Manual
IP-Watcher 2x2 Digital PoE

Typ	IP-Watcher 2x2 Digital PoE
Modell	#57655
Release	EN 3.19 08/2010 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!

W&T

Contents

W&T

1. Introduction

The IP Watcher from W&T uses cyclical polling to monitor network components. If a device no longer responds, this status can be reported by triggering local or remote alarms. Local alarms indicate non-response by switching a connected consumer on one of the two digital outputs. A remote alarm is set for example by email, FTP, SNMP or Syslog over a TCP/IP network.

An individual acknowledgement can be configured for all alarms. This is done either by wiring one of the digital inputs on the device (hardware acknowledgement) and/or sending an acknowledgement command via TCP/IP from the controller side to the IP Watcher (software acknowledgement). An acknowledgement ensures proper detection and handling of an alarm situation by an operator.

An integrated Web server provides configuration pages for setting the device parameters. Browser-based software is used to operate and monitor the alarms, and can also be loaded from the Web server of the IP Watcher into any browser. This software is self-refreshing and indicates the status of the activated alarms while offering the possibility of acknowledging pending alarms.

Power can be supplied either via Power over Ethernet through the network or from an external power supply.

The properties of the IP Watcher make it ideal for stand-alone monitoring tasks. Switching an output when there is an alarm can generate a local response, for example turning on a rotating flashing beacon. An alarm sent over a network quickly reaches even distant personal and prompts them to act. Network alarming allows the use of an existing network infrastructure and thereby makes it possible to send messages individually and without additional cabling. Thanks to the built-in, browser-based software, operation and monitoring are possible not only in the Intranet, but also worldwide over the Internet.

2. Startup

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

2.1 Supply voltage

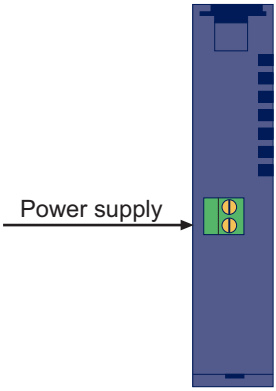
The following describes the two methods of providing power to the IP-Watcher.

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 IP-Watcher 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

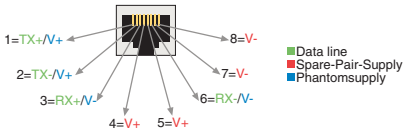
The IP-Watcher is equipped for use in Power over Ethernet environments per IEEE802.3af. The voltage is then provided by the network infrastructure using the RJ45 terminal. The device supports both phantom feed using data pairs 1/2 and 3/6 or spare-pair power using the unused wire pairs 4/5 and 7/8.

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

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

2.2 Network connection

The IP-Watcher 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 IP-Watcher 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.

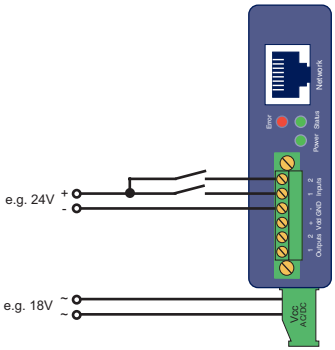
Thanks to the integrated Power over Ethernet technology, the device can be supplied with the necessary operating voltage through the network connection.

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 IP-Watcher 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

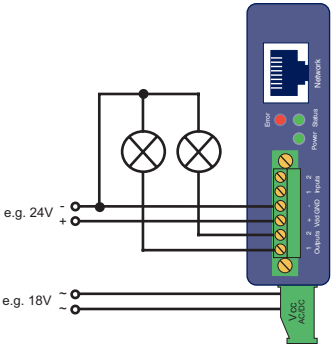
If you need to use the inputs for monitoring the states of potential-free contacts, the supply voltage for the unit can also be used as the signal voltage. In this case you need to operate the IP-Watcher with a DC voltage of 12V-30V.

2.4 Wiring the outputs

The two IP-Watcher 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 IP-Watcher 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.

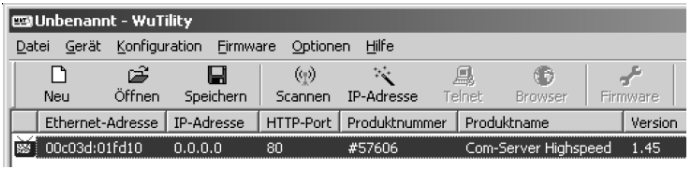
The assigned IP address must be unique within the network.

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 IP-Watcher you are configuring. Both devices must be connected to the network.

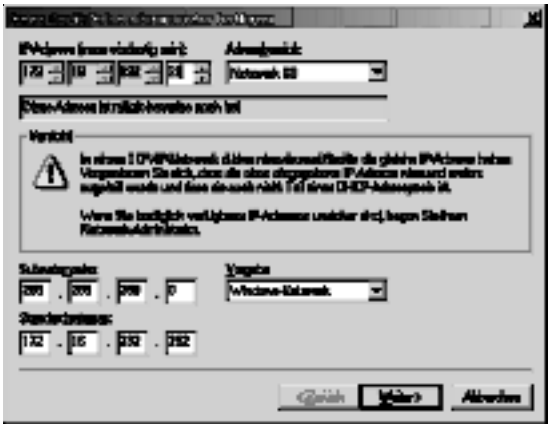
At startup the *WuTility* automatically searches the local network for connected W&T network devices and displays them in an inventory list. The scan procedure can be repeated as often as desired by clicking on the *Scan* button.

Now select the IP-Watcher 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:



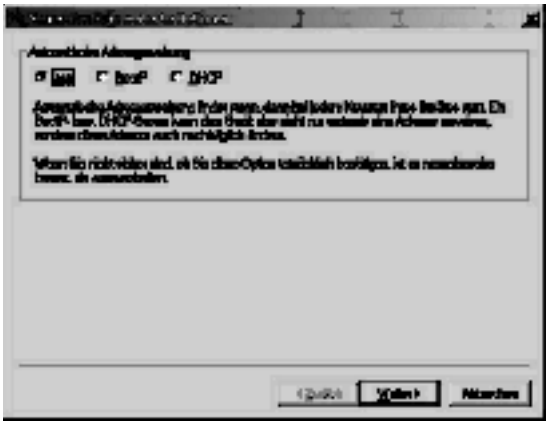
WuTility with found W&T network device

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 IP-Watcher 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 IP-Watcher, 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 IP-Watcher 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 IP-Watcher identifies itself within DHCP with its system name. The factory set name is *IP-Watcher 2x2 Digital-* followed by the last three places in the Ethernet address. For example, the factory set system name of an IP-Watcher having Ethernet address 00:c0:3d:01:02:03 is *IP-Watcher 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 IP-Watcher 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 IP-Watcher 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

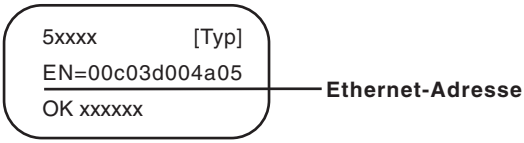
`Home >> Doc >> Property`

is displayed in seconds.

If after the assigned lease time has expired the DHCP server cannot be reached, the IP-Watcher 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 IP-Watcher 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 IP-Watcher, so that in these application cases it makes sense to reserve a particular IP address for the IP-Watcher 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 IP-Watcher 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 Language selection

The first time one of the controller pages(*home.htm*, *user.htm*) is opened by the device's own Web server, you are prompted to select the device language.

In the address bar of your browser enter the IP address of the device or the IP address followed by the name of one of the controller pages and send the query. On the loaded page select the desired system language and confirm you selection by clicking the *OK* button. This completes this configuration step, and you are taken to the start page of the device.

