and stores it in the FlashROM. If *Generated* appears, the process was successful.

(6)   Make sure both keys have been duly generated. If necessary, repeat the process described above.

Login via SSH

To log in via SSH, follow these steps:

If you are sure that all the necessary keys are available on the device, check whether an SSH client is installed on

your PC. Most UNIX and Linux distributions install a SSH client by default. Additional software, e.g., PuTTY, usually has to be installed on a Windows PC.

Follow these steps to log in via SSH:

UNIX

(1) Enter **ssh <IP address of the device>** in a terminal. The login prompt window appears. You are now in the SN-MP shell of the device.

(2) Follow the provisions set forth in *Login* on page 21.

Windows

(1) The way an SSH connection is set up largely depends on the software used. Check the documentation related to the program you are using. The login prompt window will appear as soon as you have connected to the device. You are now in the SNMP shell of the device.

(2) Follow the provisions set forth in *Login* on page 21.

6.2 Login

With the help of certain access data, you can log in on your device and carry out different actions. The extent of the actions available depends on the authorizations of the user concerned.

A login prompt appears first, regardless of how you access your device. You cannot view any information on the device or change the configuration without authentication.

6.2.1 User names and passwords in ex works state

In the ex works state, your device is provided with the following user names and passwords:

User names and passwords in ex works state

Login name	Password	Authorizations
admin	admin	Read and change system variables, save configurations; use **GUI**.
write	public	Read and write system variables (except passwords) (changes are lost when you switch off your device).
read	public	Read system variables (except passwords).

The user name **admin** allows you to change and save configurations, and to modify access information (user names and passwords). For security reasons, passwords generally appear on the Setup Tool screen only as asterisks (not in plain text). User names, however, are displayed as plain text.

The security feature on your device allows you to read all configuration settings via the read user name, but not the access information. Therefore, it is impossible to log in with **read**, read the password of the admin user and log in as **admin** to make changes to the configuration.

> ⚠️ **Caution**
>
> All Teldat devices are delivered with the same username and password. As a result, and for as long as said password remains unchanged, they are not protected against unauthorized use. Section *Modify system password* on page 10 shows how to change passwords.
>
> Make sure you change the password to stop your device from being unduly accessed!
>
> If you have forgotten your password, you must reset your device to the ex works state (meaning your configuration will be lost).

6.2.2 Logging in for configuration

Set up a connection to the device. Section *Access options* on page 19 describes the access options.

GUI (Graphical User Interface)

Log in via the HTML surface as follows:

(1)   Enter your user name in the **User** field of the input window.

(2)   Enter your password in the **Password** field of the input window and confirm with **Return** (or click on the **Login** button).

The **GUI** status page opens in the browser.

SNMP shell

Log into the SNMP shell as follows:

(1)   Enter your user name (e.g., **admin)** and confirm with **Return**.

(2)   Enter your user password (e.g., **admin)** and confirm with **Return**.

Your device logs in at the input prompt, e.g., `w2002t-n:>`. The login was successful. You are now in the SNMP shell.

To leave the SNMP shell after completing the configuration, enter **exit** and press **Return**.

6.3 Configuration options

This chapter offers an overview of the various tools you can use to configure your device.

You can configure your device using:

- **GUI**
- An assistant.
- SNMP shell commands.

The configuration options available to you depend on the type of device connection:

Types of connections and configurations

Type of connection	Possible types of configuration
LAN	Assistant, **GUI**, shell command.

> **Note**
>
> To change the device configuration, you must log in with the **admin** user name. If you do not know the password, you cannot make any configuration settings. This applies to all types of configuration.

6.3.1 GUI for advanced users

GUI is a web-based graphic user interface that you can use on any PC with an up-to-date web browser via an HTTP or HTTPS connection.

GUI allows you to perform all configuration tasks easily and conveniently. It is integrated in your device and is available in English. Other languages may be available for download from *www.teldat.com* and installed on your device.

The settings you carry out using **GUI** will take effect upon pressing the **OK** or **Apply** menu buttons. You do not have to restart the device.

