Manual

Web-Alarm 6x6 Digital

W&T

Typ	Web-Alarm 6x6 Digital
Modell	#57651
Release	EN 3.07 02/2009

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!

Contents

1. Introduction

The W&T Web-Alarm makes it possible to trigger local and remote alarms based on digital input signals and counter states. Local alarms are generated by the switching of a consumer connected to one of the six digital outputs. A remote alarm can be triggered for example by e-mail, FTP, SNMP or syslog over a TCP/IP network.

An individual acknowledgement can be configured for all the alarms. This is done network by configuring one of the digital inputs on the unit (hardware acknowledgement) and/or by sending an acknowledgement command per TCP/IP from the controller side to the Web-Alarm (software acknowledgement). An acknowledgement ensures proper recognition and handling of an alarm situation on the part of the operator.

The unit also takes on the function of a data logger. All IO and counter events as well as the triggering, clearing and acknowledging of alarms is recorded with time stamps in internal, non-volatile 8MB flash memory. The recording of events allows you at any time to reconstruct device activity, which can be used for example for analysis purposes.

An integrated Web server provides configuration pages for setting the device parameters. The alarms are operated and monitored using browser-based software which can also be loaded from the Web-Alarm web server into any browser. The software automatically refreshes the display of the current status of the activated alarms, the last event for each alarm, and provides the capability of software acknowledgement. The data logger can also be read out by this software. Various filters can be applied to organize the data as clearly as possible and reduce it to a minimum.

The power can be provided either per PoE over the network or from an external power supply.

The Web-Alarm is particularly useful for autonomous monitoring tasks. Switching an output when there is an alarm situation can trigger a local alarm, for example using a beacon light. It is also possible to place the alarm-triggering unit into a safe state. An alarm over the netowrk reaches even distant personnel quickly and prompts them to act. Network alarming enables the use of an existing network infrastructure, making it possible to send messages individually and without additional cabling. Thanks to the integrated, browser-based software, operation and monitoring is possible not only in the Intranet, but also worldwide over the Internet.

2. Startup

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

2.1 Supply voltage

The following describes the two methods of providing power to the Web-Alarm.

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

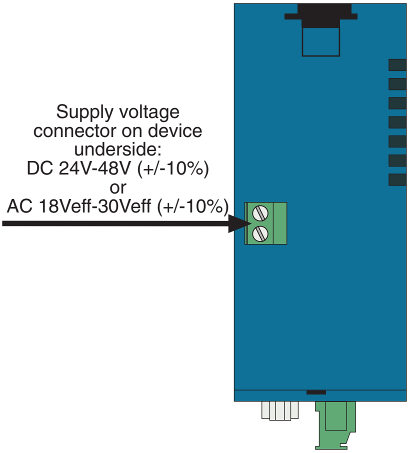
⚠ *If the device is powered using PoE, connecting or disconnecting an additional external power source while the device is running may result in the Web-Alarm restarting. The device resumes normal function after just a few seconds, but IO events which may have taken place in the meantime will not be stored in the internal logger.*

2.1.1 External supply voltage

Connect a supply voltage of 24V...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.

⚠ *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, note correct polarity. Labeling can be found on the screw terminals on the green power plug.



Underside of the device with terminal for the external power supply

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

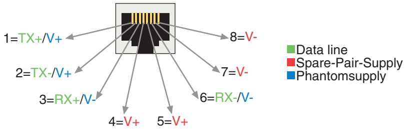
The Web-Alarm is equipped for use in Power over Ethernet environments per IEEE802.3af. The voltage is then provided by the network infrastructure using the RJ45 terminal. The device supports both phantom feed using data pairs 1/2 and 3/6 or spare-pair power using the unused wire pairs 4/5 and 7/8.

To enable power management for the supplying components, the Web-Alarm identifies itself as a Power Class 1 device with a power draw of 0.44W to 3.84W.

⚠ *With an external power supply the Web-Alarm can also be used in networks not providing PoE support.*

2.2 Network connection

The Web-Alarm 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 Web-Alarm 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 500V with respect to the power supply as well as the digital IOs and serial port.

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

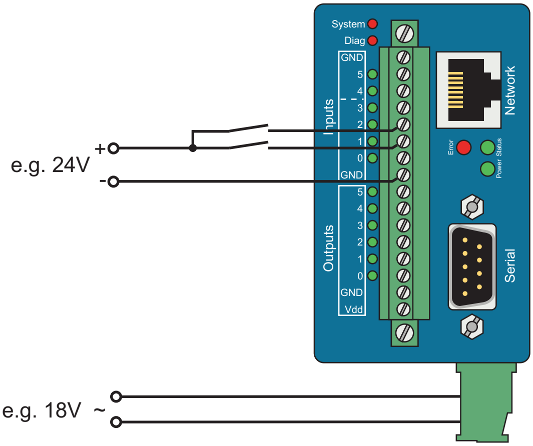
2.3 Wiring the inputs

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 Web-Alarm as an ON or 1 signal. Input voltages between 7V and 9V should be avoided, since their meaning may be ambiguous.

