Manual
Trap-Receiver 2x2 Digital

Typ	Trap-Receiver 2x2 Digital
Modell	#57656
Release	US 3.21 08/2012 PA

Subject to errors and changes:

Since we can make errors, none of our information should be used without verification. Please inform us of any mistakes or misunderstandings so that we can detect and eliminate them as quickly as possible..

Carry out work on and with W&T products only if it is described here and you have fully read and understood the manual. Unauthorized actions can result in hazards. We are not liable for the consequences of unauthorized actions. When in doubt, please contact us or your dealer first!

Content

1. Introduction

The **Trap-Receiver** can receive **SNMP-Traps** and **Syslog-Messages** and performs then previously defined actions.

The device has two digital outputs, which can be used for local alerting. Other messages (e.g. Mail, FTP, TCP-Message...) are also available in case of alarm.

Via the integrated webserver each webbrowser can be used to request websites from the device, which show the current state of the alarms. Also the configuration of the device is done via the browser.

2. Startup

Just a few steps are needed to incorporate the Trap-Receiver into your network and get it running.

2.1 Supply voltage

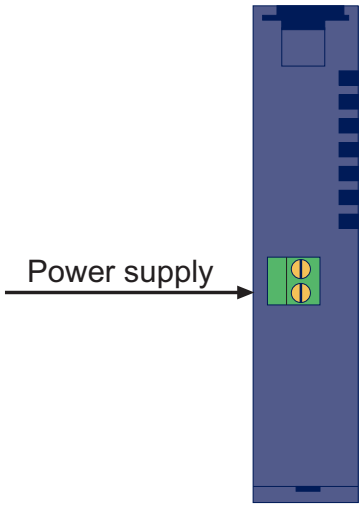
The following describes the two methods of providing power to the Trap-Receiver.

The types of voltage supply described here provide only power to the device. Wiring the in- and outputs requires an additional power supply.

If the device is powered using PoE, connecting or disconnecting an additional external power source while the device is running may result in the Trap-Receiver restarting.

2.1.1 External supply voltage

Connect a supply voltage of 18V...48V DC (+/-10%) or 18Veff...30Veff AC (+/-10%) to the terminal on the underneath of the device. You may use power supplies sold by W&T or any desired power supply which meets the technical requirements.



Underside of the device with terminal for the external power supply

The external supply voltage for the device is always required in networks not providing PoE, but may also be used in PoE environments.

When powering with DC voltage, correct polarity is not required.

It is also possible to power the device with 12V DC. There however you must take into account the very poor efficiency of the power supply and the associated elevated current draw.

2.1.2 Voltage supply using PoE

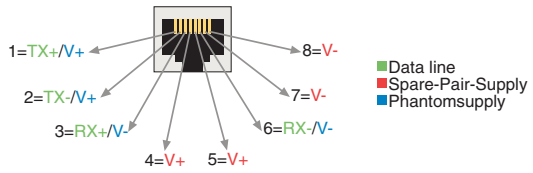
The Trap-Receiver is equipped for use in Power over Ethernet environments per IEEE802.3af. The voltage is then provided by the network infrastructure using the RJ45 terminal. The device supports both phantom feed using data pairs 1/2 and 3/6 or spare-pair power using the unused wire pairs 4/5 and 7/8.

To enable power management for the supplying components, the Trap-Receiver identifies itself as a Power Class 2 device with a power draw of 3.84W to 6.49W.

With an external power supply the Trap-Receiver can also be used in networks not providing PoE support.

2.2 Network connection

The Trap-Receiver provides an IEEE 802.3 compatible network connection on a shielded RJ45 connector. Pin assignments correspond to an MDI interface (see figure), so that connection to a hub or switch is made using a 1:1 wired and shielded patch cable.



Configuration of the RJ45 PoE network jack

The factory default setting for the Trap-Receiver on the network side is for Auto-Negotiation. Data transmission speed and duplex procedure are automatically negotiated with the connected switch/hub and set appropriately.

The network connection is galvanically isolated to 1kV with respect to the power supply as well as the digital IOs.

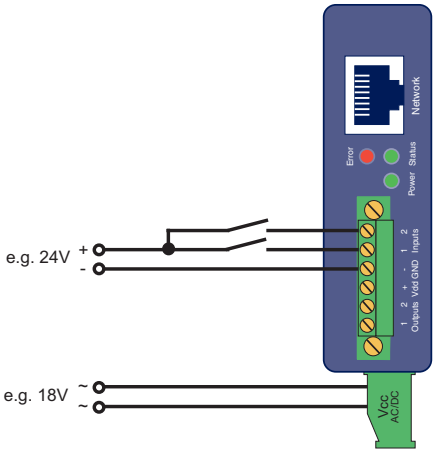
Thanks to the integrated Power over Ethernet technology, the device can be supplied with the necessary operating voltage through the network connection.

2.3 Wiring the inputs

The permitted input voltage range is +/-30V with respect to reference ground.

The switching threshold of the inputs is 8V +/-1V. Lower voltages are recognized as an OFF or 0 signal. Voltages higher than 8V are evaluated by the Trap-Receiver as an ON or 1 signal. Input voltages between 7V and 9V should be avoided, since their meaning may be ambiguous.

The following wiring example shows how two inputs are controlled. It is important that both signals have the same reference ground.



Controlling the two digital inputs

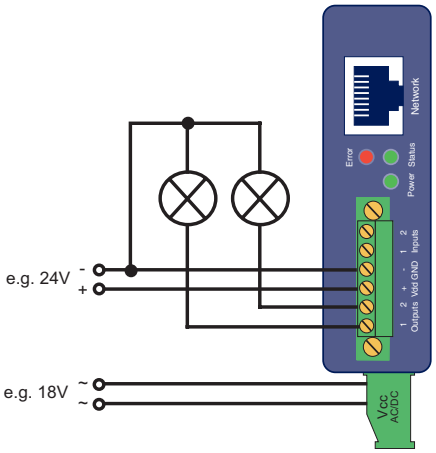
If you need to use the inputs for monitoring the states of potential-free contacts, the supply voltage for the unit can also be used as the signal voltage. In this case you need to operate the Trap-Receiver with a DC voltage of 12V-30V.

2.4 Wiring the outputs

The two Trap-Receiver outputs are current sourcing. The supply voltage for the outputs may be between 6V and 30V DC and is fed through the terminals Vdd and GND in the output terminal area. The maximum switching current per output is 500mA.

When the outputs are switched using an inductive load (e.g. a relay), a snubber diode should be used to protect them from damage.

The outputs also have thermal overload protection and are short-circuit protected.



Output wiring with separate power supply

When sizing the output supply voltage, the required current should be taken into account. If the device is powered by a 12V-30V external power supply whose capacity is also sufficient for supplying the consumers connected to the outputs, the output supply may likewise be connected to the device supply.

The range of the device supply voltage exceeds the range of the switchable output voltage. Use the device

supply for supplying the outputs as well, but use no more than 30V for powering the device.

In the configuration you can set up, to give the power supply of the Trap-Receiver directly to the terminals Vdd and GND. In this case an external supply for the IOs is not required. Powered internally, both outputs can drive 150mA as maximum.

2.5 Assigning the IP address using Wutility

Once the hardware has been powered as described above using either PoE or an external power supply, the IP address required for operating in a TCP/IP network needs to be assigned. The necessary values (IP address, net mask, etc.) can be obtained from your system administrator.

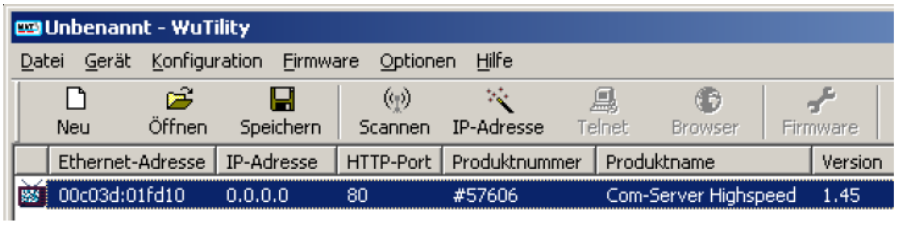
The assigned IP address must be unique within the network.