Language selection at initial startup

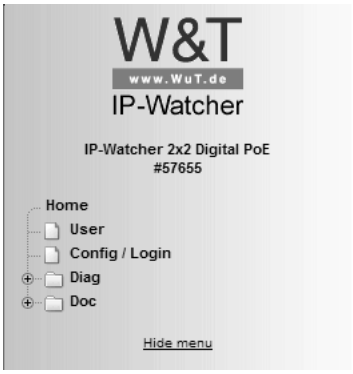
2.8 Assigning the basic network parameters

Open the start page of the IP-Watcher 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 IP-Watcher>/index.htm
```

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

Select the menu item *Config/Login*.



Configuration menu in the base state

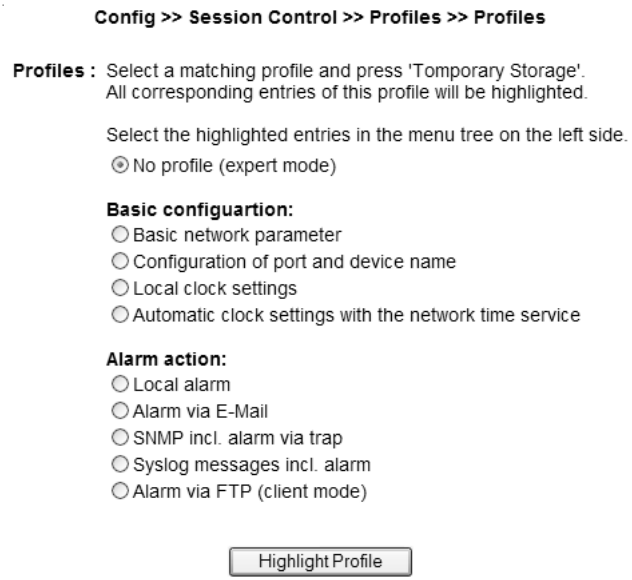
You are now prompted to enter a password. By default no password is assigned, so that you can simply click on the *Login* button without entering a password. You are now logged in with administrator rights.

Login dialog

On the next page select the configuration path using the profiles

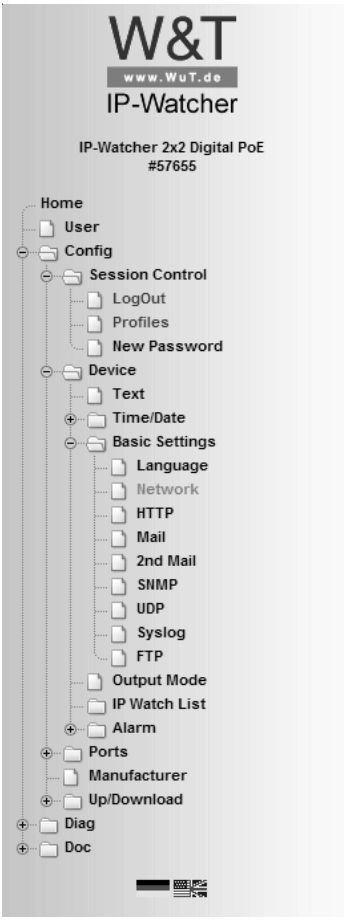
Selection for profiles or Expert mode

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



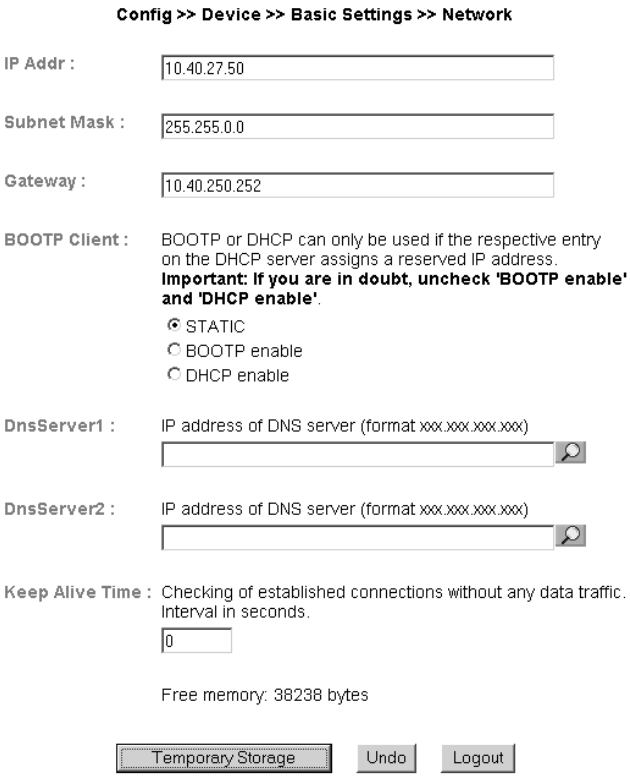
Profile selection

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 IP-Watcher.



Configuration menu with activated profile assistance

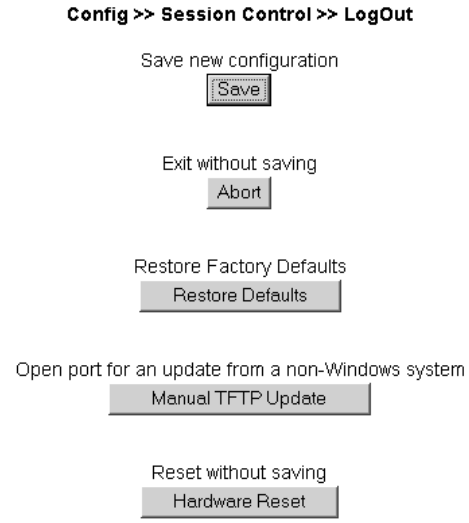
First edit *Network* and then logout using *LogOut*. On the following page enter all the required network parameters and accept them by clicking on the *Save* button.



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 IP-Watcher 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 and makes it possible for the logged in user to confirm alarms using software acknowledgement:

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

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

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

The user page displays - also automatically refreshed - the status of the IOs and all alarms:

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

Diagnostics messages can be retrieved at the following address:

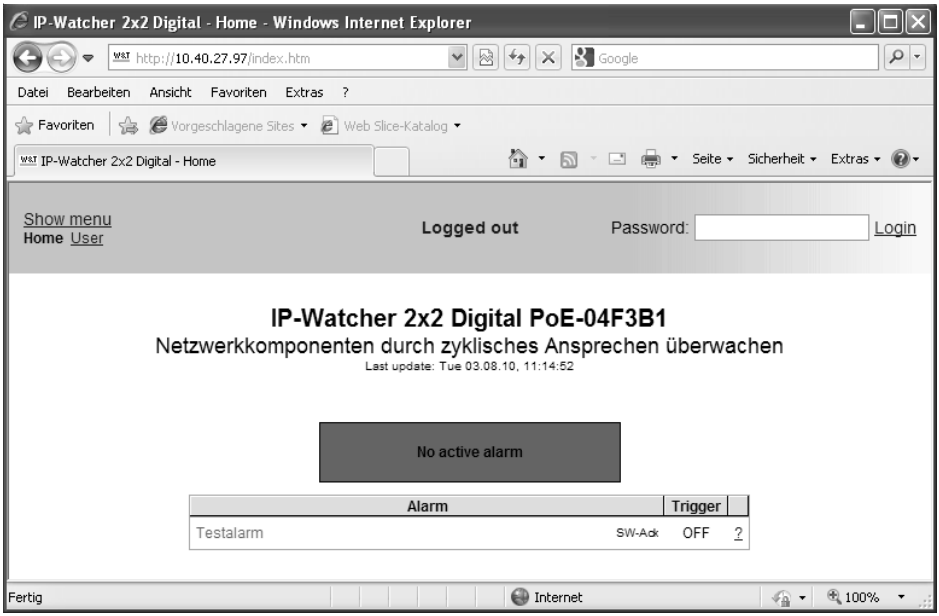
```
http://<IP address of the IP-Watcher>/diag.htm
```

3.2 Homepage

The homepage, which can be opened using address

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

- ...provides an overview of the status of all configured alarms.
- ...allows pending alarms to be reset using software acknowledgement.



Homepage with one configured alarm

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.

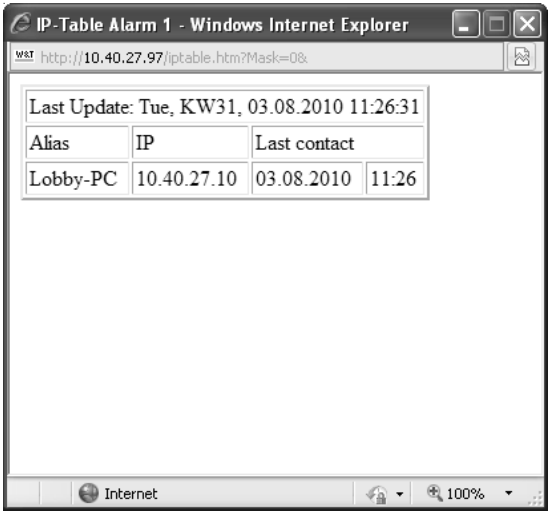
The displayed information is refreshed once a second. This is done automatically without user intervention. The time of the last update is shown beneath the headers. The time shown there is the system time of the IP-Watcher. If the time is followed by an asterisk, the system clock of the device is synchronized with the time server set in the configuration.

Below the update time is a message box which summarizes the status of all the activated alarms. If no alarm has been tripped, the box is highlighted in green and the message *No active*

alarm is displayed. If one or more alarms are active, the background color changes to red and the number of active alarms is shown. If one or more alarms were triggered manually from the test page in the configuration menu for test purposes, this information is also indicated. The message box is used for getting a quick overview of the overall status. The color background is intended to facilitate a quick assessment of the situation.

The main component of the homepage is the overview of the activated alarms. The table provides the following information for each alarm.

- Symbolic name which can be assigned from the configuration menu.
- Information as to whether the artificial trigger has been set from the test page (red flashing)
- Acknowledgement options (software or hardware Ack)
- Status of the trigger condition
- In logged-in state and if software acknowledgement has been configured, a button for alarm acknowledgement
- A question mark linking to more details about the alarm.



Further information about a triggered alarm

When no one is logged in, the page is used only for monitoring purposes. No access to the acknowledgement buttons is provided. Logging in with operator or administrator rights enables these functions.

After successful login the user interface changes as follows:

- If alarms are activated with software acknowledgement, the buttons are displayed and can be used to confirm alarms. These appear then in the line of the affected alarm.
- The control elements for the login procedure on the upper edge of the screen are replaced by a link for logging out.

The symbolic name of the alarms is shown corresponding to the current alarm status. If the alarm was triggered, the name is shown in bold red type; in the rest state it is green and in a normal font.

If an alarm is present which can be acknowledged in software, this can be accomplished using the corresponding acknowledgement button.

If an alarm is acknowledged, it releases immediately, even if the trigger, the trigger condition, still remains.

3.3 User page

The user page provides an overview of the state of the

- Inputs
- Outputs
- Activated alarms

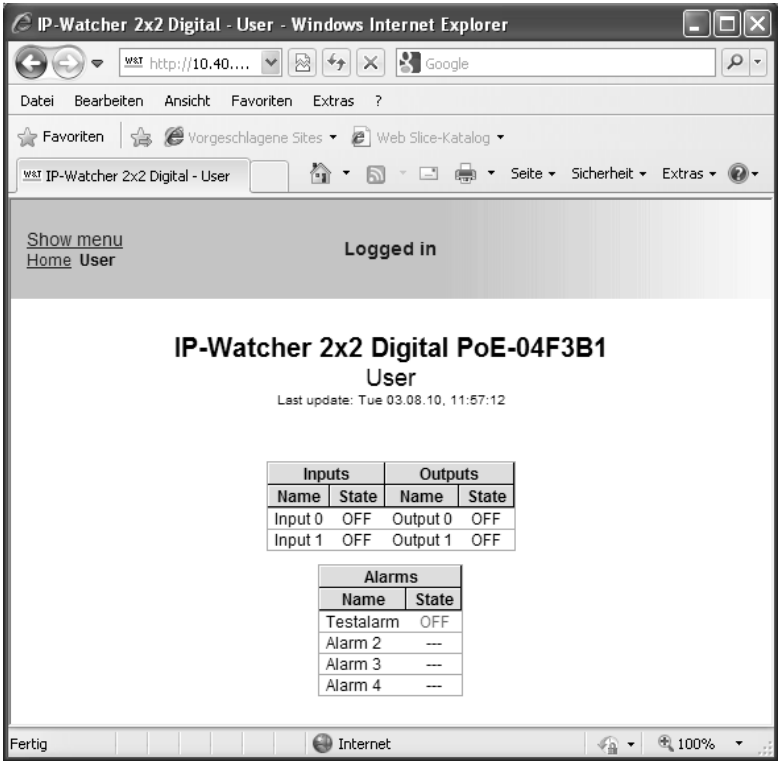
The page can be opened by clicking on links or by entering the following address:

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

The display is refreshed once a second. The time of the last update is shown above the tables. That time also represents the system time of the IP-Watcher.

The links in the upper left corner allow you to show the configuration menu and navigate directly to the homepage.

The overviews show activated inputs and outputs highlighted in green. Deactivated ones are shown in black. Alarms are red if activated and green if deactivated.



User page with self-refreshing system overview of the IP-Watcher

The alarm overview shows only the status of the configured alarms. The rest of the alarms are greyed out.

If the configuration menu was used to set an artificial trigger for an alarm to generate the messages for the alarm, the word *Test* flashes in the alarm overview. If an alarm is in this state, the set trigger must be first rescinded from the configuration page before the device can again trigger alarms based on an actual input condition.

3.4 Hiding and showing the configuration menu

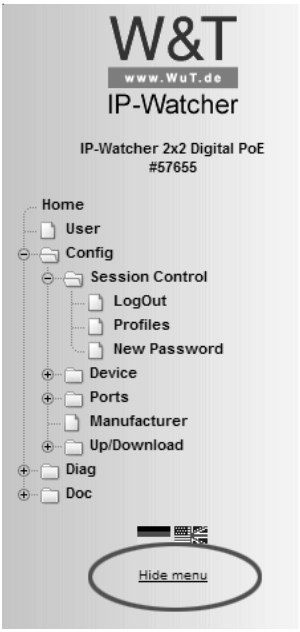
If the configuration menu is not visible, the pages

- Home (*home.htm*)
- User (*user.htm*)

in the upper left corner provide the link *Show menu* for making the menu tree visible.

Link for showing the configuration menu