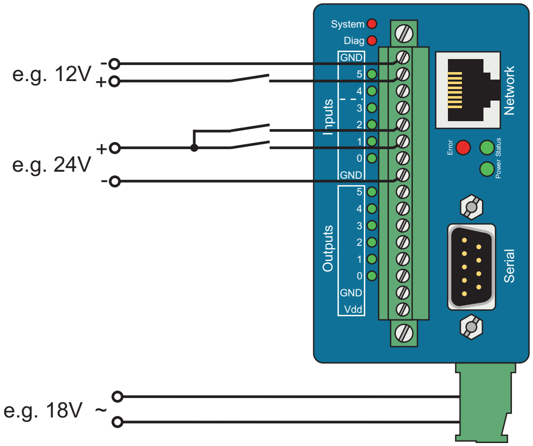
The Web-Alarm inputs are divided into two groups: Inputs 0 - 3 and inputs 4 + 5. These groups are galvanically isolated from each other to 2kV. A separate reference ground is brought out for each input group.

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



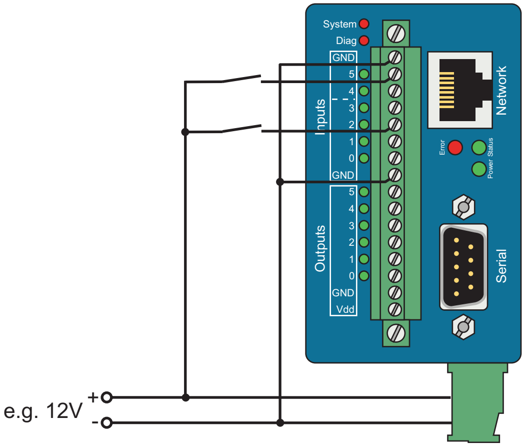
Controlling two inputs in a group

If the input signals have a different reference ground, they should be divided between the two input groups.



Signals with different reference ground

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 Web-Alarm with a DC voltage of 12V-30V. A corresponding wiring example is shown in the following illustration.



Supply voltage as signal voltage

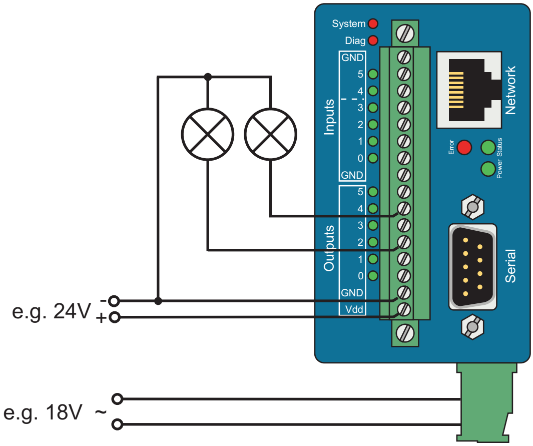
In addition to detecting the input status ON and OFF, each input also has a counter. By default pulses (positive edges) are counted. The counters can however be configured for edge counting. Furthermore, two inputs can be used together for incremental, direction-dependent counting. Here the counter which first detected the change is incremented.

2.4 Wiring the outputs

The six Web-Alarm 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.

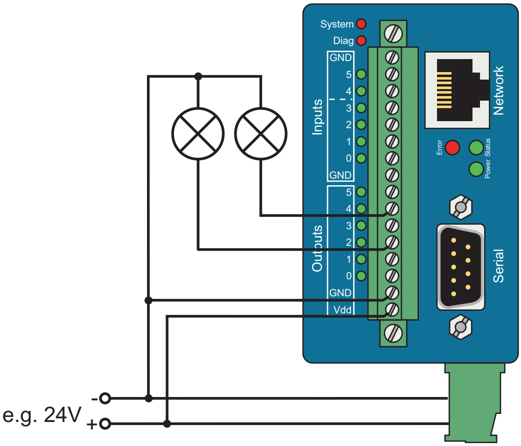
When the outputs are switched using an inductive load (e.g. a relay), a snubber diode should be used to protect them from damage.

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.



Feeding outputs from the unit power 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.*

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.

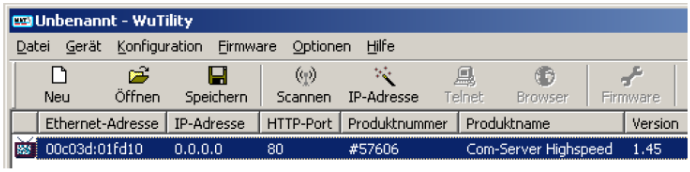
⚠ *The assigned IP address must be unique within the network.*

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 Web-Alarm 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.

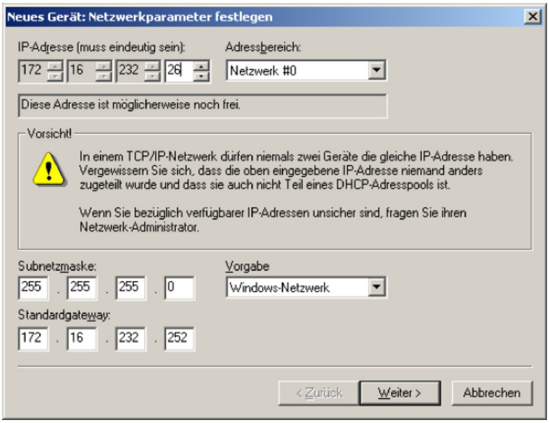
Now select the Web-Alarm from the displayed list. If you have more than one unconfigured W&T network devices in your network, you can use the MAC address to create the relationship between list entry and terminal device:



Ethernet-Adresse	IP-Adresse	HTTP-Port	Produktnummer	Produktname	Version
00c03d:01fd10	0.0.0.0	80	#57606	Com-Server Highspeed	1.45

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:



IP-Adresse (muss eindeutig sein): 172 . 16 . 232 . 26

Adressbereich: Netzwerk #0

Diese Adresse ist möglicherweise noch frei.