There are several ways to assign the IP address. To make the process as convenient as possible, we have developed the *WuTility* program, which you can download from our homepage *http://www.wut.de*. This procedure is described in the following. A summary of possible alternatives can be found in the Appendix to this manual.

Ensure that the PC you are assigning the IP address with is in the same subnet as the Trap-Receiver you are configuring. Both devices must be connected to the network.

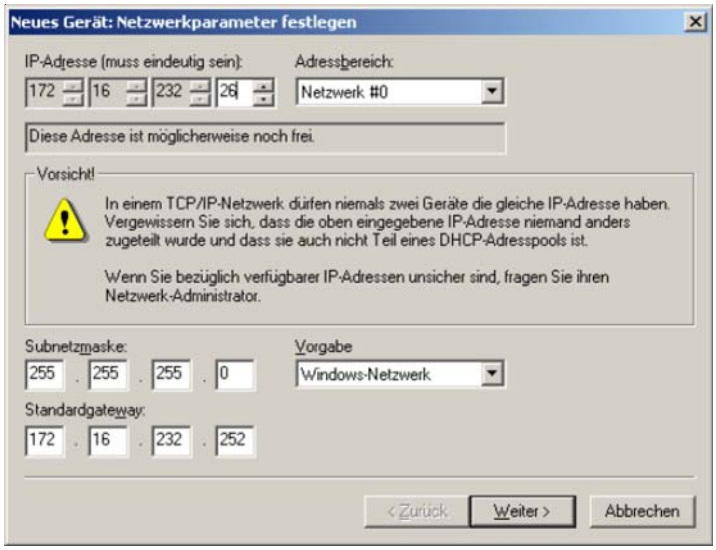
At startup the *WuTility* automatically searches the local network for connected W&T network devices and displays them in an inventory list. The scan procedure can be repeated as often as desired by clicking on the *Scan* button.

Now select the Trap-Receiver from the displayed list. If you have more than one unconfigured W&T network devices in your network, you can use the MAC address to create the relationship between list entry and terminal device:



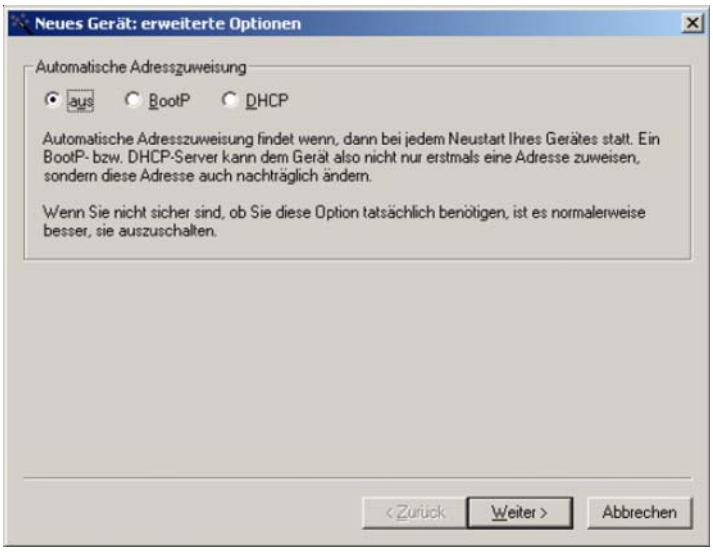
WuTility with found W&T network device

Use the button *IP address* to go to the configuration dialog box. There you enter the desired network parameters for the device. Confirm your entry by clicking on the *Next* button:



Configuration dialog box for network parameters

In the following window you can activate the BOOTP or DHCP client of the device for automatic IP address assigning:



Configuration dialog box for address assigning

By clicking on the *Next* button the Trap-Receiver is assigned the entered network parameters. All the columns of the inventory list in *WuTility* are filled with information. Clicking on the *Browser* button opens your standard browser and you can see the start page for the device.

2.6 Automatic IP address assignment

Many networks use either DHCP (Dynamic Host Configuration Protocol) or its predecessor BOOTP, described in the following section, for centralized and dynamic assignment of the network parameters. The factory default setting is for DHCP activated in your Trap-Receiver, so that all you need to do in network environments with dynamic IP address assignment is connect the device to the network. The following parameters can be assigned using DHCP:

- IP address
- Subnet mask
- Gateway
- DNS server
- Lease-Time

To prevent unintended address assignments or address changes, we recommending deactivating DHCP and BOOTP/RARP unless they are expressly used in the respective network environment. W&T network devices with incorrectly assigned IP addresses may be subsequently reconfigured using the WuTility.

2.6.1 Activating/deactivating assignment procedures

The factory default setting is for DHCP activated. The following options are available for deactivating, specifying a different assignment procedure or for reactivating at a later time:

- **WuTility:** In the inventory list select the desired Trap-Receiver and click on the *IP-Address* button. In the first dialog box you enter the network parameters you want to assign and confirm by clicking on *Next*. In the following dialog box activate the desired protocol for automatic IP address assigning or turn this option off there. Click on *Next* to apply the configured parameters to the device.
- **Web-Based Management:** Using Web-Based Management you can alternatingly activate the protocols or deactivate both of them. For detailed information please refer to the section *Assigning the basic network parameters*.

2.6.2 System name

In order to support any later automated updating of the DNS system by the DHCP server, the Trap-Receiver identifies itself within DHCP with its system name. The factory set name is *Trap-Receiver 2x2 Digital-* followed by the last three places in the Ethernet address. For example, the factory set system name of an Trap-Receiver having Ethernet address 00:c0:3d:01:02:03 is *Trap-Receiver 2x2 Digital-010203*. The system name of the device can be changed using Web-Based Management.

2.6.3 Lease-Time

The lease time determined and conveyed by the DHCP server specifies the time of validity of the assigned IP address. After half the lease time has expired the Trap-Receiver attempts to extend the validity or update the address. If this is not possible by the time the lease time expires, for example because the DHCP server is no longer accessible, the Trap-Receiver deletes

its IP address and starts a cyclical search for alternate DHCP servers in order to assign a new IP address.

If DHCP is activated, the remaining lease time together with the current IP address in the menu branch

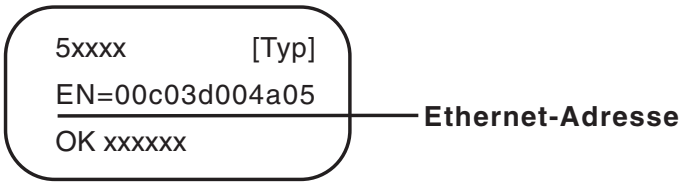
```
Home >> Doc >> Property
```

is displayed in seconds.

If after the assigned lease time has expired the DHCP server cannot be reached, the Trap-Receiver deletes its IP address. All existing TCP and UDP connections between the device and other network devices are interrupted by this action. To prevent situations of this type, we recommend configuring the lease time in the DHCP server for infinite if possible.

2.6.4 Reserved IP addresses

The Trap-Receiver provides services which other devices (clients) in the network can make use of as needed. To open a connection they of course need the current IP address of the Trap-Receiver, so that in these application cases it makes sense to reserve a particular IP address for the Trap-Receiver on the DHCP server. As a rule this is done by linking the IP address to the worldwide unique Ethernet address of the device which can be found on the housing sticker.



Ethernet address on sticker on the side of the housing

2.6.5 Dynamic IP addresses

Fully dynamic IP address assignment, whereby the Trap-Receiver receives a different IP address each time it restarts or after the lease time has expired, only makes sense in network environments having automatic cross-connection between the DHCP and DNS services. In other words: When assigning a new

IP address to the device, the DHCP server then automatically updates the DNS system as well. The new IP address is associated with the respective domain name. For detailed information concerning your network environment, refer to your system administrator when in doubt.