If you finish and want to save your settings as the boot configuration to be loaded when you reboot your device, click on the **Save configuration** button.

You can also use **GUI** to monitor the critical operating parameters of your device.

Fig. 11: **GUI** *home page*

6.3.1.1 Calling up GUI

(1)   Make sure the device is connected and switched on and that all necessary cables are correctly connected (see *Technical Data* on page 14).

(2)   Check the settings of the PC you want to use to configure your device (see *Configuring a PC* on page 8).

(3)   Open a web browser.

(4)   Enter *http://192.168.0.252* (or the IP address dynamically assigned by your DHCP server, or the address statically assigned by you using **Dime Manager**) in the web browser's address field.

(5)   Enter **admin** in the User field and admin in the Password field and click on **LOGIN**.

You are now in the status menu of your device's **GUI**.

6.3.1.2 Operating elements

GUI window

The **GUI** window is divided into three areas:

• The header.

• The navigation bar.

• The main configuration window.
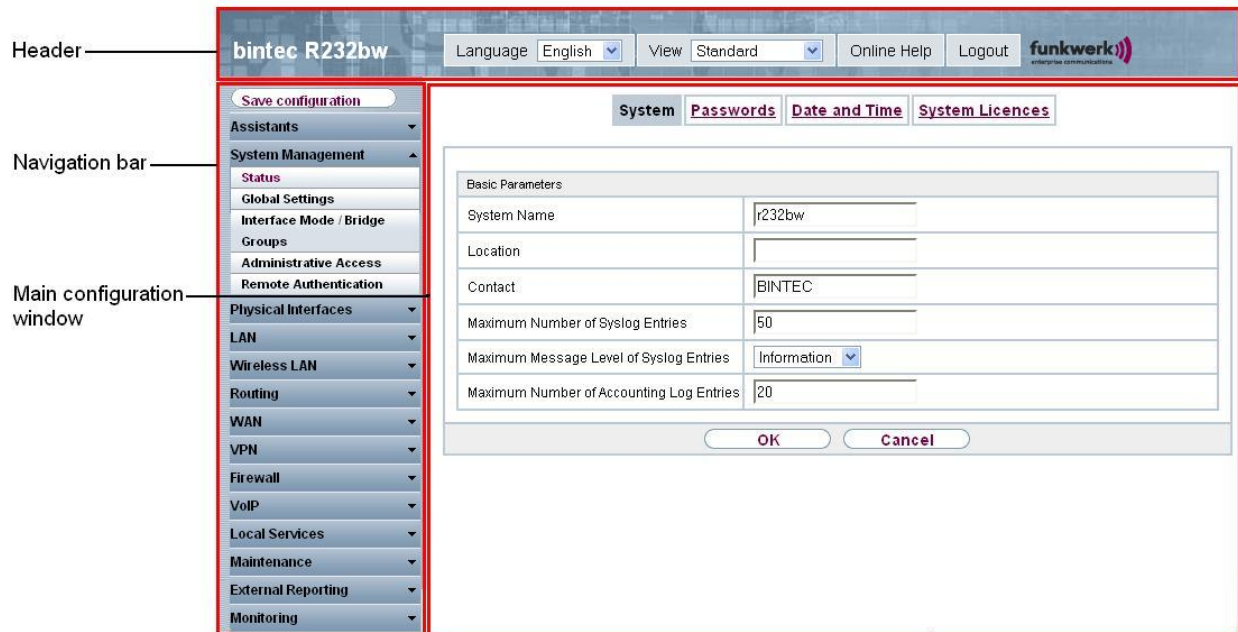
Fig. 12: Areas of the **GUI**

Header

Fig. 13: **GUI** *header*

GUI header

Menu	Position
Language English	**Language**: English is the only language currently available.
View Standard	**View**: Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.
Online Help	**Online Help**: Click this button if you need help with the current menu. A description of the sub-menu you are currently at will be displayed.
Logout	**Logout**: If you want to end the configuration, click on this button to log out of your device. A window opens and offers you the following options: • Save configuration, save previous boot configuration, then exit. • Save configuration, then exit. • Exit without saving.