In addition to the link for showing the configuration menu, the pages listed above also provide links for opening the other control page.



Link for hiding the configuration menu

The link for hiding the configuration menu is then only visible beneath the menu tree if one of the two main pages (*home.htm, user.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 IP-Watcher 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 IP-Watcher can now be read out and displayed. Acknowledging alarms or changing the configuration is however not possible.

- *Administrator*: The administrator password provides full access to the device. Changing the configuration and acknowledging alarms is now possible.
- *Operator*: Operator access rights are limited to acknowledging alarms, 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 Alarms

The IP-Watcher allows up to four different alarms to be used which are tripped based on observation of network devices. Messages can be output depending on the status of the alarms. Various network protocols are available for this.

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

It is also possible to report switching of one of the integrated digital outputs locally when a predefined alarm condition is met.

The device also allows you to configure acknowledgeable alarms. An acknowledgeable alarm remains active after it is triggered until a confirmation is issued, even if the trigger (condition) is no longer in effect. The acknowledgement can be made per software using the page *home.htm* and/or per hardware by wiring one of the previously defined inputs.

Four messages can be defined for each alarm:

- Alarm ON: Sent when the alarm is activated by the preset trigger condition..
- Re-Trigger ON: Sent when the trigger condition is met again after a clear and the alarm was already activated by an earlier trigger and is still present.
- Trigger OFF: When the trigger condition is cleared this message is sent..
- Alarm Ack: An acknowledgement of the alarm causes the device to send this message..

If an alarm switches an output, the latter remains active for non-acknowledgeable alarms until the trigger condition has been cleared. For acknowledgeable alarms the output remains active until acknowledgement.

For an alarm to be triggered the trigger signal must be present for at least 25ms. The response of the IP-Watcher follows...

- ...immediately when an output is switched.
- ...every 10s for mail alarms.
- ...once a second for all other network-based message types.

Since generating messages can be done considerably faster than they can be sent, there are rules which regulate messages:

- If the system has received an acknowledgment (ACK) for an acknowledgeable alarm, this alarm cycle is considered to be finished. Messages not yet sent continue to be delivered.
- If an acknowledged alarm whose messages are not yet completely sent is triggered again, all messages for the old alarm cycle are deleted. Activation starts a new run which should not be mixed with messages from past and processed triggers..
- If the triggering of an alarm, the trigger clear and the acknowledgement takes place faster than the device can detect these status changes, an ordered message sequence is no longer possible. If the acknowledgement is not detected due to too high a switching frequency and the alarm is then triggered again, this status is considered to be a re-triggering of the alarm.

If delays occur when sending messages, for example due to wait times in opening the connection, these delays also affect the as yet unsent messages.

4.1 IP Watch List

The trigger condition for an alarm is always the non-response of a network component. Before the alarms can be configured in detail, the network components in question must be added to the *IP Watch List*. This centralized list is later used to assign the components to the individual alarms.

IP addresses and host names are managed on the page

Config >> Device >> IP Watch List

Here you find functions for...

- ...Adding new deices.
- ...Scanning a network sector
- ...Editing an existing entry.
- ...Deleting an individual entry.
- ...Deleting all entries.

The *IP Watch List* may contain up to 250 entries.

Empty IP Watch List

4.1.1 Insert entry

The *Insert* button takes you to the screen for adding new devices to the *IP Watch List*.

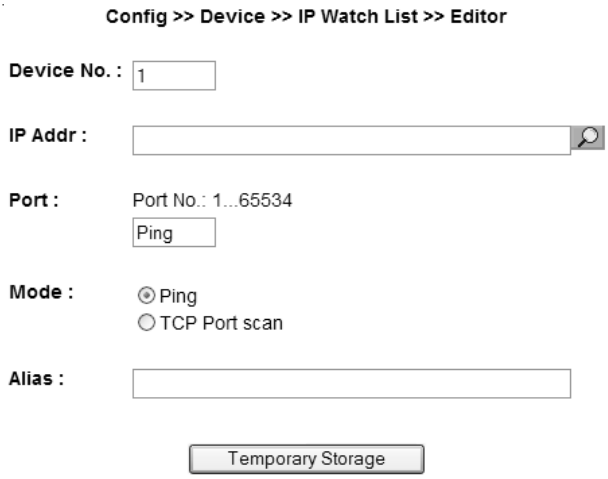
The value *Device No.* determines the position of the device in the list. In the field *IP Addr* you enter the IP address or host name of the network component you wish to watch.

The IP Watcher supports two methods for cyclically polling the monitored network components:

- Ping: Sending out an ICMP „Echo Request“ which must be responded to with an ICMP „Echo Reply“ according to the protocol definition.
- Opening and closing a TCP port: A freely selectable TCP port is opened and then properly closed.

Be sure that the selected monitoring method is supported by the network component in question.

At Alias you can enter an individual text, which describes the device to be observed abstractly.



Adding network components to the IP Watch List

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

4.1.2 Automatic insertion by scanning

Behind the *Scan* button is a dialog box you can use to scan a definable network segment once. Here all the IP addresses for the specified address range are either pinged or scanned by opening and closing a selectable TCP port. If an address responds the scan, the IP Watcher adds it to the *IP Watch List*.

The parameter *Device No.* specifies the position starting at which the found IP addresses are added to the list. Any entries already found at this position are moved down one.

In the fields *Start IP Address* and *Stop IP Address* enter the limits of the IP address range you want to scan. (Example: 192.168.1.1 - 192.168.1.100).

The scan procedure is started by clicking on the *Scan* button. The progress of a running scan is indicated by a status bar.

Scanning the network range

4.1.3 Editing entries

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

4.1.4 Deleting

The entry selected from the pull-down box can be removed from the *IP Watch List* by clicking on the *Delete* button.

4.1.5 Deleting the IP Watch List

Clicking on the *Delete all* removes all entries from the *IP Watch List*.

4.2 Configuring alarms

You can use the configuration menu to set parameters for the available alarms 1 - 4. To do this, open the configuration page

Config >> Device >> Alarm >> Alarm X