For time server queries, sending of e-mails or other client applications where the device actively searches for the connection to server services in the network, dynamic IP addresses can also be used.

2.7 Assigning the basic network parameters

Open the start page of the Trap-Receiver by entering the IP address in the address bar of your browser and use the link *Show menu* to show the configuration menu of the device. Alternately you can also open the address

```
http://<IP address of the Trap-Receiver>/index.htm
```

Here the configuration menu is already visible and does not have to be manually shown.

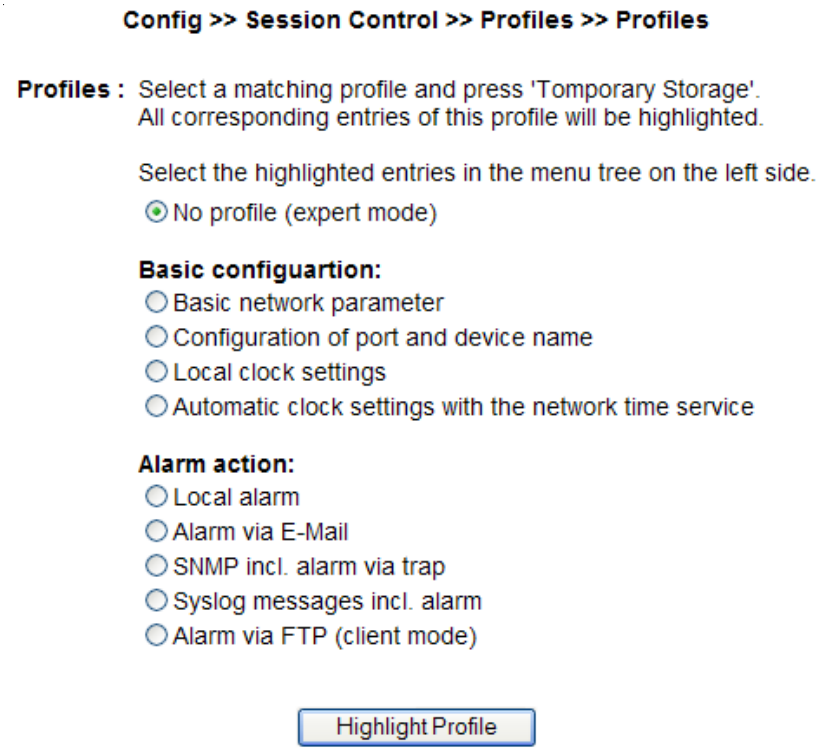
Select the menu item *Config/Login*.

You are now prompted to enter a password. By default no password is assigned, so that you can simply click on the *Login* button without entering a password. You are now logged in with administrator rights.

On the next page select the configuration path using the profiles.

Selection for profiles or Expert mode

Select the profile *Basic network parameter* and click on the *Highlight Profile* button.

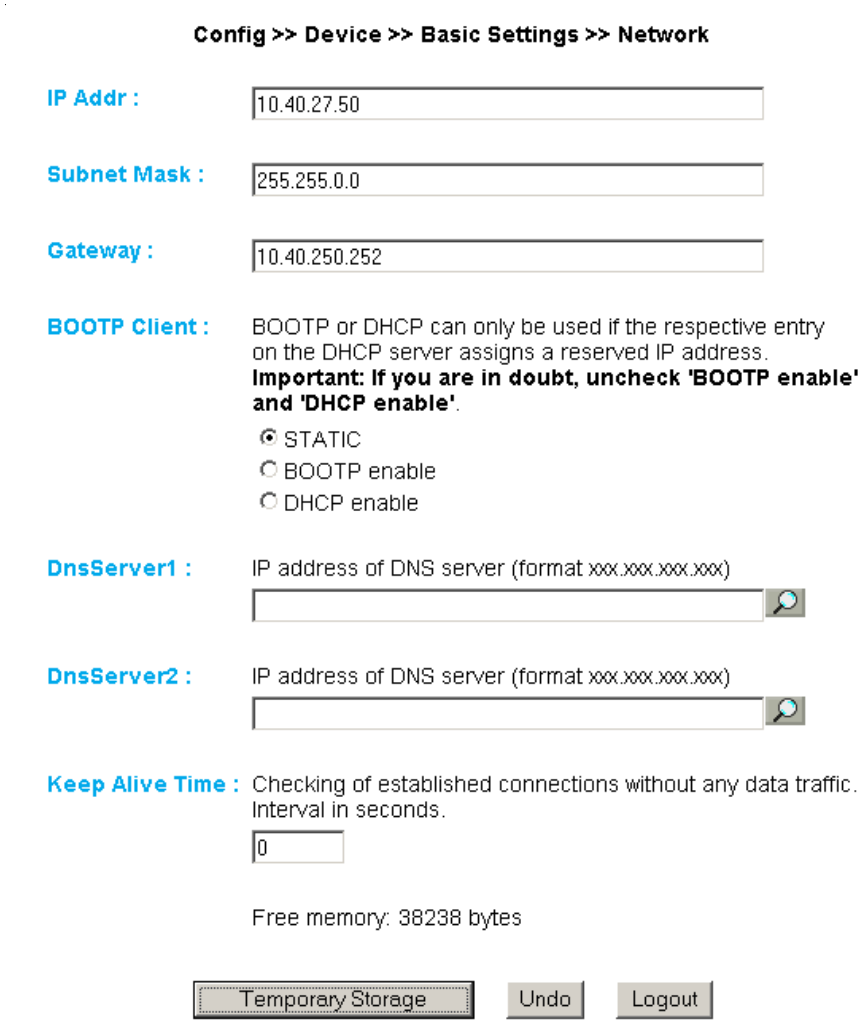


Profile selection

The device now shows the necessary menu items highlighted in blue which need to be edited for configuring the selected

profile. Save or cancel changes using the red highlighted menu items *Logout* and *Profiles*, or display a new profile for further configuring the Trap-Receiver.

First edit *Network* and then logout using *LogOut*. On the following page enter all the required network parameters and accept them by clicking on the *Save* button.

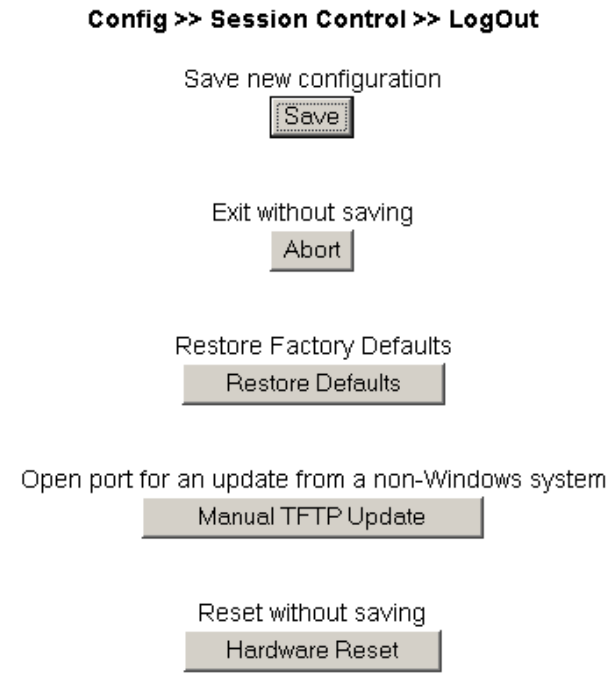


Network configuration

The *Logout* button ends the configuration procedure and saves the changes in the device.

Then clicking on the *Save* button saves your settings in the device and ends the configuration session. If network

parameters were changed during the session, the device automatically restarts itself to apply the changed values.



Logout options

The device is now ready to use in your network. Again use the profiles for additional configurations and continue through the configuration process.