Navigation bar

Fig. 14: Save Configuration button
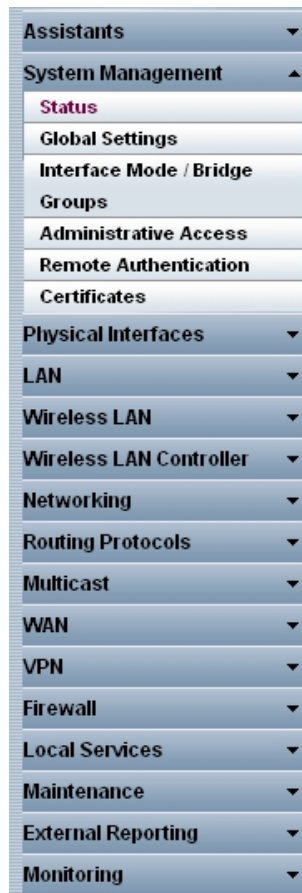
Fig. 15: Menus

The **Save configuration** button is found in the navigation bar.

If you save the current configuration, you can save it as the boot configuration and file the previous boot configuration as a backup.

If you click on the **Save configuration** button in the **GUI**, you will be asked "Do you really want to save the current configuration as a boot configuration?"

You have the following two options:

• **Save configuration**, i.e. save the current configuration as the boot configuration.
• **Save configuration and backup previous boot configuration**, i.e. save the current configuration as the boot configuration and file the previous boot configuration as backup.

If you want to load the previously filed boot configuration into your device, go to the Maintenance-> Software & Configuration menu, select **Action = Import configuration** and click on **Go**. The backup filed is used as the ccurrent boot configuration.

If you want to load the previously filed boot configuration into your device, go to the **Maintenance**->**Software &Configuration**menu, select **Action** = *Import configuration* and click on **Go**. The backup filed is used as the current boot configuration.

The navigation bar also contains the main configuration menus and their sub-menus.

Click the main menu you require. The corresponding sub-menu then opens.

If you click the sub-menu you want, the entry selected will be displayed in red. All the other sub-menus will be closed. You can see the sub-menu you are in at a glance.

Status page

If you call the **GUI**, the status page of your device is displayed after you log in. The most important data of your device can be seen on this at a glance.
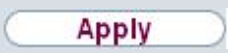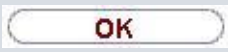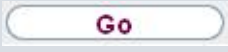
Main configuration window

The sub-menus generally contain several pages. These are called using the buttons at the top of the main window. If you click on a button, the window is opened with the basic parameters. You can extend this by clicking on the **Advanced Settings** tab, which displays the additional options.

Configuration elements

The following buttons trigger the actions you can perform when configuring your device with **GUI**:

GUI buttons

Button	Position
Apply	Updates the view.
Cancel	If you do not want to save a newly configured list entry, cancel this and any settings made by pressing **Cancel**.
OK	Confirms the settings of a new entry and the parameter changes in a list.
Go	Immediately activates the configured action.
New	Calls the sub-menu to create a new entry.
Add	Inserts an entry in an internal list.

GUI buttons for special functions

Button	Position
Import	In the **System Management**->**Certificates**->**Certificate List** menu and the **System Management**->**Certificates**->**CRLs** menu, this button activates the sub-menus for certificate configuration or CRL imports.
Request	In the **System Management**->**Certificates**->**Certificate List** menu, this button activates the sub-menu for certificate configuration.

Various icons indicate the following possible actions or statuses:

GUI symbols

Symbol	Position
🗑	Deletes the list entry.
🔧	Displays the menu to change the settings of an entry.
🔍	Displays the entry details.
⬍	Moves an entry. A combo box opens and allows you to select the list entry in front of/after which a given entry is going to be placed.
📄	Creates another list entry first and opens the configuration menu.
⬇	Sets the status of the entry to Inactive.
⬆	Sets the status of the entry to Active.
🔵	Indicates "Dormant" status for an interface or connection.
🟢	Indicates "Up" status for an interface or connection.
🔴	Indicates "Down" status for an interface or connection.
🔴	Indicates "Blocked" status for an interface or connection.
🟡	Indicates "Going up" status for an interface or connection.
🔒	Indicates that data traffic is encrypted.