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

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

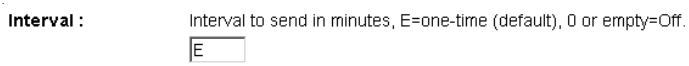
In the *IP Watch List* block you will find all network components which have already been added to the *IP Watch List*. Check the box in front of the entries you want to be monitored by the alarm.

If you assign an alarm to multiple IP addresses, a single non-responding IP address is sufficient to trigger the alarm. Is there another non-responding IP address the alarm is triggered again.

User the parameter *Trigger Count* to specify the number of permitted failed poll attempts.

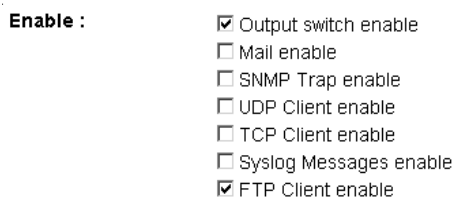
The value *Polling Rate* determines the interval in seconds at which the IP addresses assigned to the alarm are polled. Note here that the attempt to poll and IP address may take up to five seconds if it is no longer reachable.

Use the *Interval* field to determine the send interval for the alarm. *E* is preset, which corresponds to one-time sending. Here yhou can enter any number of minutes as a send interval.



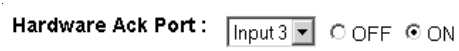
The repetition takes place only as long as the alarm is active. For acknowledgeable alarms this is until an ACK, otherwise until the trigger has been cleared.

The *Enable* block contains all the message types. Here you select the communication path for reporting the alarm.



A possible acknowledgement can be set in the *Ack Enable* block. A hardware and/or software acknowledgement may be selected.

If a hardware acknowledgement was selected, use the option *Hardware Ack Port* to specify the input that acknowledges the alarm. In addition you must specify the edge used for triggering the ACK.



Apply the changes by clicking on *Save*.

4.2 Formulating message texts

For the messaging types reporting over the network, three messages each can be formulated which are sent by the device depending on the alarm status:

- Alarm ON message: This message is sent whe the alarm is activated.

- Re-Trigger ON message: If the alarm is still present because it has not yet been acknowledged but the trigger has already been cleared and then tripped again, this message is sent.
- Trigger OFF message: This message is sent when the trigger is cleared.
- Alarm ACK message: This message is sent when the alarm is acknowledged.

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

`Config >> Device >> Alarm >> Alarm 1 >> Mail`

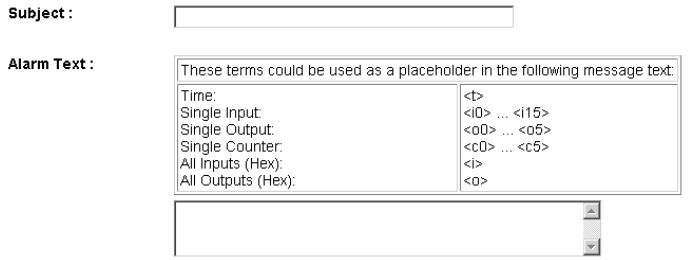
There you select the alarms you want to be sent in the *Enable Text* block.

Selecting the possible messages for an alarm

In the fields *Subject* and *Alarm Text* you enter the subject and the message text which you want sent for *Alarm ON message* and *Re-Trigger ON message*.

The fields *Alarm Ack Subject* and *Alarm Ack Text* contain the subject and message text for the message which is sent directly after acknowledging an alarm.

For *Trigger OFF Subject* and *Trigger OFF Text* you enter the subject line and message text you want sent when the trigger is cleared.



Subject and message entry for Alarm and Re-Trigger

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.

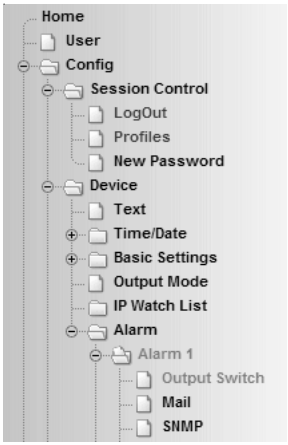
Alarm Variable	Beschreibung
<dn>	Device Name (Config >> Device >> Text)
<i>	Input state, hex
<i**x**>	State of Input no. **x** (ON / OFF)
<in**x**>	Name of input no. **x**
<o>	Output state, hex
<on**x**>	Name of output no. **x**
<L>	information about all non-responding devices
<t>	Time of event (TT.MMM.YYY hh:mm:ss)
<$y>	Year (YYYY)
<$m>	Month (MM)
<$d>	Day (DD)
<$h>	Hour (hh)
<$i>	Minute (mm)
<$s>	Second (ss)
x liegt zwischen 0 und 1	

Mail tags for dynamic creation of message texts

In addition to the alarm messages, the specific parameters for the messaging type still need to be set on the message pages. More detailed information can be found in the respective sections of this manual.

4.3 Local alarming

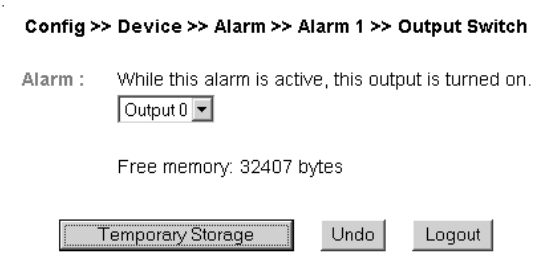
To switch a digital output when there is an alarm, open the profile *Local Alarming*.



„Local alarm“ profile

Configure the alarm condition for the desired alarm using the steps explained in the section *Configuring alarms*.

On the sub-page *Output Switch* specify the output you want to switch when there is an alarm. The selected output is active for acknowledgeable alarms until ACK, otherwise until the trigger condition is no longer met.

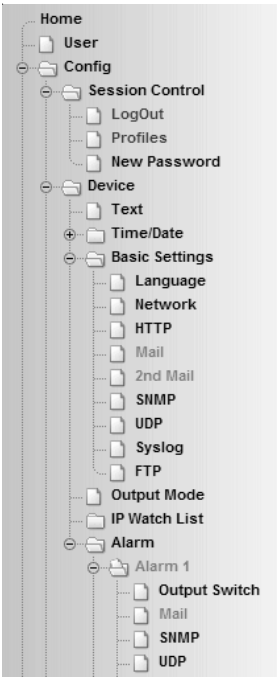


Definition of the switching output

Apply the changes by clicking on *Temporary Storage*.

4.4 Alarming per e-mail

Open the profile *Alarm via E-Mail*.



„Alarm via E-Mail“ profile

Configure the alarm condition for the desired alarm using the steps explained in the section *Configuring alarms*.

4.4.1 General settings

First go to thepage

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

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

The e-mail function allows an alarm 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*.

On the following configuration page, 2nd Mail, you can set up an alternate mail account. This alternate onewill be used automatically, if the first one is not accessable.

„Mail enable“ on the configuration page „Mail“ must be checked to activate 2nd Mail.

4.4.2 Mail parameters and texts

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

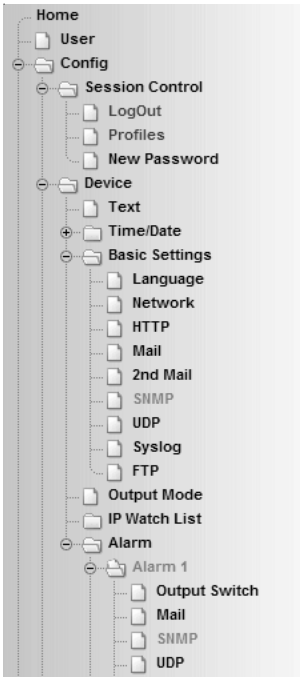
```
Config >> Device >> Alarm >> Alarm X >> Mail
```

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 texts as described in the section *Formulating message texts*and apply the changes by clicking on *Save*.

4.5 Alarming per SNMP trap

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



„SNMP incl. alarm via trap“ profile

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

4.5.1 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*.

4.5.2 SNMP parameters and texts

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

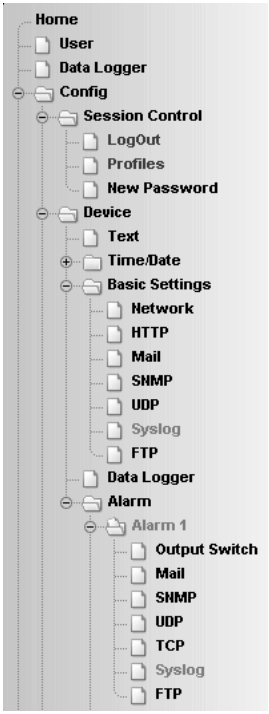
Config >> Device >> Alarm >> Alarm X >> SNMP

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

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

4.6 Alarming per Syslog

Open the profile *Syslog messages incl. alarm*.



Profile „Syslog messages incl. alarm“

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

4.6.1 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 IP-Watcher and thereby allows sending of messages using the syslog protocol.

Apply the changes by clicking on *Save*.

4.6.2 Syslog parameters and texts

Go to page