3 Operation and Monitoring from the Browser

Once the Trap-Receiver has been configured with the required basic network parameters and connected to the network, you may further configure and operate/monitor the device from your browser.

3.1 Addresses

There are four pages which you can directly address from the browser. In the following the URLs are briefly explained and listed.

The homepage automatically refreshes to show the status of the configured alarms:

```
http://<IP address of the Trap-Receiver>/home.htm
```

The following link opens the homepage, as described above, along with the configuration menu:

```
http://<IP address of the Trap-Receiver>/index.htm
```

On the user-page the user-defined website is displayed:

```
http://<IP address of the Trap-Receiver>/user.htm
```

Diagnostics messages can be retrieved at the following address:

```
http://<IP address of the Trap-Receiver>/diag.htm
```

3.2 Homepage

The homepage, which can be opened using address

```
http://<IP address of the Trap-Receiver>/home.htm
```

- ...provides an overview of all received SNMP-Traps, Syslog-Messages and configured actions
- ...shows all user defined buttons and the state of the IOs

At the top left of the screen you will find links used to display the configuration and for navigating to the other main page. There you can also use control elements to log in.

The displayed information is refreshed once a second. This is done automatically without user intervention. The time of the last update is shown beside the heading *Ticker*. The time shown there is the system time of the Trap-Receiver. If the time is followed by an asterisk, the system clock of the device is synchronized with the time server set in the configuration.

Below the update time is a message box which summarizes all received SNMP-Traps and Syslog-Messages.

The main component of the homepage is the overview of the configured alarms, shown below the Ticker. The table provides the following information for each alarm:

- Symbolic name which can be assigned from the configuration menu.
- Information about the last event, concerning the alarm.

On this page are also overviews which display the user defined buttons and the IO-staes of the terminals.

3.3 User page

The user can upload an own HTML-page, which is then shown on the user-page. The uploaded file must start with:

```
<user.htm>
```

3.4 Hiding and showing the configuration menu

If the configuration menu is not visible, the page *home.htm* in the upper left corner provide the link *Show menu* for making the menu tree visible.

The link for hiding the configuration menu is then only visible beneath the menu tree if *home.htm* is shown in the right section of the browser. Otherwise a configuration page is displayed which provides information about a running configuration process. This requires access to the complete menu tree, which is why hiding the menu is not supported at this point.

3.5 Login and Logout

Depending on the login, the Trap-Receiver distinguishes between three different access levels:

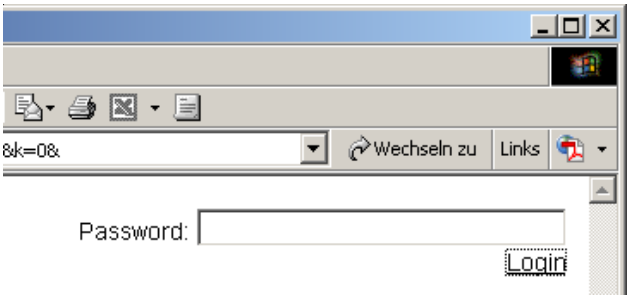
- *Default User*: Every user who accesses the device without a password has this status initially. The status of the Trap-Receiver can now be read out and displayed. Operating user defined buttons or changing the configuration is however not possible.
- *Administrator*: The administrator password provides full access to the device.
- *Operator*: Operator access rights are limited to the user defined buttons, changing the alarm outputs and changing the device time and language.

Regardless of the access level, each operator is able to read out accumulated errors from the diagnostics page and view device information under the *Doc* heading.

The more access rights a user has, the more complete the menu tree. Items not available based on the login are hidden.

A login can be done either using the dialog in the upper rightcorner on the *home.htm* page or using the sub-item

Config/Login from the menu tree. The dialog box on the homepage is then only visible if the menu tree is hidden.



Login dialog on the homepage

It makes no difference where login is done. But if the configuration of the device was changed, logout must be done from the „Logout“ page in the menu tree. If you log out from the homepage, the changes you made are lost.

A login with administrator rights can overwrite an already existing login. In this case the user is prompted during the login to accept the existing login.

Prompt on the homepage for accepting an existing login

A login is rejected if an incorrect password is entered or if you attempt to overwrite an existing login using insufficient access rights.

Message for rejected login on the homepage

The entered password is hashed, using the MD5-algorithm (derived from RSA Data Security, Inc. MD5 Message Digest Algorithm), and send secure.

4 Basic Settings

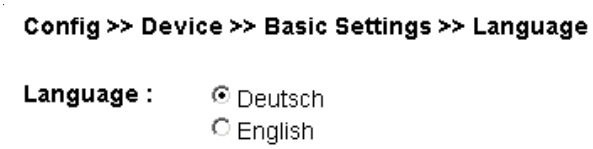
4.1 Language

You can use the configuration menu to specify the system language. This can be done either using the flag link below the configuration menu, or navigate to:

`Config >> Device >> Basic Settings >> Language`

Flag link below the configuration menu

On the opened page select the desired language and save you change by clicking on *Temporary Storage*.



Language selection

Changing the language requires operator or administrator rights.

4.2 Text

From the configuration menu open the page

`Config >> Device >> Text`

to edit the following texts:

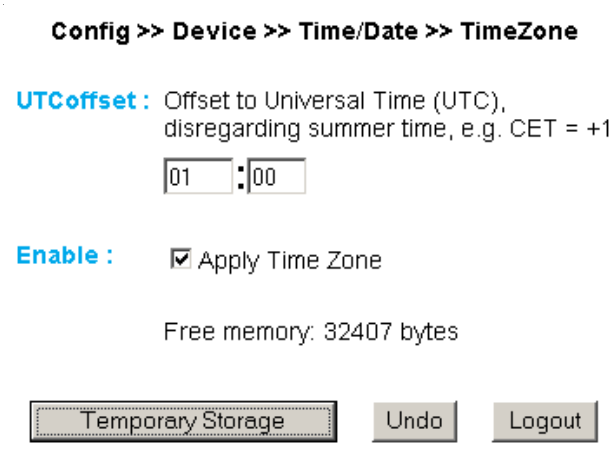
- Device Name: Name of the Trap-Receiver
- Device Text: More detailed description
- Location: Location where the Trap-Receiver is installed
- Contact: Contact address for service

Save your changes by clicking on the *Temporary Storage* button before you exit the page.

4.3 Time / Date

4.3.1 Timezone

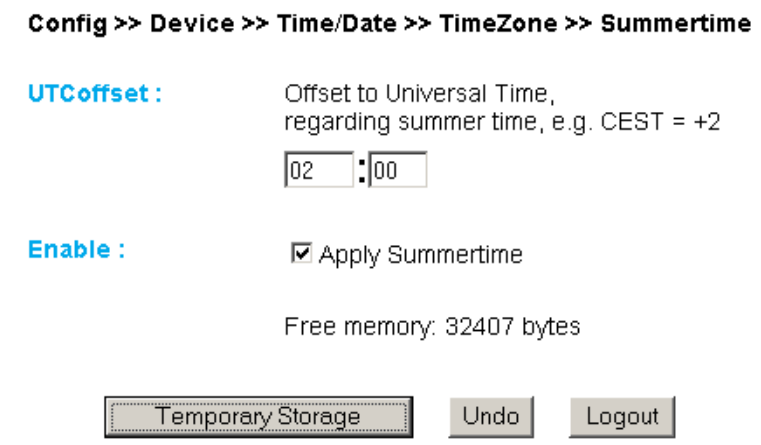
On this page you specify the time zone in which the device is located. The settings refer to UTC (Universal Time Coordinated). Apply the settings by clicking on *Save*.