Symbol	Position
🖼️	Triggers a WLAN bandscan.
»	Displays the next page in a list.
«	Displays the previous page in a list.

You can select the following operating functions in the list view:

GUI list options

Menu	Position
Update Interval	Here you can set the interval in which the view is to be updated. To do this, enter a period in seconds in the input field and click on Apply.
Filter	You can have the list entries filtered and displayed according to certain criteria. You can determine the number of entries displayed per page by entering the required number in **View** x **per page**. Use the « and » buttons to move from one page to the next and back. Using certain keywords within the configuration parameters, you can filter by selecting the filter rule under**Filter in x <Option> y** and entering the search word in the input field. GO launches filter operation.
Configuration elements	Some lists contain configuration elements. This means you can change the configuration of the corresponding list entry directly in the list.

Automatic Refresh Interval 60   Seconds   Apply

Fig. 16: Configuration of the update interval

View 20   per page « » Filter in None ▾ equal ▾   Go

Fig. 17: Filter list

Structure of the GUI configuration menu
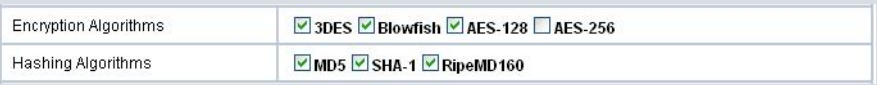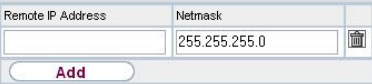
GUI menus include the following basic structures:

GUI Menu architecture

Menu	Position
Basic configuration menu/list	When you select a menu from the navigation bar, the basic parameter menu is displayed first. In a sub-menu made up of several pages, the menu containing the basic parameters is displayed on the first page. This contains a list of all the configured entries or the feature's basic settings.
Sub-menu New	Every menu that displays a list of all the configured entries has a **New** button. Click on it to display the configuration menu needed to create a new list entry.
Sub-menu 🔧	Click on this button to process the existing list entry. It takes you to the configuration menu.
Menu Advanced Settings	Click on this tab to display more configuration options.

The following configuration options are available:

GUI configuration elements

Menu	Position
Input fields	e.g., empty text field Text field with hidden input ●●●●●● Enter the data.
Radio buttons	e.g., Address Mode ⊙ Static ○ DHCP Select the corresponding option.
Checkboxes	e.g., activation by selecting checkbox ☐ Enabled Selection of several possible options Encryption Algorithms ☑ 3DES ☑ Blowfish ☑ AES-128 ☐ AES-256 Hashing Algorithms ☑ MD5 ☑ SHA-1 ☑ RipeMD160
Dropdown menus	e.g., Configured Speed / Mode Full Autonegotiation ▼ Full Autonegotiation ▼ Full Autonegotiation ▼ Full Autonegotiation ▼ Click on the arrow to open the list. Select the required option using the mouse.
Internal lists	e.g., Remote IP Address Netmask 255.255.255.0 🗑 Add Click on ⟨ Add ⟩. A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm using **OK**. Delete the entries by clicking on the 🗑 icon.

Display of options that are not available

Options that are not available (because they depend on the selection of other options) are generally hidden. If displaying these options proved helpful to make a configuration decision, they would appear greyed out and be impossible to select.

> ⚠ **Important**
>
> Please look at the messages displayed in the sub-menus. These provide information on incorrect configurations.
>
> **Warning symbols**
>
> | Symbol | Meaning |
> |--------|---------|
> | 🔴 | This symbol appears in messages about settings made with the Setup Tool. |
> | ⚠ | This symbol appears in messages about values that were incorrectly entered or selected. |
>
> Pay particular attention to the following message:
>
> "Warning: Changes not supported by the Setup Tool!" Using **GUI** can cause inconsistencies or mal-

functions. Therefore, it is recommended that you keep using the Setup Tool for configuration purposes.