Vorsicht!

In einem TCP/IP-Netzwerk dürfen niemals zwei Geräte die gleiche IP-Adresse haben. Vergewissern Sie sich, dass die oben eingegebene IP-Adresse niemand anders zugeteilt wurde und dass sie auch nicht Teil eines DHCP-Adresspools ist.

Wenn Sie bezüglich verfügbarer IP-Adressen unsicher sind, fragen Sie ihren Netzwerk-Administrator.

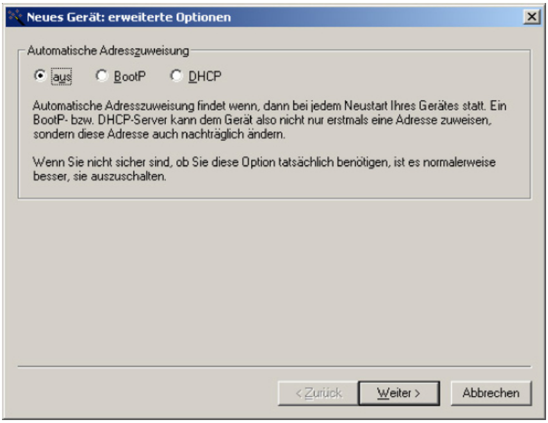
Subnetzmaske: 255 . 255 . 255 . 0

Vorgabe: Windows-Netzwerk

Standardgateway: 172 . 16 . 232 . 252

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:



Neues Gerät: erweiterte Optionen

Automatische Adresszuweisung

● aus ○ BootP ○ DHCP

Automatische Adresszuweisung findet wenn, dann bei jedem Neustart Ihres Gerätes statt. Ein BootP- bzw. DHCP-Server kann dem Gerät also nicht nur erstmals eine Adresse zuweisen, sondern diese Adresse auch nachträglich ändern.

Wenn Sie nicht sicher sind, ob Sie diese Option tatsächlich benötigen, ist es normalerweise besser, sie auszuschalten.

Configuration dialog box for address assigning

By clicking on the *Next* button the Web-Alarm 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 Web-Alarm, 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 Web-Alarm 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.
- **Serial port:** As part of serial IP address assignment you can specify directly following the address string the following options for activating/deactivating the DHCP and BOOTP/RARP protocols: -**0** (deactivates DHCP and BOOTP/RARP), -**1** (activates BOOTP/RARP) and -**2** (activates DHCP). A detailed description of the procedure is found in the section *Alternative IP address assigning*.
- **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 *Network Basic Settings*.

2.6.2 System name

In order to support any later automated updating of the DNS system by the DHCP server, the Web-Alarm identifies itself within DHCP with its system name. The factory set name is *Web-Alarm 6x6 Digital-* followed by the last three places in the Ethernet address. For example, the factory set system name of a Web-Alarm having Ethernet address 00:c0:3d:01:02:03 is *WEBIO-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 Web-Alarm 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 Web-Alarm 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

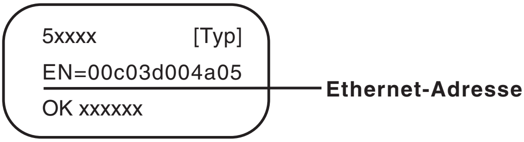
`Home >> Doc >> Property`

is displayed in seconds.

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

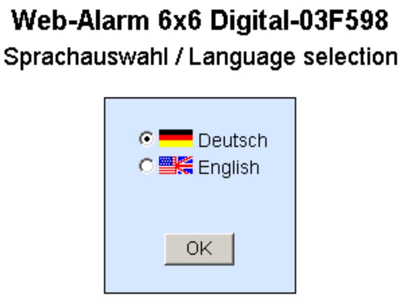
Fully dynamic IP address assignment, whereby the Web-Alarm receives a different IP address each time it restarts or after the lease time has expired, only makes sense in network environments having automatic cross-connection between the DHCP and DNS services. In other words: When assigning a new IP address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



Web-Alarm 6x6 Digital-03F598

Sprachauswahl / Language selection

● Deutsch

○ English

Language selection at initial startup

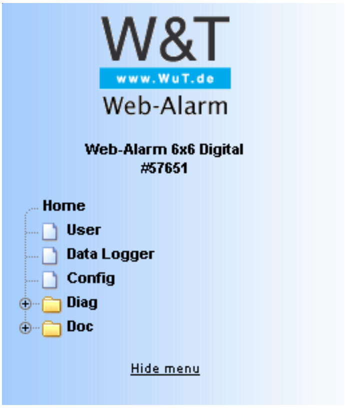
2.8 Assigning the basic network parameters