Time zone configuration

4.3.2 Summertime

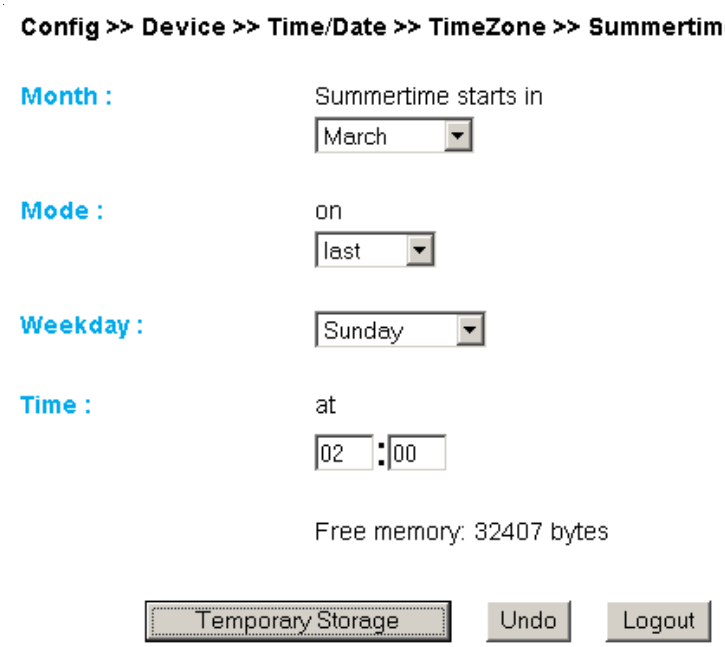
If you want your device to automatically adjust to daylight saving time, first enter the offset to UTC. The standard value (including for Germany) is two hours. Activate this function by checking the box *Apply Summertime* and save the settings.



Setting daylight saving time

On the *Start* and *Stop* pages you can modify the rule for when to begin and end daylight saving time.

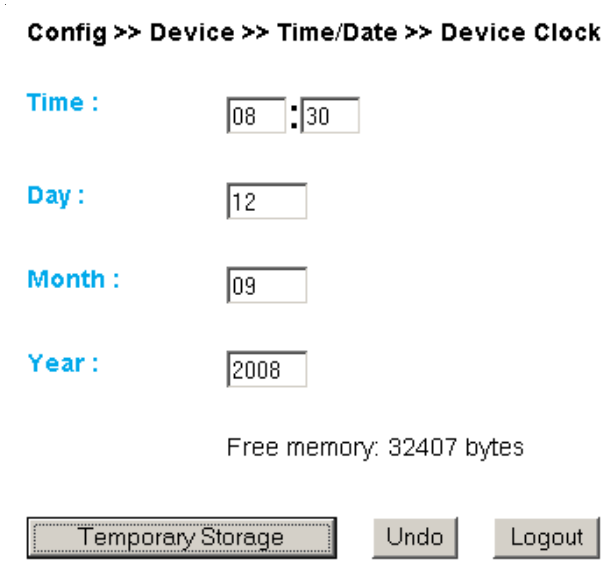
The factory default setting is for daylight saving time to begin on the last Sunday in March at 2:00 a.m. The end of daylight saving time is preset for the last Sunday in October at 3:00 a.m.



Rule for beginning daylight saving time

4.3.3 Device Clock

If you do not wish to use a time server, you can set the clock manually here. Then click on *Logout* and save your settings.



Manually setting the system clock

The clock is battery backed, so that the setting remains intact even after interrupting power to the device and you do not have to reset the time after the next restart.

4.3.4 Automatic time setting using a network service

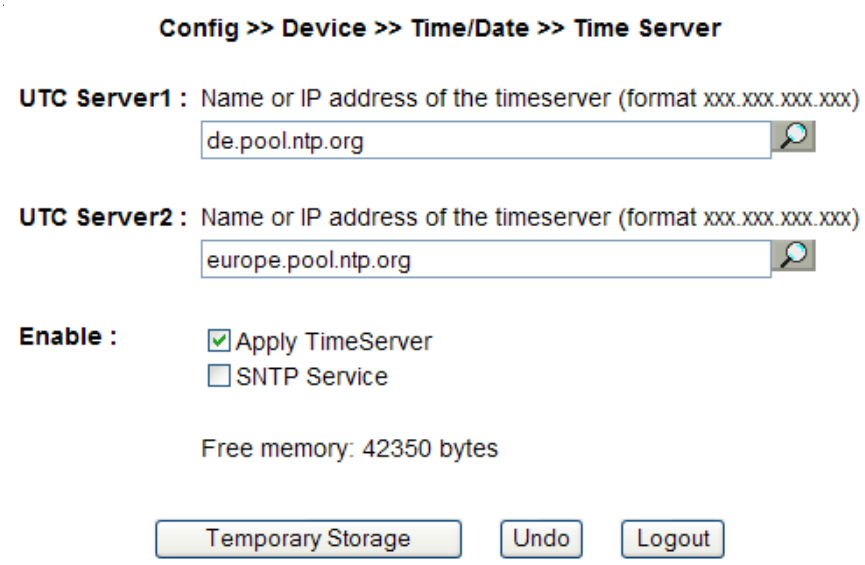
The configuration for the local time setting using a time server can also be made using a profile.

Just as for the local time setting, here also you must take into account and change as needed the configuration pages *Time-zone*, *Summertime*, *Start* and *Stop*.

In addition, you also configure for the actual time compensation via network service on the *Time Server* page.

Here you can store the addresses of two time servers, so that the time can be compensated even if one of the servers cannot be reached. Clicking on the magnifying glass symbol behind the addresses allows you to check the availability of the servers. You can also indicate the whole hour at which the compensation should be done daily.

Then activate the option *Apply Timeserver*.



Options for time servers

The preset addresses are only an example and do not necessarily have to be used.

If you enter a name as the time server address, be sure that you have first configured both a gateway and a DNS server. Otherwise the address cannot be resolved. .

Click on *Temporary Storage* to save your settings.

4.3.5 Activate SNTP time server

If the system time for the device is synchronized with a time server, the Trap-Receiver itself can assume the function of a time server.

SNTP (Simple Network Time Protocol) is supported here.

To start the time server service, activate the option *SNTP Service* on the configuration page

`Config >> Device >> Time/Date >> Time Server`

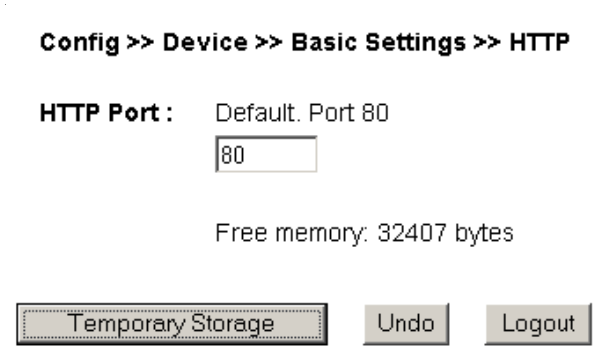
4.4 HTTP-Port

From the page

`Config >> Device >> Basic Settings >> HTTP`

you can specify the port through which the device is accessed. The default setting is the standard HTTP port 80. If you would like to use a different port, this may have to be explicitly indicated when opening the page, for example when opening the page *home.htm*:

`http://<IP address of the Trap-Receiver>/home.htm:<portnumber>`



Configuring the port number

5 Actions

For configuring actions there must be defined an inventory of Inputs or In-Events at first. These Inventory is then offered when setting up the actions. The behaviour of network-outputs (e.g. Mail, FTP) is defined beneath each action.

5.1 Configuring In-Events

The event list can hold a maximum of 1000 events. The trigger condition for an action can be the occurrence of an event in the network. Before the actions are configured in detail the network components to be monitored must be added to the list of the known network events. Association of the components with the individual actions is derived from this central list.

The SNMP-Traps and Syslog-Messages are managed on the page:

Config >> Device >> Prepare In-Events >> Listed Traps / Syslog

Here you will find functions for ...

- ...Inserting new events.
- ...Editing an existing entry.
- ...Deleting an individual entry.
- ...Deleting all entries.

5.1.1 Insert entry

Clicking on the *Insert* button takes you to the screen for adding new devices or events to the list.