```
Config >> Device >> Alarm >> Alarm 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.

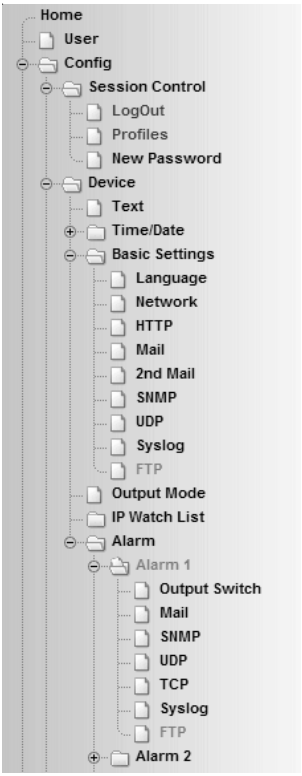
Finally, configure the require message texts as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

4.7 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 alarm condition for the desired alarm as described in the section *Configuring alarms*.



„Alarming via FTP (client mode)“ profile

4.7.1 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.

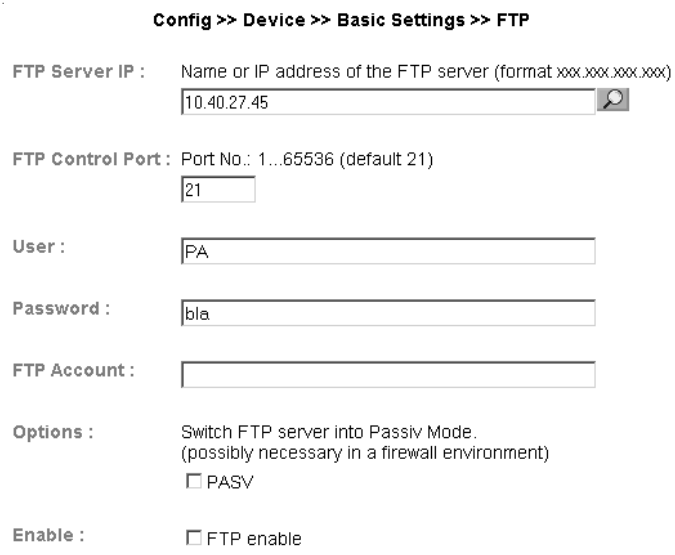
In the *FTP Control Port* field specify the port you want to use for the connection. The standard port for FTP access is 21. This port is already preset and should work on most systems on the

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 IP-Watcher. 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*.

4.7.2 FTP parameters and texts

Go to page

```
Config >> Device >> Alarm >> Alarm X >> FTP
```

and enter the alarm-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 texts 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*.

4.8 Alarming per TCP client

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

Go to page

```
Config >> Device >> Alarm >> Alarm 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 require message texts as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

4.9 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 alarm condition for the desired alarm as described in the section *Configuring alarms*.

Go to page

```
Config >> Device >> Alarm >> Alarm 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 texts as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

5 Basic settings

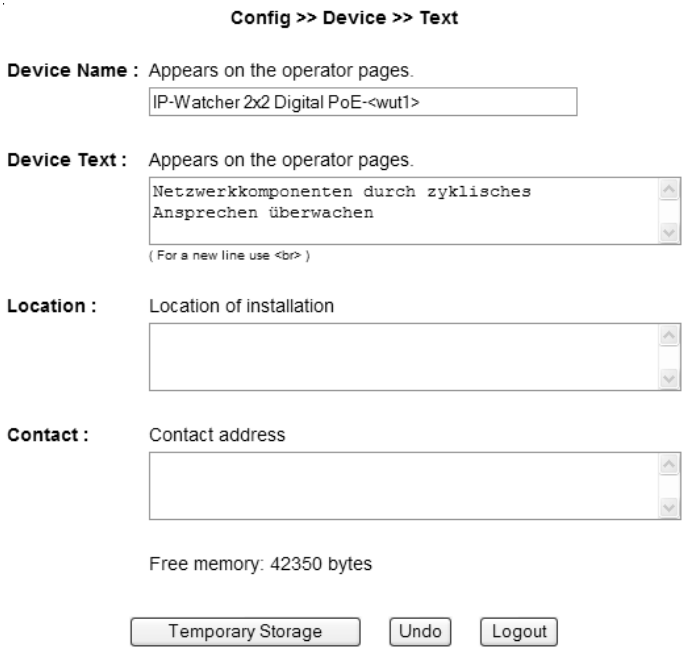
5.1 Device name

From the configuration menu open the page

`Config >> Device >> Text`

to edit the following texts:

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

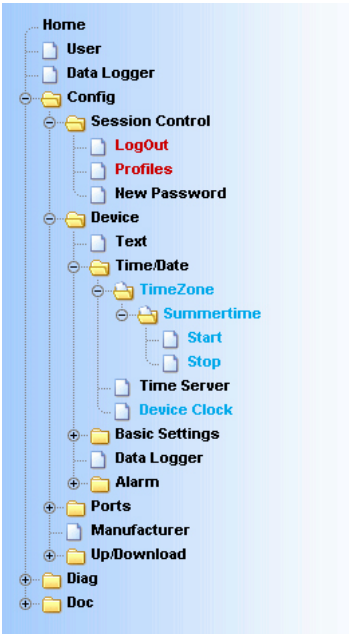


Configuration page for device texts

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

5.2 Local time setting

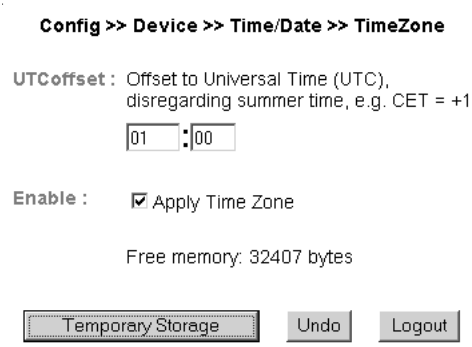
To manually set the system clock, the device provides a guided procedure using the profiles. To do this, open the profile *Local time setting*.



Configuration tree with selected profile for local time setting

5.2.1 Time zone

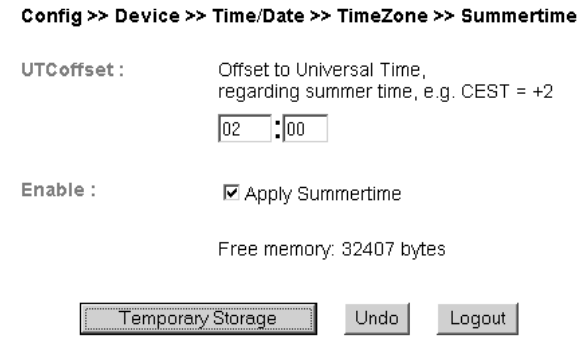
On this page you specify the time zone in which the device is located. The settings refer to UTC (Universal Time Coordinated). Apply the settings by clicking on *Save*.



Time zone configuration

5.2.2 Summertime

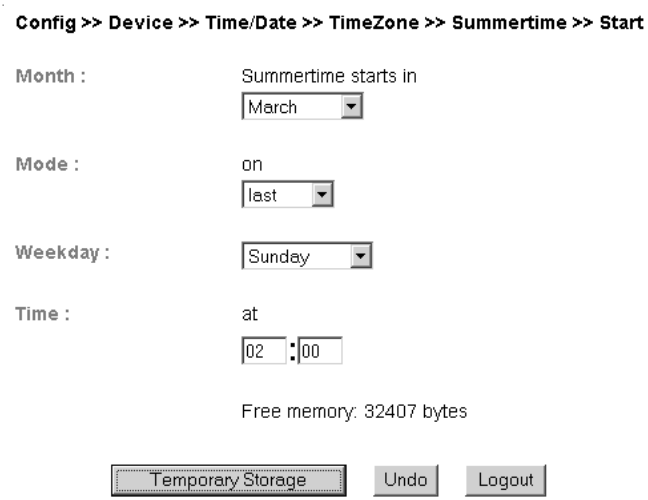
If you want your device to automatically adjust to daylight saving time, first enter the offset to UTC. The standard value (including for Germany) is two hours. Activate this function by checking the box *Apply Summertime* and save the settings.



Setting daylight saving time

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

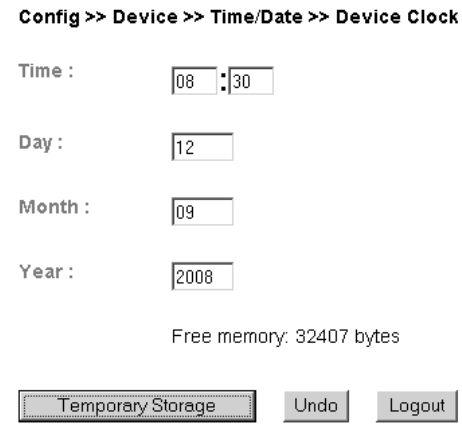
The factory default setting is for daylight saving time to begin on the last Sunday in March at 2:00 a.m. The end of daylight saving time is preset for the last Sunday in October at 3:00 a.m.



Rule for beginning daylight saving time

5.2.3 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.

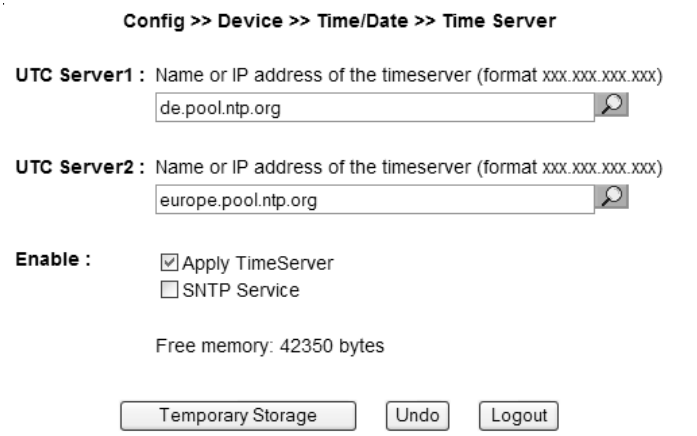
5.3 Automatic time setting using a network service

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.

5.4 Activate SNTP time server

If the system time for the device is synchronized with a time server, the IP Watcher itself can assume the function of a time server.

SNTP (Simple Network Time Protocol) is supported here.

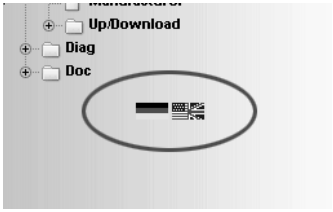
To start the time server service, activate the option *SNTP Service* on the configuration page

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

5.5 Language

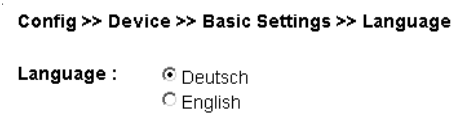
You can use the configuration menu to specify the system language. This can be done either using the flag link below the configuration menu, or navigate to:

`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.

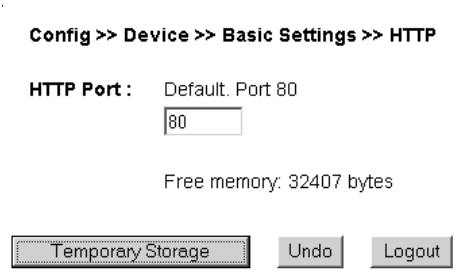
5.6 HTTP-Port

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 IP-Watcher>/home.htm:<portnumber>`



Configuring the port number

5.7 System traps per SNMP and SNMP basic configuration

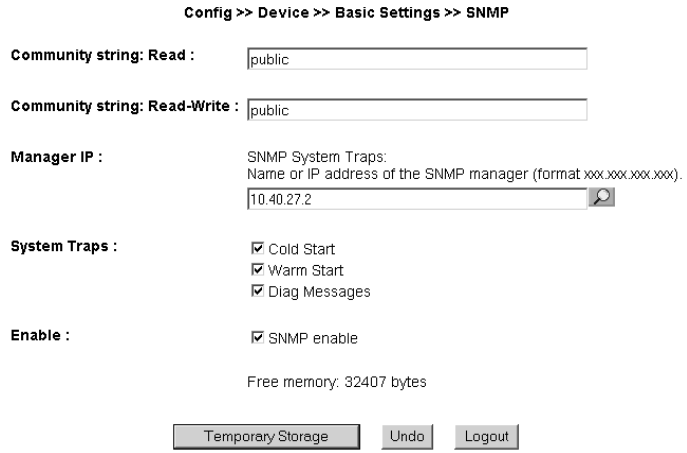
The following traps can be sent to an SNMP manager using SNMP protocol:

- Cold Start: Restart after power has been interrupted or has failed
- Warm Start: Restart after device reset

In addition, diagnostic messages which have arrived in the device can be sent.