Open the start page of the Web-Alarm 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 Web-Alarm>/index.htm
```

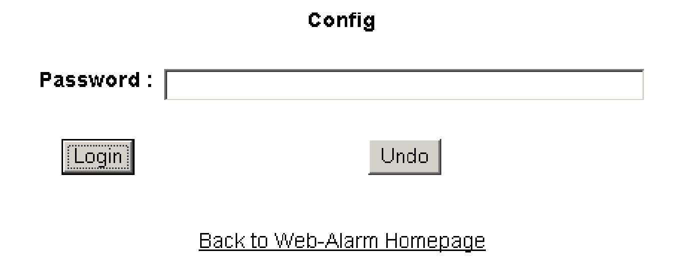
Here the configuration menu is already visible and does not have to be manually shown.

Select the menu item *Config*.



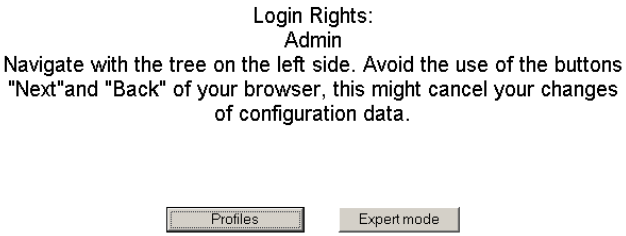
Configuration menu in the base state

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

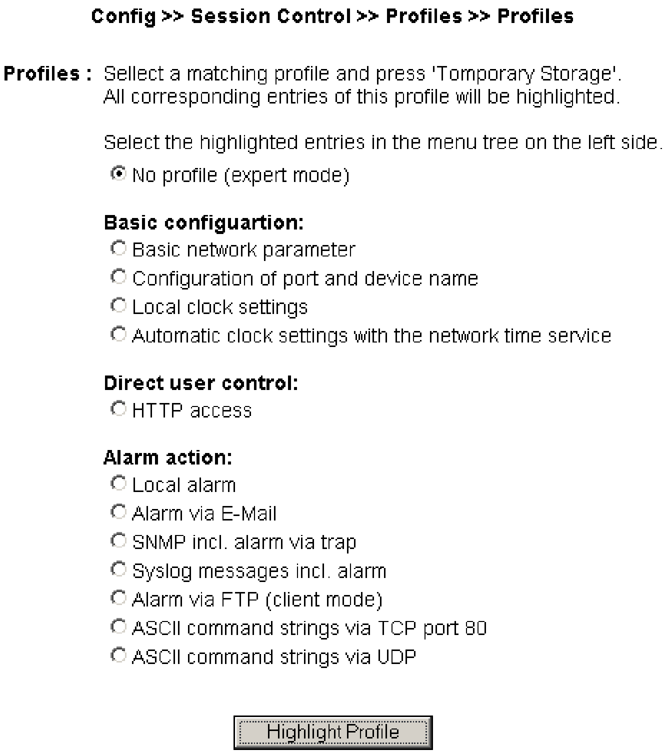
On the next page select the configuration path using the profiles



Login Rights:
Admin
Navigate with the tree on the left side. Avoid the use of the buttons "Next"and "Back" of your browser, this might cancel your changes of configuration data.

Selection for profiles or Expert mode

Select the profile *Network base parameters* and click on the *Display profiles* button.



Config >> Session Control >> Profiles >> Profiles

Profiles : Sellect a matching profile and press 'Tomporary Storage'.
All corresponding entries of this profile will be highlighted.

Select the highlighted entries in the menu tree on the left side.

● No profile (expert mode)

Basic configuartion:

○ Basic network parameter
○ Configuration of port and device name
○ Local clock settings
○ Automatic clock settings with the network time service

Direct user control:

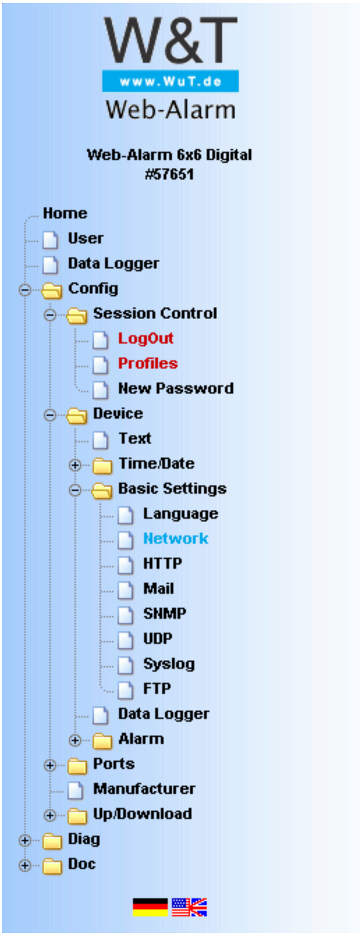
○ HTTP access

Alarm action:

○ Local alarm
○ Alarm via E-Mail
○ SNMP incl. alarm via trap
○ Syslog messages incl. alarm
○ Alarm via FTP (client mode)
○ ASCII command strings via TCP port 80
○ ASCII command strings via UDP

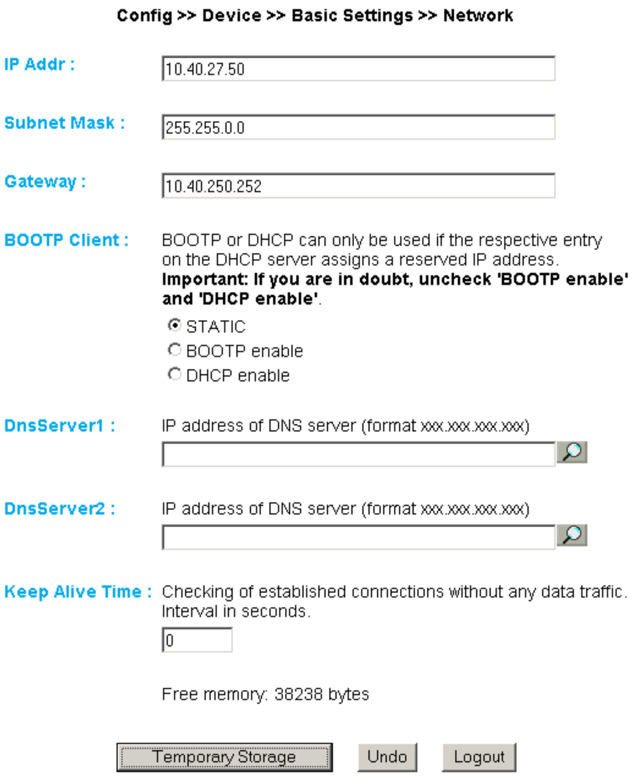
Profile selection

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 Web-Alarm.



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.



Config >> Device >> Basic Settings >> Network

IP Addr : 10.40.27.50

Subnet Mask : 255.255.0.0

Gateway : 10.40.250.252

BOOTP Client : BOOTP or DHCP can only be used if the respective entry on the DHCP server assigns a reserved IP address.
Important: If you are in doubt, uncheck 'BOOTP enable' and 'DHCP enable'.

● STATIC
○ BOOTP enable
○ DHCP enable

DnsServer1 : IP address of DNS server (format xxx.xxx.xxx.xxx)

DnsServer2 : IP address of DNS server (format xxx.xxx.xxx.xxx)

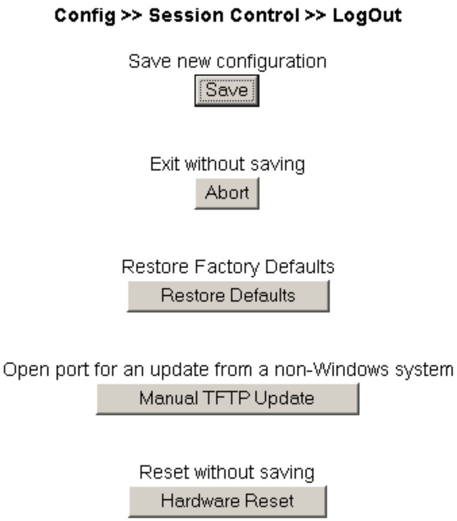
Keep Alive Time : Checking of established connections without any data traffic. Interval in seconds.
0

Free memory: 38238 bytes

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.



Config >> Session Control >> LogOut

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 Web-Alarm 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 five pages which you can directly address from the browser. In the following the URLs are briefly explained and listed.

The main page (homepage) automatically refreshes to show the status of the activated alarms and makes it possible for the logged in user to confirm alarms using software acknowledgement and display the content of the data logger:

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

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

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

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

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

To export the contents of the data logger to a CSV file:

```
http://<IP address of the Web-Alarm>/logger.htm
```

Diagnostics messages can be retrieved at the following address:

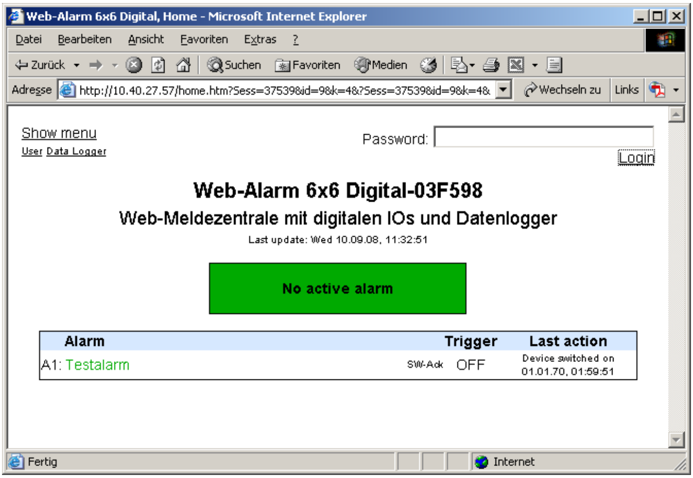
```
http://<IP address of the Web-Alarm>/diag.htm
```

3.2 Homepage

The homepage, which can be opened using address

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

- Provides an overview of the status of all activated alarms and gives alarm-specific information..
- Allows pending alarms to be reset using software acknowledgement.
- Provides tools for reading alarm and input informationfrom the data logger.


Web-Alarm 6x6 Digital, Home - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
Wechseln zu
Links
Fertig
Internet

http://10.40.27.57/home.htm?Sess=37539&id=9&k=4&?Sess=37539&id=9&k=4&

Show menu

User Data Logger

Password:

Login

Web-Alarm 6x6 Digital-03F598

Web-Meldezentrale mit digitalen IOs und Datenlogger

Last update: Wed 10.09.08, 11:32:51

No active alarm

Alarm		Trigger	Last action
A1: Testalarm	SW-Ack	OFF	Device switched on 01.01.70, 01:59:51

Homepage in its initial state

At the top left of the screen you will find links used to display the information menu and for navigating to the other two main pages. 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 Web-IO. If the time is followed by an asterisk, the system clock of the Web-IO 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 alarm active* 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 information 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.

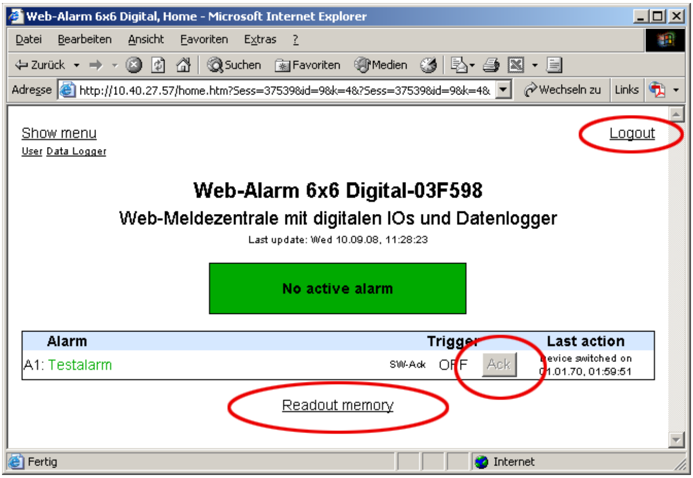
- Alarm identifier (A1 - A12)
- Symbolic name which can be assigned from the configuration menu
- Information as to whether the artificial trigger has been set from the test page (red flashing)
- Acknowledgement options (software or hardware Ack)
- Status of the trigger condition
- In logged-in state and if software acknowledgement has been configured, a button for alarm acknowledgement
- The last event pertaining to the alarm including time (e.g. trigger, SW or HW acknowledgement or releasing)

When no one is logged in, the page is used only for monitoring purposes. Neither access to the acknowledgement buttons nor to the contents of the data logger 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.
- Below the alarm overview table a link is displayed which opens the dialog for reading the data logger.