The value *Item No.* determines the position of the device in the list. Use the *IP Addr.* Field to specify the IP address or host name of the network device you wish to monitor.

Any entries already stored in this position are moved back.

The Trap Receiver does not actively monitor the network components from which events are expected.

Be sure that the selected network components are properly connected and working. If necessary you may use the Trap-Receiver for determining whether a network device is ready yet.

Alias allows you to enter text which makes it easier to associate the abstract IP addresses or host names with the actual network components to be monitored.

Finish the procedure by clicking on the *Apply* button.

5.1.2 Edit entries

To edit an entry select it first using the pull-down box and click on the *Edit* button. This takes you to a screen for modifying the entry parameters. Finish the procedure by clicking on the *Apply* button.

5.1.3 Delete

Remove the entry selected from the pull-down box by clicking on the *Delete* button.

5.1.4 Delete events list

Clicking on the *Delete all* button removes all entries from the events list.

5.1.5 Automatic adding using the Heard List

Config >> Device >> Prepare In-Events >> Received Traps / Syslog

The device is always ready to receive SNMP traps and Syslog messages. The received traps are then entered in the Heard List.

Again selecting *Config >> Device >> Prepare In-Events >> Received Traps / Syslog* displays newly received network events. Prerequisite: Events which are already entered in the Events list no longer appear here.

It may be desired to display the arrival of network events. The *Live Update* button is provided for this purpose. Clicking on this button displays the last two arriving traps or messages in the Scan box.

The searched for events should appear during scanning. The progress of an ongoing scan is indicated during the procedure by a status bar. Click on *Cancel* to stop a scan.

Found SNMP-Traps and Syslog-Messages are listed in the Heard-List. Several entries can there be checked for transfering them to the Watchlist using the button *Transfer to NET event list*.

Delete All clears the Hears-List.

5.1.6 Timer

A total of 2 timers can be configured as desired.

For example select in the navigation tree:

```
Config >> Divice Prepare In-Events >> Timer >> Timer 1
```

Click on the *Enable* button to activate the timer.

For *Name* enter a name you would like to see displayed on the homepage in the browser.

In the *Timer 1* block you specify at what times the timer becomes active. The times are entered in so-called cron format. „*“ stands for „any“. If for example all the fields are filled with „*“, the timer would become active each minute.

5.1.7 Buttons for configuring the homepage

As an example the buttons 7 and 8 are preconfigured from the factory.

A total of 8 buttons can be configured as desired.

For example in the navigation tree select:

```
Config >> Divice Prepare In-Events >> Buttons >> Button 1
```

Check *Enable* if you want to activate the button.

For *Name* enter a name you would like to appear on the button on the homepage in the browser.

The description entered in the *Text* field can for example further describe the function or effect of clicking the button.

In the *Access Level* block you specify who is allowed to use the buttons and trigger the associated actions. Guest is active if there is no login. Operators and Administrators must log in with a password. Login without an assigned password always results in Administrator rights.

5.1.8 Port settings - Inputs

Individual basic settings can be made for each of the two inputs.

For example to change the settings for Input 0, go in the navigation tree to:

```
Config >> Divice Prepare In-Events >> Inputs >> Input 0
```

For *Name* enter a name for the input. This name is then displayed in the browser to represent Input 0.

The description entered in the *Text* field can serve for example to further describe the function or installation location of the sensor.

Filter is used to specify a minimum time for which a signal must be present in order to be detected. If a signal level is present for less than the time specified here, it is ignored. The

time is specified in 1/000 of a second. If no value is entered here, this function is disabled.

5.2 Configure Out- Events

`Config >> Device >> Prepare Outputs >> Output x`

For example, select the settings for Output 0.

Name: In this field you enter a name for the output. This name is then displayed in the browser for Output 0 and can for example further describe the function or installation location of the actuator.

Power: Here you set whether 24V is provided on Vdd.

Duration: In addition to the purely static switching of the outputs to ON or OFF, the Trap Receiver also allows you to output pulses. This means the output is switched and holds this state for a time which corresponds to the settable pulse length. Then it switches according to the pulse polarity. For *Duration* enter the desired pulse length in thousandths of a second. A value of 1000 then corresponds to a 1 second long pulse.

Pulse polarity: The turn-on and quiescent state of the output is factory set to OFF (0V). You can also configure so that the output is ON (Vdd, on) when the device is powered up. At the same time this configures the output to turn off or on after the pulse ends. You can also switch the output manually in the direction of pulse polarity and thereby shorten the pulse.

5.3 Configure Actions

There can be up to 12 actions be configured in the Trap-Receiver. An action is released when an In-Event occured (SNMP-Trap or Syslog-Message is received, a button is hit, a timer releases, an input is triggered). A released action fires an Out-Event (e.g. sending a mail or a TCP-Message or switches an output).

Go to:

```
Config >> Device >> Actions >> Action X
```

for configuring the actions.

In the *Action Name* field enter a name for the action. This name is displayed on all control and operating pages.

The check box *Action Enable* must be activated for the action to be triggered when the trigger condition is met. To deactivate the action, simply deactivate the check box again. It is then not necessary to clear the settings.

Check all options beneath In-Events, which should be observed by the action. The action will be fired at occuring of one of the checked events.

Time Window allows to define a start and stop-date. In-Events, which trigger outside this window, doesn't fire the action. The start and stop-date has to be entered in CRON-syntax.

Out-Events define, which messaging method should be used when the action fires:

- Mail (SMTP)
- SNMP
- Syslog
- UDP Peer
- TCP Client
- FTP Client

Define here also to which state the outputs should be set, when the action fires.

5.4 Formulating message texts

For the messaging types reporting over the network, there can be formulated what is sent.

The various messages are configured on the sub-pages of the individual actions, for example:

```
Config >> Device >> Actions >> Action 1 >> Mail
```

Enter the address to which the mail should be sent ind *E-Mail-Addr.*

In the fields *Subject* and *Action Text* you enter the subject and the message text which you want send.

In order to fill the message texts dynamically with current information for the device, the tags listed in the following tagble are provided. When they are inserted into the message text, these placeholders are replaced by the actual current system value when the message is sent.

```
Time:              <t>
Signle Input:      <i0> .. <i1>
Single Output:     <o0> .. <o1>
All Inputs (Hex):  <i>
All Outputs (Hex): <o>
```

5.5 Alarming per E-Mail

Open the profile *Alarm via E-Mail*.

Configure the condition for the desired action using the steps explained in the section *Configure Actions*.