6.3.1.3 GUI menus

Sub-menus contain configuration options for your device (displayed in the navigation bar found in the left-hand side of the window).

6.3.2 The setup tool for experts

The Setup Tool is a menu-controlled ASCII tool used to configure and manage your device. In addition to granting access to SNMP commands, it allows configuration parameters to be entered.

To start the Setup Tool, you can connect to the device any way you like. It does not matter whether you connect to the device via the LAN or via a serial connection.

Proceed as follows to start a Setup Tool session:

(1)   Log in to your device as **admin** (see *Logging in for configuration* on page 21).

(2)   Enter **setup** after the input prompt and press *Return*.

The main menu of the ASCII Setup Tool opens.

Setup Tool menu

The main menu layout may vary depending on the configuration level of your device. Every Setup Tool menu contains three areas:

• The menu line contains a navigation aid detailing your current position in the Setup Tools menu system. The system name of your device is also displayed. This is especially helpful if you are using several Teldat devices with different system names.

• The configuration window is where the actual entries are made and the respective settings displayed. Inverted colors show the field where the cursor is.

• The help line tells you how to move around in the current menu, the entries you can change, and suggests possible values for an entry.

Basically, a menu looks like this:

Fig. 18: Setup Tool menu

6.3.2.1 Menu navigation

You can use the following keys or key combinations to move about in the Setup Tool:

Navigation in the Setup Tool

Key combination	Meaning
Tabulator	Jumps to the next field menu.
Return key	Opens a sub-menu or activates a command (e.g., **SAVE**).
up or **down** (arrow keys)	Goes to the next or previous field in the menu (works with VT 100 emulation when using a terminal program).
left or **right** (arrow keys)	Shows next and previous field values (works with VT 100 emulation when using a terminal program).
EscEsc	**Esc** twice in succession: Returns to the previous menu. Changes are lost.
Space	Selects list entries to be deleted. The selected entries are marked with a D. Pressing *Space* again removes the selection. Selects possible variable values (same as arrow keys).
Ctrl - l	Updates display.
Ctrl - n	Jumps to the next field in the menu.
Ctrl - p	Jumps to the previous field in the menu.
Ctrl - f	Scrolls down in a list that cannot be displayed in full. A "-" sign at the bottom-right corner indicates the list has come to an end, while a "v" symbol indicates there is more to come.
Ctrl - b	Scrolls up in a list that cannot be displayed in full. A "-" sign at the top-right corner indicates the start of the list and a " ^ " symbol indicates there is more to come.
Ctrl - c	Exits the Setup Tool.

6.3.2.2 Menu commands

Browsing through the Setup Tool, you will notice that some menus have special command options, such as **DELETE**, **SAVE** and **CANCEL**. The meaning of the commands is explained below:

Buttons in the Setup Tool

Button	Meaning
ADD / **APPEND**	Adds a new item to a list. A sub-menu opens, allowing you to enter the desired settings.
CANCEL	Deletes all changes in the menu just displayed.
DELETE	Deletes, from a list, all entries selected with the *Space* bar. These changes become effective immediately.
OK	Confirms the changes in the current menu. These changes become effective when **SAVE** is pressed in the next menu.
SAVE	Saves all current menu entries and all the sub-menus in the working memory. These changes become effective immediately.
EXIT	Leaves the current menu and returns to the main menu. Any entries made are lost.

> **Note**
>
> To save the configuration to the flash memory, you must leave the Setup Tool in **Save as boot configuration and exit** mode.