- The control elements for the login procedure on the upper edge of the screen are replaced by a link for logging out.


Web-Alarm 6x6 Digital, Home - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
Wechseln zu
Links
Fertig
Internet

Adresse: http://10.40.27.57/home.htm?Sess=37539&id=9&k=4&?Sess=37539&id=9&k=4&

Show menu
User Data Logger

Logout

Web-Alarm 6x6 Digital-03F598

Web-Meldezentrale mit digitalen IOs und Datenlogger

Last update: Wed 10.09.08, 11:28:23

No active alarm

Alarm	Trigger			Last action
A1: Testalarm	SW-Ack	OFF	Ack	device switched on 01.01.70, 01:59:51

Readout memory

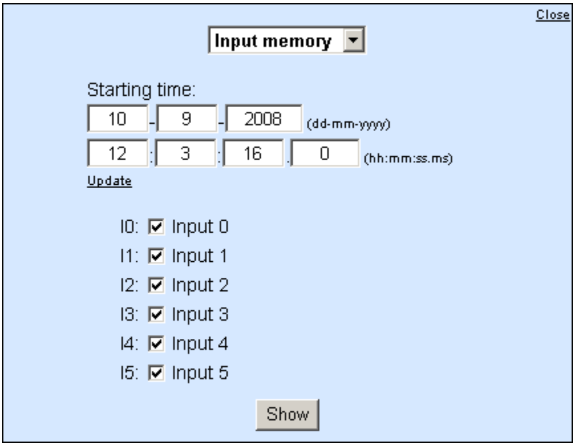
Homepage when logged in (changes are circled)

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.*

The link *Read memory* opens the dialog box for reading out the data logger. This dialog box allows you to show information about the alarm events (alarm trigger, trigger release and acknowledgement) and the input events (signal trace and counter states) in table form.



Close

Input memory ▾

Starting time:

10 - 9 - 2008 (dd-mm-yyyy)

12 : 3 : 16 . 0 (hh:mm:ss.ms)

Update

I0: ☑ Input 0

I1: ☑ Input 1

I2: ☑ Input 2

I3: ☑ Input 3

I4: ☑ Input 4

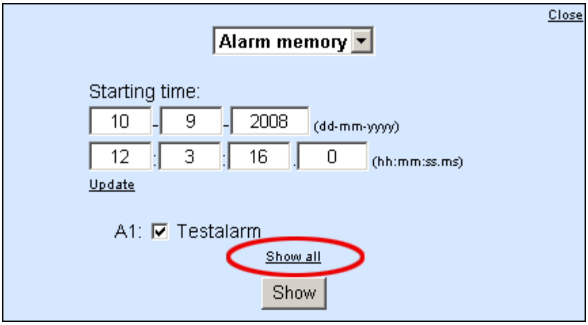
I5: ☑ Input 5

Show

Dialog box for reading out the data logger

To close the dialog, click on the link *Close* at the upper right corner of the box.

If you want to read out the alarm memory, first only the activated alarms are offered. You can also show all the available alarms using the link below the alarm list. When reading out the input memory access to all the inputs is given to you directly.



Close

Alarm memory ▾

Starting time:

10 - 9 - 2008 (dd-mm-yyyy)

12 : 3 : 16 . 0 (hh:mm:ss.ms)

Update

A1: ☑ Testalarm

Show all

Show

Link for showing all alarms in the readout dialog box

Readout is done in four steps:

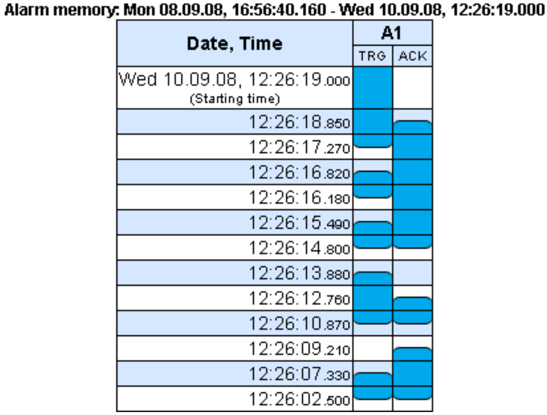
- Use the pull-down box to select the memory type you want to read (alarm or input memory).

- Enter the time at which you want to jump to the memory. You are given the 30 previous status changes starting from this point going from most recent to oldest.
- Check the boxes corresponding to the alarms or inputs you want to read out.
- Clicking on the *Show* button requests the data from the Web-Alarm and then displays them.

The returned table is overwritten with the memory type and limits of the time period used.