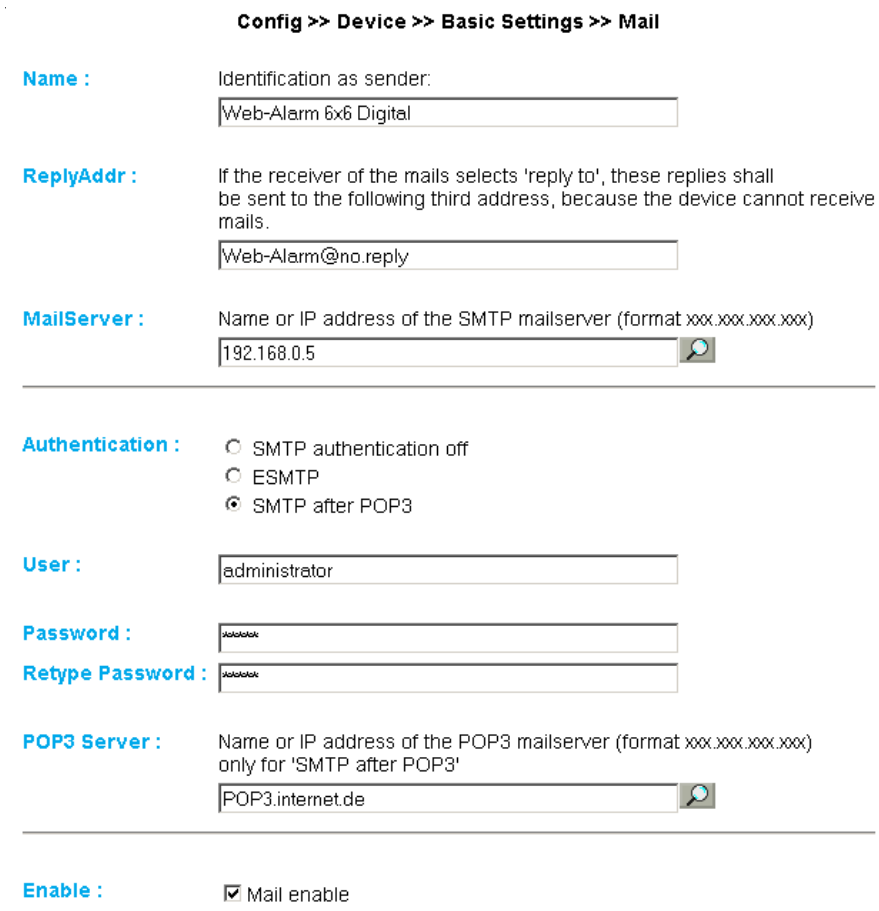
5.5.1 General settings

Go to the page:

```
Config >> Device >> Basic Settings >> Mail
```

to configure the basic settings for sending e-mails as explained below.

The e-mail function allows an mail to be sent to one or more e-mail recipients.



E-mail configuration

Here you set the following parameters:

In the *Name* field enter the name you want to appear as the e-mail sender.

ReplyAddr represents the address the device uses to identify itself.

In the next step (*MailServer*) set the IP address of your mail server or its host name (for configured DNS servers only) you want the device to use. If the e-mail port is not the standard port 25, you can append the port to the addressusing a colon:

`mail.provider.de:<Port>`

If authentication is required for the mail server, select the corresponding procedure for identifying the user:

- SMTP authentication off: No authentication
- ESMTP: A user name and password are required for logging in to the mail server.
- SMTP after POP3: For an SMTP server it is necessary first to access using POP3 so that the user can be identified. For this setting you also specify an associated POP3 server.

Then activate the mail function by checking *Mail enable*.

Apply the changes by clicking on *Temporary Storage*.

5.5.2 Mail parameters and texts

Finally you need to define the messages and the specific mail parameters. To do this open the page

```
Config >> Device >> Actions >> Action X >> Mail
```

In the field *E-Mail-Addr* enter the address of the recipient. If you are sending the e-mail to multiple recipients, separate the addresses from each other with a semicolon.

Finally, configure the required message text as described in the section *Formulating message texts* and apply the changes by clicking on *Save*.

5.6 Alarming per SNMP-Trap

Open the profile *SNMP incl.alarm via trap*.

Configure the condition for the desired action using the steps explained in the section *Configure Actions*.

5.6.1 General settings

Open the page

```
Config >> Device >> Basic Settings >> SNMP
```

Activate the check box *SNMP enable*. This starts the SNMP function in the device which processes sending of messages per SNMP.

Apply the changes by clicking on *Temporary Storage*.

5.6.2 SNMP parameters and texts

Finally you need to define the message and the specific SNMP parameters. To do this open the page

```
Config >> Device >> Actions >> Action X >> SNMP
```

In the *Manager IP* field enter the IP address of the SNMP manager you want to receive the message and display or evaluate it.

Finally, configure the required message text as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

5.7 Alarming per UDP client

Go to page

```
Config >> Device >> Basic Settings >> UDP
```

and select the option *UDP enable* and click on *Save* to apply the change

Configure the condition for the desired action as described in the section *Configuring Actions*.

Go to page

```
Config >> Device >> Actions >> Action X >> UDP
```

and in the field *IP Addr* enter the IP address of the UDP server. For *Port* specify the destination port.

Finally, configure the require message text as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

5.8 Alarming per TCP client

Configure the condition for the desired action as described in the section *Configuring alarms*.

Go to page

```
Config >> Device >> Actions >> Action X >> TCP
```

and in the field *IP Addr* enter the IP address of the TCP server. For *Port* specify the destination port.

Finally, configure the required message text as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

5.9 Alarming per Syslog

Open the profile *Syslog messages incl. alarm*.

Configure the condition for the desired action as described in the section *Configuring Actions*

5.9.1 General settings

On the configuration page

```
Config >> Device >> Basic Settings >> Syslog
```

activate the option *System Messages enable*.

This option enables the syslog function in the Trap-Receiver and thereby allows sending of messages using the syslog protocol.

Apply the changes by clicking on *Save*.

5.9.2 Syslog parameters and texts

Go to page

```
Config >> Device >> Actions >> Action X >> Syslog
```

In the *IP Addr* field enter the IP address of the recipient. Under Port use the port number that will be used to handle communication.

Finally, configure the require message texts as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

5.10 Alarming per FTP

Send the messages per FTP and write them directly to an FTP server.

Open the profile *Alarming via FTP (client mode)*.

Configure the condition for the desired action as described in the section *Configuring Actions*.

5.10.1 General settings

On the page

```
Config >> Device >> Basic Settings >> FTP
```

specify the basic parameters for message sending per FTP.

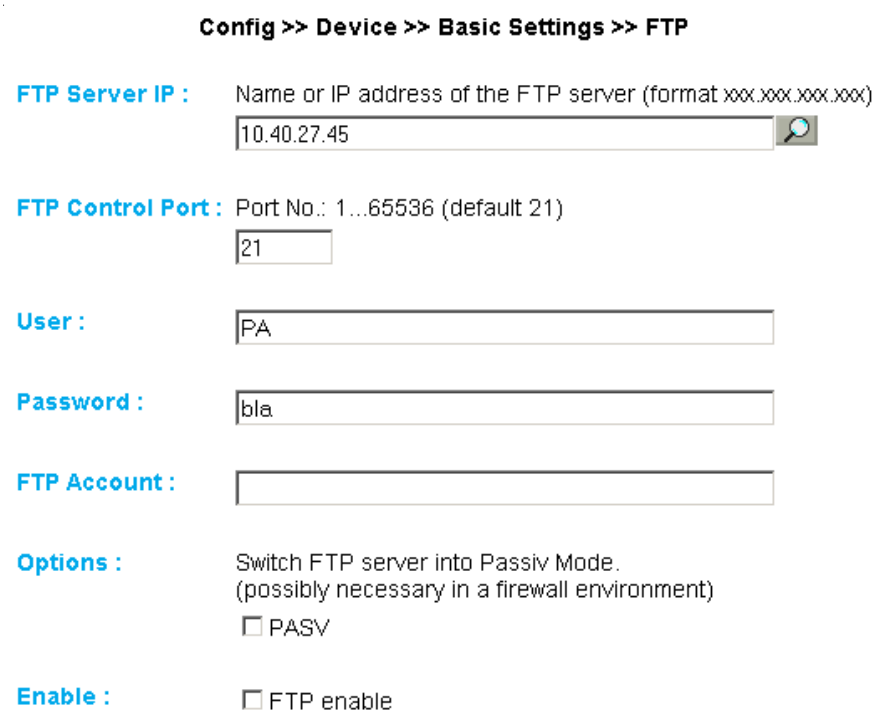
For *FTP Server IP* enter the IP address or host name (only for configured DNS servers) of your FTP server you want to receive the data.

In the *FTP Control Port* field specify the port you want to use for the connection. The standard port for FTP access is 21. This port is already preset and should work on most systems on the first try. If you need to use a different port, please consult with your system administrator.

For User and Password enter the access data required for the FTP access.

Some FTP servers require a special account entry for the login. If this is true of your server, enter the account name using *FTP Account*.

If the check box *PASV* under *Options* is activated, the server is instructed to run in passive mode. This means that the data connection is opened by the Trap-Receiver. If this option is deactivated, the FTP server opens the data connection. If the server is protected with a firewall, you should activate the PASV option, since otherwise connection attempts could be blocked.