The SNMP configuration is made on the following page:

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



SNMP configuration

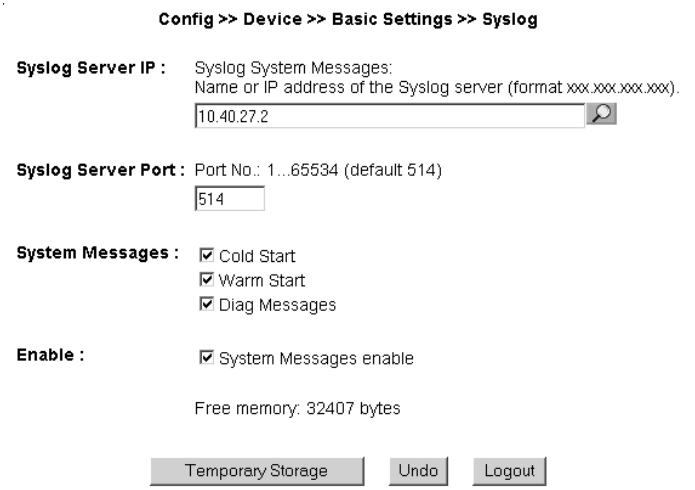
As opposed to the other messaging procedures, SNMP is activated by default.

Here you define the basic parameters needed for SNMP operation:

- Community String: Read: This character string can be used for read access to the device in your SNMP manager.
- Community String: Read-Write: This string gives you both read and write access to the device in your SNMP manager.
- Manager IP: Contains the IP address of your SNMP manager. IP-Watcher SNMP messages are sent to this address.
- System Traps: Select the messages you want to send.
- Enable: Enable the SNMP function

5.8 System Messages per syslog

Just as for the SNMP traps, you can send Cold Start, Warm Start and diagnostic messages to a syslog server.



System messages using the syslog protocol

To enable this message system, go to the configuration page

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

and enter the IP address of a syslog server and the port number through which you want communication to take place.

Select the message types you want to send to the server and check *System Messages enable*.

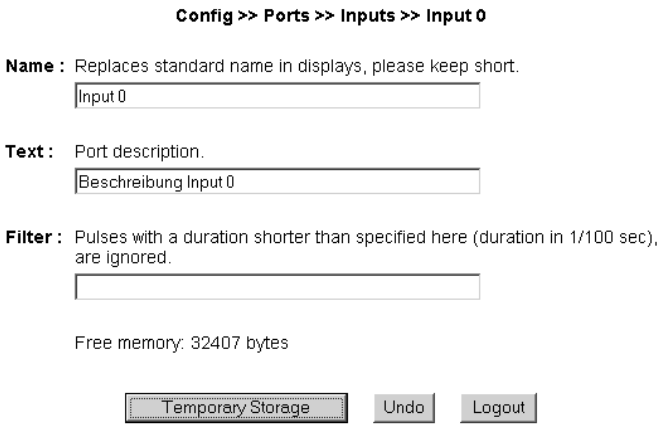
Save your settings by clicking on *Temporary Storage*.

5.9 Port settings - Inputs

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

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

```
Config >> Ports >> Inputs >> Input 0
```



Basic configuration „Input 0“

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

The description entered in the *Text* field can for example provide a more detailed description of the function or installation location of the sensor.

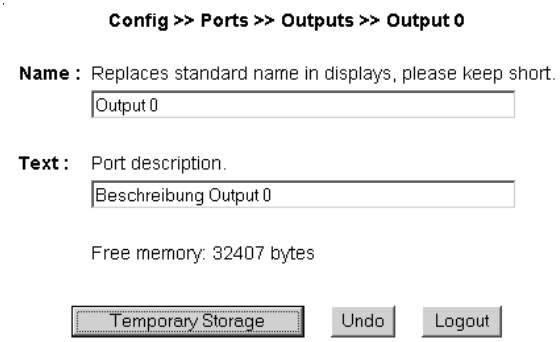
Under *Filter* you can specify a time for which a signal must be present (minimum) in order to be recognized. If a level is present for less than the time specified here, it will be ignored.

The units are in 1/1000 seconds. If no value is entered here, this function is disabled.

5.10 Port settings - Outputs

To change the settings for Output 0 for example, go to:

```
Config >> Ports >> Outputs >> Output 0
```



Settings„Output 0“

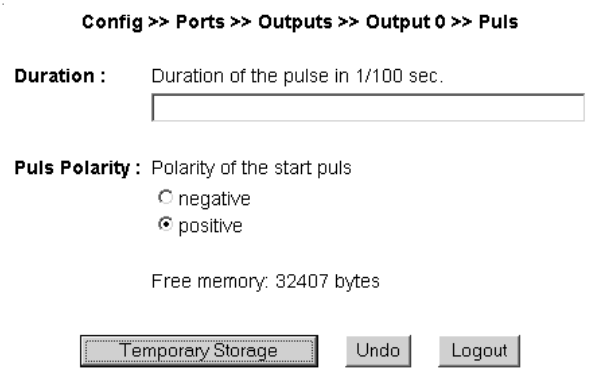
In this field you enter a name for the output. This name is then displayed in the browser for Output 0.

The description entered in the *Text* field can for example provide a more detailed description of the function or installation location of the actuator.

In addition to the purely static switching of the outputs to ON or OFF, the IP-Watcher also allows you to output pulses. This means an output can be switched ON or OFF for a preset time, returning to its rest state after the set pulse length.

For example, to configure Output 0 on the device to output pulses, go to the navigation tree and select:

```
Config >> Ports >> Outputs >> Output 0 >> Puls
```



Pulse configuration for outputs

For Duration enter the desired pulse length in 1/100‘s of seconds. A value of 1000 corresponds to a 1 second long pulse.

If the polarity of the pulse is set to positive, the output is not switched when in the rest state. If the output is set to ON by an alarm trigger, the IP-Watcher switches supply voltage to the output for the set pulse duration.

For negative pulse polarity the rest level of the output is the same as supply voltage. When the output is switched the level is turned off for the set time.

Enter a *0* for *Duration* and a negative *Puls Polarity*, the output is inverted.

On

`Config >> Device >> Output Mode`

you can check the option *Internal 24V enable*. Then 24V is internally switched on the terminals Vdd and GND. Doing this an extra power supply for the IOs is not required. Then a maximum current of 150mA can be used on the outputs.

6 Troubleshooting and Testing

The IP-Watcher uses internal error management and diagnostics. This can be found in the configuration tree under the heading

`Diag`

6.1 Report

When an error occurs, it is documented in a diagnostics report and can be read out there at any time.

All error messages are stored in the device and remain there even after the cause of the error has been resolved. If the error is no longer current, it is moved from the Diagnostic Report to the Diagnostic Archive.

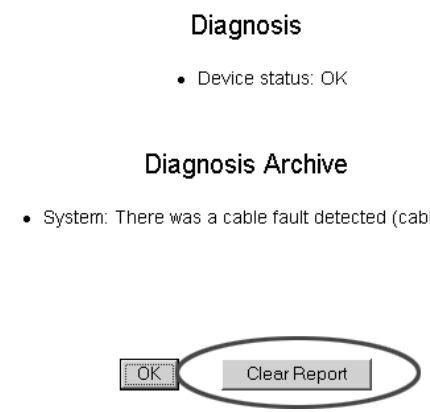
Diagnostic Report and Diagnostic Archive

The Diagnostic Report and Diagnostic Archive can be viewed at

`Diag >> Report`

Clicking on the *Delete report* button deletes all existing messages from the memory.

To clear both error memories using the „Delete report“ button, you must be logged in with Administrator rights.



Access with Administrator rights

A reset, whether caused by interrupting the supply voltage or performing a reset from the *Logout* page, also deletes the report.

In addition, error and diagnostic messages can be processed using SNMP traps or as a syslog message. For additional information, please refer to the sections *System Traps per SNMP* and *System Messages using syslog*.

6.2 Check Config

The device allows an Administrator to view and check the current configuration on an overview Web page.

This is opened using the configuration menu:

```
Diag >> Test >> Check Config
```

This Web page shows which access and message types are enabled with which parameters. The device performs a plausibility check of the settings. If missing parameters are

detected which prevent proper operation of the access type, the corresponding fields are highlighted in orange. Clicking on the link to the incorrect configuration takes you directly to the corresponding settings page

Parameter	HTTP	UDP	SNMP	Mail	Syslog	FTP
Enable Flag	----	OFF	ON	ON	OFF	OFF
Source Port	80	42279	161	auto	514	auto
Source IpAddr	10.40.27.57	10.40.27.57	10.40.27.57	10.40.27.57	10.40.27.57	10.40.27.57
Destination Port	n.a.	n.a.	----	25	----	----
Destination IpAddr	----	----	----	----	----	----
Active	OFF	OFF	**ON**	FAIL	OFF	OFF

Overview and plausibility check of the settings with an error

Also checked and displayed is which send paths have been selected for the alarms and whether all the necessary parameters have been configured. Here again the access types are highlighted in orange if they have not been completely configured.