6.3.2.3 Searching lists

Some Setup Tool menus contain lists with several entries (e.g., the VSS configuration menu, which lists all wireless networks):

```
WI1040n Setup Tool                                           bintec elmeg GmbH
[WLAN-1][WIRELESS]: Interface List                                    wi1040n


      Network Name              Status    Security  ACL-Filter  ifc     Cl.#
      ----------------------------------------------------------------------
       *Funkwerk-ec             disable   WPA PSK   disable     vss1-0   32






      ADD                    DELETE                 EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

Fig. 19: Setup Tool search

An incremental search function is provided (useful when searching for an item in very long lists).

Follow these steps:

(1)   Enter the first letter of the entry you are looking for, with the cursor located on a list entry. Entries can be made in upper or lower case.

(2)   If necessary, enter more characters to narrow down the search.

(3)   The *Backspace* or *Delete* key can be used to edit the search string.

The cursor automatically jumps to the first match it finds with the corresponding initial letters. The characters entered for the search are displayed in the help line at the bottom of the menu.

Do not enter invisible characters, such as *Tabulator* or *Space*, as they stop the search and could cause a function to execute.

> **Note**
>
> Make sure the cursor is positioned in a list element. The search cannot run if the cursor is located in a command field, e.g., **ADD** or **DELETE**.

In the menu shown above, the entries provide the following search results:

Search results

Input	Cursor jumps to entry
v or V	Visitors
bi, Bi, bI, BI	BigBoss
Department	**Department1** to **Department2**, on entering *2*

6.3.2.4 Changing the password

The following process applies to all passwords on your device: the access passwords for user names *admin*, *read* and *write*, the HTTP password, the PPP password and the provider password.

Any character may be used when entering a password. Passwords are only displayed as asterisks, even while changes are being made. The number of asterisks is the same as the number of characters in the password.

> **Note**
>
> To start your device's Setup Tool in a mode where passwords can be displayed in plain text and changed through one-time editing, enter **setup-p**. This option is only available if you have logged in with the *admin* user name. In the password field, the *backspace* key always deletes the complete entry, not just one character.

Follow these steps:

(1)   Select the password field in the desired menu and enter the new password.

(2)   The field switches to change mode and the Change Password message appears in the help line.

(3)   Now press *Return*, *Tabulator* or a *Cursor* key to confirm. The field changes to confirm mode and **Confirm Password** appears in the help line.

(4)   Now re-enter the new password and confirm by pressing *Return*, *Tabulator* or a *Cursor* key. If you have typed the new password correctly, the password is changed. The new password is saved on leaving the menu with the **SAVE** button. If you leave the menu by pressing **CANCEL** or **Esc Esc**, the password change is not saved. If both entries do not match, the field is reset to the old password and the help line shows the following message: "Password doesn't match. Try again."

6.3.3 SNMP shell

SNMP (Simple Network Management Protocol) sets the way you can access the configuration settings.

All configuration settings are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly from the SNMP shell via SNMP commands. This type of configuration requires a detailed knowledge of our devices.

6.4 BOOTmonitor

BOOTmonitor is only available over a serial connection to the device.

BOOTmonitor offers the following features, which you select by entering the corresponding number:

(1)   Boot System (reboot the system):
       The device loads the compressed boot file from the flash memory to the working memory. This happens automatically on starting.

(2)   Software Update via TFTP:
       The device performs a software update via a TFTP server.

(3)   Software Update via XMODEM:
       The device performs a software update via a serial interface with XMODEM.

(4)   Delete configuration:
       The device is reset to the ex works state. All configuration files are deleted and the BOOTmonitor settings are set to the default values.

(5)   Default BOOTmonitor Parameters:
       You can change the default BOOTmonitor settings, e.g., the baud rate for serial connections.

(6)   Show System Information:
       Shows useful information about your device, e.g., serial number, MAC address and software versions.

Devices go through different operating states when starting:

• Start mode.

- BOOTmonitor mode.

- Normal mode.

After some self-tests have been successfully carried out in the start mode, your device reaches the BOOTmonitor mode. The BOOTmonitor prompt is displayed if you are serially connected to your device.

```
Press <sp> for boot monitor or any other key to boot system


W1002 Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by bintec elmeg GmbH

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show System Information

Your Choice> _
```

Fig. 20: BOOTmonitor

Once the BOOTmonitor prompt is displayed, press the space bar in less than four seconds to use the BOOTmonitor functions. If you do not make said entry within four seconds, the device returns to normal operating mode.

> **Note**
>
> If you change the baud rate (the preset value is 9600 baud), make sure the terminal program used also uses this baud rate. If this is not the case, you will not be able to establish a serial connection.