FTP basic configuration

Finally, activate the FTP function of the device using the check box *FTP Enable* and apply the changes by clicking on *Save*.

5.10.2 FTP parameters and texts

Go to page

`Config >> Device >> Actions >> Action X >> FTP`

and enter the specific FTP parameters.

For *FTP Local Data Port* specify the local data port of the IP-Watcher. Valid values are between one and 65536. Entering *Auto* causes the device to select the port dynamically.

Under File Name enter the file path for the file you want the device to access. The file name can use the same tags as in the FTP alarm text.

You can use the options STORE and APPEND to select whether the sent data are written to a new file or appended to an existing file. If the file does not yet exist, it is created in both cases.

FTP options „STORE“ and „APPEND“

Finally, configure the required message text as described in the section *Formulating message texts*. If you want a line feed, insert a CRLF by pressing the Enter key at the end of the line. Apply the changes by clicking on *Save*.

6 Appendix

6.1 LEDs

In the following the meaning and function of the LEDs on the front panel of the Trap-Receiver is explained

6.1.1 Power-LED

Indicates presence of supply voltage. If the LED is not on, please check for correct wiring of the power supply.

6.1.2 Status-LED

Flashes whenever there is network activity with the Trap-Receiver. Periodic flashing indicates that the port has a connection to another station.

6.1.3 Error-LED

The Error-LED uses various flashing codes to indicate error states on the device or network port.

1x flashing: Check network connection. The Trap-Receiver is not receiving a link pulse from a hub or switch. Check the cable or the hub/switch port.

2x or 3x flashing: Perform a device reset by momentarily interrupting power to the unit. If this does not clear the error, restore the device to its factory defaults. Since this resets all network settings, you should write them down first.

If the Power, Status and Error LEDs are all on at the same time, the self-test performed after each start and reset of the device could not be correctly finished. The reason for this may be an incomplete firmware update. The Trap-Receiver is no longer operable in this state. Please return the unit through your dealer to W&T for inspection

6.2 Factory defaults

Some situations require that the Trap-Receiver be restored to its factory default settings. There are two ways to do this:

- Using Web-Based Management
- Using the Reset jumpers

Restoring the factory default settings returns the unit to its state as shipped from the factory. First write down all the settings so that you can later restore the configuration as needed.

6.2.1 Web-Based Management

To restore the factory default settings using Web-Based Management, log in to the configurationpages and navigate to

```
Config >> Session Control >> LogOut
```

On the page shown in the main window you can click on the *Restore Defaults* button to return the unit to its original settings.

6.2.2 Reset jumpers

If you are unable to restore the factory default settings using the Web interface, you can load the factory settings by jumpering the Rest jumper contacts.

For this you must open the device by pulling out the circuit boards together with the front panel.

Always disconnect the device from power first before opening it. Otherwise the IP-Watcher could be damaged.

You will see one open jumper contacts on the upper board. Close this contact.

Apply power to the Trap-Receiver for approx. 15s. The device is now reset to its factory defaults. The LEDs on the front panel will flicker irregularly during this procedure.

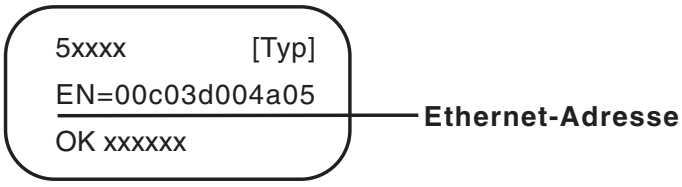
Once the factory default settings have been restored, disconnect the unit from power, remove the jumper and close up the unit. Now proceed to startup.

6.3 Alternative IP address assignment

The following describes methods for assigning an IP address to the unit instead of using the *WuTility* program.

6.3.1 ARP command

Required is a PC which is located in the same network segment as the Trap-Receiver and on which TCP/IP is installed. Read the MAC address of the Trap-Receiver on the device (e.g. EN=00C03D004a05).



Ethernet address on the sticker located on the side of the unit

Under Windows you now ping another network device and then insert a static entry into the computer‘s ARP table using the command line described below:

```
arp -s <IP address> <MAC address>
```

e.g. under Windows:

```
arp -s 172.0.0.10 00-C0-3D-00-12-FF
```

e.g. under SCO UNIX:

```
arp -s 172.0.0.10 00:C0:3D:00:12:FF
```

Now ping the device, here

```
ping 172.0.0.10
```

The IP address is now stored in non-volatile memory.

This method can only be used if no IP address has yet been assigned to the Trap-Receiver, i.e. the entry is 0.0.0.0. To change an already existing IP address, you must open the configuration menu from the browser or select the serial path.

6.3.2 RARP server (UNIX only)

Working with an RARP server enabled under UNIX is basded on entries in the configuration files */etc/ethers* and */etc/hosts*. First expand */etc/ethers* by one line with the assignment of the Ethernet address of the Trap-Receiver to the desired IP address. In */etc/hosts* the link with an alias is then determined. After you have connected the device in the network segment of the RARP server, you can use the network to assign the desired IP address to the device.

Your Trap-Receiver has for example the MAC address *EN=00C03D0012FF* (sticker on the device) and shoudl get IP address *172.0.0.10* and alias *WT_1*.

Entry in the file */etc/hosts*: 172.0.0.10 WT_1

Entry in the file */etc/ethers*: 00:C0:3D:00:12:FF WT_1

If the RARP daemon is not yet active, you must start it now using the command *rarpd -a*.

6.4 Firmware update

The operating software of the Trap-Receiver is being continually improved. The following section describes how to perform a firmware upgrade

6.4.1 Current firmware

The most current firmware including the available update tools and a revision list is published on our Web site at *http://www.WuT.de*.

Before downloading, please write down the 5-digit model number found on the Trap-Receiver. From our Web site you can get to the product overview sorted by article numbers, through which you can get directly to the data sheet for the device. Here you follow the link to the current version of the firmware.

6.4.2 Firmware update over the network

Required is a PC running Windows 9x/NT/2000/XP/Vista with a network connection and activated TCP/IP stack. For the update process you need two files, which as already mentioned are available for downloading from our homepage:

- The executable update tool for sending the firmware to the Trap-Receiver
- The file with the new firmware to be sent to the Trap-Receiver

No special preparation of the Trap-Receiver is necessary for the update.

The *WuTility* tool used for the update detects all the W&T devices located in your network and is for the most part self-explanatory. If you do have questions or anything is unclear, please use the associated documentation or the online help.

Never intentionally interrupt the update process by disconnecting the power supply. The Trap-Receiver will be rendered non-functional after an incomplete update.

Never mix files having different version numbers in the name. This will result in non-functionality of the device.

The Trap-Receiver automatically detects when transmission of the operating software is complete and then carries out a reset.

6.5 Up- and download

Under the heading Up/Dolwnload, which can also be reached from the configuration menu, you can up- and download the device configuration:

```
Config >> Up/Download >> Download
```

and

```
Config >> Up/Download >> Upload
```

When downloading the device configuration, which is stored in XML format, you can download the Trap-Receiver's settings and make any necessary changes. The changed settings can then be loaded back into the device using the Upload function.

For the XML upload you create or change a text file with the corresponding parameters and then load them into the device. The configuration of the Trap-Receiver must begin with the expression

```
<io-Digital2x2TR2.1>
```

and end with the expression

```
</io-Digital2x2TR2.1>
```

The syntax for configuring per XML is as follows:

```
<Option>
    <Parameter1>value</Parameter1>
    <Parameter2>value</Parameter2>
</Option>
```

The individual options and parameters correspond to the configuration items in the menu tree.

Note, especially for mass updates and configurations, that the IP address stored in the XML file is always the programmed in the device. This must first be modified.

In addition, the SNMP MIB you need for incorporating the device into SNMP management systems can be downloaded. Depending on the system language selected, load the German or English version.