Parameter	Set Output	Alarm Mail	SNMP Trap	UDP Client	TCP Client	Syslog Message	FTP Message
Alarm / Trap	ON	OFF	OFF	OFF	OFF	OFF	OFF

Alarm send paths

6.3 Check Alarm

To check whether the configured message types are functioning properly for the enabled alarms, you can go to the

`Diag >> Test >> Check Alarm`

page and manually set trigger, acknowledgement and reset for the available alarms

These buttons allow triggering of all alarm messages for the enabled alarms without the actual trigger condition having to occur.

Clicking on the *Trigger* button tells the device that the triggering condition for the alarm has been met. The reachability of linked entries from the *IP Watch List* is here irrelevant, but the actual trigger condition should still not be met. This is simply a virtual alarm triggering.

The *ACK* button acknowledges the alarm triggered when you clicked on *Trigger*. Acknowledgement is only possible if at least one acknowledgement variant has been set for the alarm. If no alarm confirmation is configured, the ACK button is greyed out.

The *Reset* button resets the artificially set trigger. This is an absolute requirement when testing the alarms, since otherwise an actually occurring alarm will not be recognized.

If the *Trigger* button was used to set an artificial trigger, this is also indicated on the *home.htm* page by flashing texts. On the *home.htm* page an activated test alarm is also shown in the message box above the alarm table.

7 Documentation

7.1 Manual

Explanation of the login levels and important configurations.

Wellcome to Wiesemann & Theis IP-Watcher 2x2 Digital We would like to give you an introduction into getting started with the IP-Watcher and it's configuration.	
Login	There are three level of access with different rights, depending on the login: • **User without rights** is everybody who calls up the websites of the IP-Watcher. All entries are read-only. • **Admin** login permits full access to all alarm control and configuration. • **Operator** login permits access to the alarm control and the configuration of the alarm messages. A login take place depending on the password under this menu entry: **Config** If there is no password defined (default configuration) the access level would always be Admin rights.
Configuration	The main configuration requires **Admin Login**. The multiple functions of the IP-Watcher result in a great count of possible configurations. Don't let this confuse you. Simply walk through the navigation tree top-down and leave all entries unchanged which are not required by your configuration. The "Quick Start" manual shipped with the IP-Watcher shows you which menu items have to be regarded in the operation mode you chose. **The most important configuration parameters are**: • **Network Configuration** Config >> Device >> Basic Settings >> Network Configuration changed will be saved by pressing the "Temporary Storage" button. All changes will be activated by the Save an Logout Buttons. If you wish to restore the factory defaults please select Config >> Session Control >> Logout >> Restore Defaults.
For further informations refer to the "Quick Start" manual. A detailed reference book will be found on the IP-Watcher product page under the following link: www.wut.de	

Abbreviated „Manual“

7.2 Data sheet

The data sheet provides information about the key properties and technical data for the IP-Watcher.

Prod. No.:	**#57655 IP-Watcher 2x2 Digital**
Network:	10/100BaseT autosensing
Protocol:	TCP and UDP sockets, client and server SNMP (including traps), OPC-Server, inventorying, group management
Response times:	Data and switching traffic: typically 12ms
Digital outputs:	2 x Digital Out 6V-30V, 0.5A, groups at 2 outputs, shortcut protection by thermic fuse
Digital inputs:	2 x digital in, max. input voltage +/-30V, protected against reverse connection within this range Switching threshold 8V, +/- 1V, "On" current = 2.2 mA
Plug adapter:	1 x 6 terminal screws
Electrical isolation:	Digital outputs/inputs - network: min. 500 V Digital outputs/inputs - power supply: min. 1000 V
Displays:	Status LEDs for network
Power supply:	Device supply: POE, 18-48V DC, 18-30Veff AC Ouput supply: 6-30V DC, max. 1A
Storage temperature:	-25°C - 70°C
Operating ambient temperature:	0°C - 60°C
Housing:	Plastic housing for top hat rail installation 105 x 75 x 22 mm (l x b x h)
Weight:	approx. 140g

IP-Watcher data sheet

7.3 Property

The *Property* page contains information about the manufacturer, the hard- and software version and the identification of the device in the network.

Device Information	
Manufacturer	Wiesemann & Theis GmbH
- Address	Porschestr. 12 42279 Wuppertal Germany
- Support Hotline	+49-(0)202-2680-0
- Internet	www.wut.de
Typ	IP-Watcher 2x2 Digital PoE
Order No.	#57655
Software Revision	3.20
Hardware Revision	1.00
Bios Software Revision	3.20.3.01.340
Device Identification:	
Name of Device	IP-Watcher 2x2 Digital PoE-04F3B1
System Description	Netzwerkkomponenten durch zyklisches Ansprechen überwachen
Ethernet Address	00-C0-3D-04-F3-B1
IP Address	10.40.27.97
DHCP: DNS Server	0.0.0.0
DHCP: Lease Time	00:00:00 sec

„Property“ page

8 Appendix

8.1 LEDs

In the following the meaning and function of the LEDs on the front panel of the IP-Watcher is explained

8.1.1 Power-LED

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

8.1.2 Status-LED

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

8.1.3 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 IP-Watcher 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 IP-Watcher is no longer operable in this state. Please return the unit through your dealer to W&T for inspection

8.2 Factory defaults

Some situations require that the IP-Watcher 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.

8.2.1 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.

8.2.2 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 IP-Watcher for approx. 15s. The device is now reset to its factory defaults. The LEDs on the front panel will flicker irregularly during this procedure.

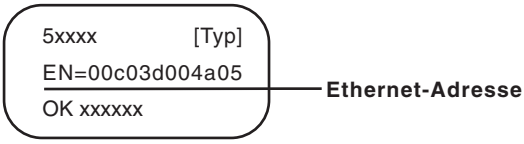
Once the factory default settings have been restored, disconnect the unit from power, remove the jumper and close up the unit. Now proceed to startup.

8.3 Alternative IP address assignment

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

8.3.1 ARP command

Required is a PC which is located in the same network segment as the IP-Watcher and on which TCP/IP is installed. Read the MAC address of the IP-Watcher 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 IP-Watcher, 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.

8.3.2 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 IP-Watcher 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 IP-Watcher 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*.

8.4 Firmware update

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

8.4.1 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 IP-Watcher. 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.

8.4.2 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 IP-Watcher
- The file with the new firmware to be sent to the IP-Watcher

No special preparation of the IP-Watcher 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 IP-Watcher 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 IP-Watcher automatically detects when transmission of the operating software is complete and then carries out a reset.

8.5 Up- and download

Under the heading UpDolwnload, 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 IP-Watcher'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 IP-Watcher must begin with the expression

```
<io-Digital2x2IPW2.1>
```

and end with the expression

```
</io-Digital2x2IPW2.1>
```

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.

8.6 Technical data

Network	Ethernet 10/100BaseT autosensing
Protokol	TCP- and UDP-Client, FTP, Mail, SNMP incl. Traps, Inventory, Groupmanagement
Response times	Data and switching traffic: typically 12ms
Digital outputs	6 x digital out 6V-30V DC, 0.5A, max. total current 3A
Digital inputs	6 x digital in, max. input voltage +/-30V, Protected against polarity reversal within this range Switching threshold 8V +/- 1V, "On" current = 2.2 mA
Connection	1 x 16 screw-type terminals
Galvanic isolation	Digital outputs - network: min. 1000 V Digital inputs - network: min. 2000 V Digital inputs - outputs: min. 1000 V
Serial port	9600Baud, 8 Datenbits, 1 Stopbit, No Parity
Displays	Status LEDs for network 12 LEDs for digital statuses
Power supply	Device: DC 24V-48V, AC 18V-30V Outputs: DC 6V-30V
Storage temperature	-25°C - +70°C
Operating temperature	spacing installation: 0°C - 55°C non spacing installation: 0°C - 50°C
Housing	Kunststoff-Kleingehäuse, 105 x 45 x 75mm (l x b x h)
Weight	approx. 200g

Technical Data