The time axis for the table runs vertically, with the most recent events at the top. For better clarity a complete time indication, including date information, is only displayed when the day changes. The time at which the jump to the memory is made is indicated by the comment *Jump time*. If there is no appropriate memory entry at the jump time, a line for this time is still inserted in the table.

The trigger condition (TRG) and acknowledgement history (ACK) is shown for each requested alarm for the alarm memory. Activated phases are highlighted in the table in blue.

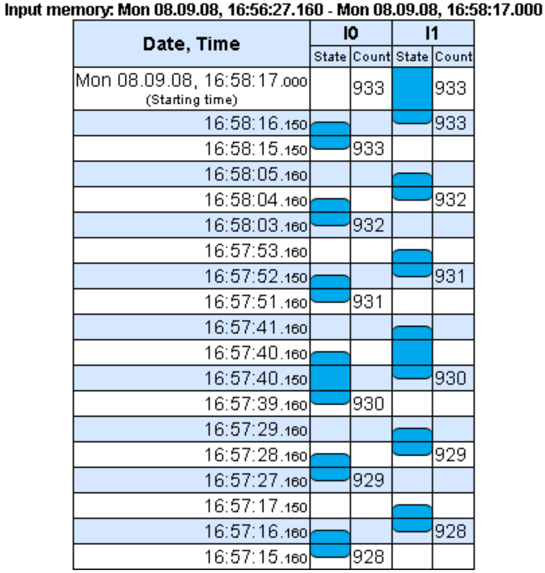


Alarm memory: Mon 08.09.08, 16:56:40.160 - Wed 10.09.08, 12:26:19.000

Date, Time	A1	
	TRG	ACK
Wed 10.09.08, 12:26:19.000 (Starting time)	■	
12:26:18.850	■	■
12:26:17.270	■	■
12:26:16.820	■	■
12:26:16.180	■	■
12:26:15.490	■	■
12:26:14.800	■	■
12:26:13.880	■	
12:26:12.760	■	■
12:26:10.870	■	■
12:26:09.210		■
12:26:07.330	■	■
12:26:02.500	■	■

Excerpt from the alarm memory

When the input memory is read out, in addition to the signal history for each input the counter value is also shown. This is shown next to the edge for each change. Here again the activated phases of the inputs are shown in blue.

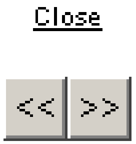


Input memory: Mon 08.09.08, 16:56:27.160 - Mon 08.09.08, 16:58:17.000

Date, Time	I0		I1	
	State	Count	State	Count
Mon 08.09.08, 16:58:17.000 (Starting time)		933	■	933
16:58:16.150	■		■	933
16:58:15.150	■	933		
16:58:05.160			■	
16:58:04.160	■		■	932
16:58:03.160	■	932		
16:57:53.160			■	
16:57:52.150	■		■	931
16:57:51.160	■	931		
16:57:41.160			■	
16:57:40.160	■		■	
16:57:40.150	■		■	930
16:57:39.160	■	930		
16:57:29.160			■	
16:57:28.160	■		■	929
16:57:27.160	■	929		
16:57:17.150			■	
16:57:16.160	■		■	928
16:57:15.160	■	928		

Excerpt from the input memory

Once a memory type has been read out and displayed, you can use the arrow key buttons below the table can be used to skip forward and backward in the table.



Control elements below the tabular representation of the memory contents

To hide the table, click on the *Close* link below the display.

3.3 User page

The user page provides an overview of the state of the

- Inputs
- Outputs
- Counters
- Activated alarms
- Data logger utilization

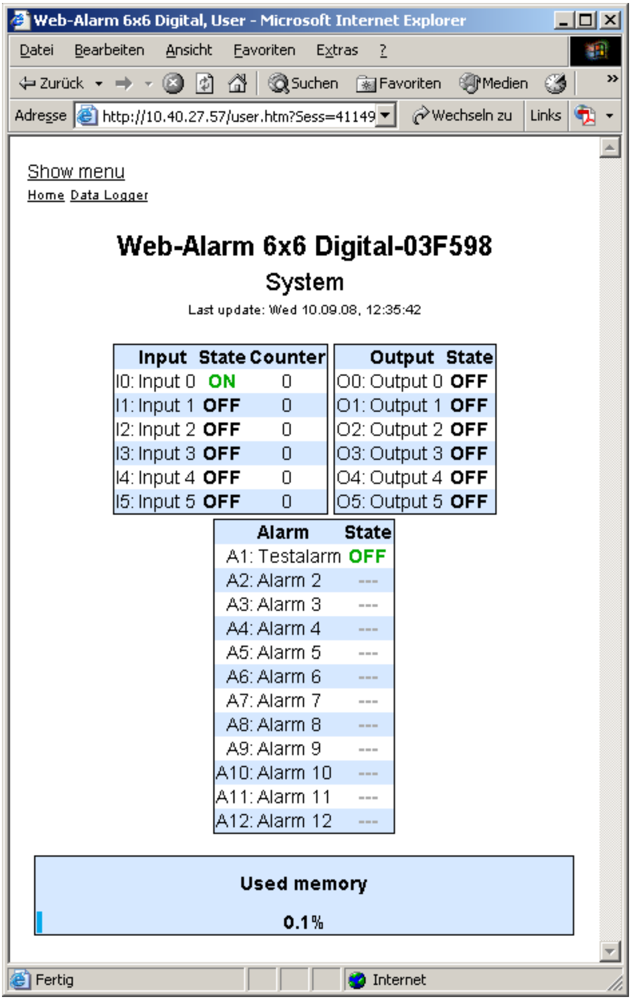
The page can be opened by clicking on links or by entering the following address:

```
http://<IP address of the Web-Alarm>/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 Web-Alarm.

The links in the upper left corner allow you to show the configuration menu and navigate directly to the pages *home.htm* and *logger.htm*.

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.


Web-Alarm 6x6 Digital, User - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://10.40.27.57/user.htm?Sess=41149
Wechseln zu Links
Fertig
Internet

Show menu
Home Data Logger

Web-Alarm 6x6 Digital-03F598

System

Last update: Wed 10.09.08, 12:35:42

Input	State	Counter
I0: Input 0	ON	0
I1: Input 1	OFF	0
I2: Input 2	OFF	0
I3: Input 3	OFF	0
I4: Input 4	OFF	0
I5: Input 5	OFF	0

Output	State
O0: Output 0	OFF
O1: Output 1	OFF
O2: Output 2	OFF
O3: Output 3	OFF
O4: Output 4	OFF
O5: Output 5	OFF

Alarm	State
A1: Testalarm	OFF
A2: Alarm 2	---
A3: Alarm 3	---
A4: Alarm 4	---
A5: Alarm 5	---
A6: Alarm 6	---
A7: Alarm 7	---
A8: Alarm 8	---
A9: Alarm 9	---
A10: Alarm 10	---
A11: Alarm 11	---
A12: Alarm 12	---

Used memory

0.1%

User page with self-refreshing system overview of the Web-Alarm

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

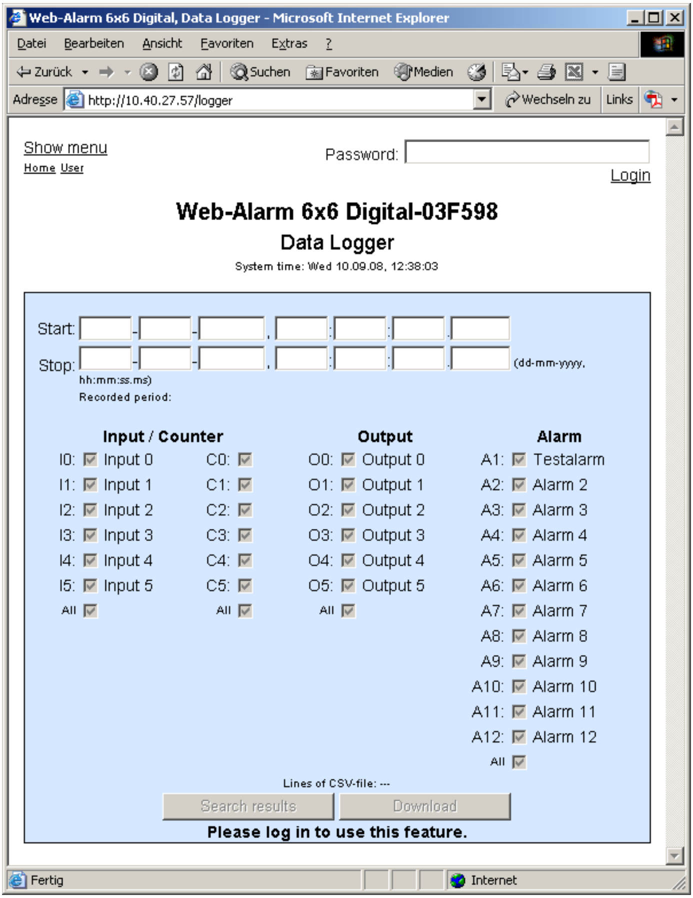
If the configuration menu was used to set an artificial trigger for an alarm to generate the messages for the alarm, the word *Test* flashes in the alarm overview. If an alarm is in this state, the set trigger must be first rescinded from the configuration page before the device can again trigger alarms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

3.4 Data logger page

By opening the data logger page at:

```
http://<IP address of the Web-Alarm>/logger.htm
```

you can export the contents of the data logger to a CSV file. This file can be used to archive or further process the data, for example using a suitable table processing program. The input screen allows the data export to focus only on individual time periods and events.


Web-Alarm 6x6 Digital, Data Logger - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://10.40.27.57/logger
Wechseln zu Links
Show menu
Home User
Login
Search results
Download
Fertig
Internet

Password:

Web-Alarm 6x6 Digital-03F598

Data Logger

System time: Wed 10.09.08, 12:38:03

Start: __ - __ - __ , __ : __ : __ . __

Stop: __ - __ - __ , __ : __ : __ . __ (dd-mm-yyyy, hh:mm:ss.ms)

Recorded period:

Input / Counter		Output	Alarm
I0: ☑ Input 0	C0: ☑	O0: ☑ Output 0	A1: ☑ Testalarm
I1: ☑ Input 1	C1: ☑	O1: ☑ Output 1	A2: ☑ Alarm 2
I2: ☑ Input 2	C2: ☑	O2: ☑ Output 2	A3: ☑ Alarm 3
I3: ☑ Input 3	C3: ☑	O3: ☑ Output 3	A4: ☑ Alarm 4
I4: ☑ Input 4	C4: ☑	O4: ☑ Output 4	A5: ☑ Alarm 5
I5: ☑ Input 5	C5: ☑	O5: ☑ Output 5	A6: ☑ Alarm 6
All ☑	All ☑	All ☑	A7: ☑ Alarm 7
			A8: ☑ Alarm 8
			A9: ☑ Alarm 9
			A10: ☑ Alarm 10
			A11: ☑ Alarm 11
			A12: ☑ Alarm 12
			All ☑

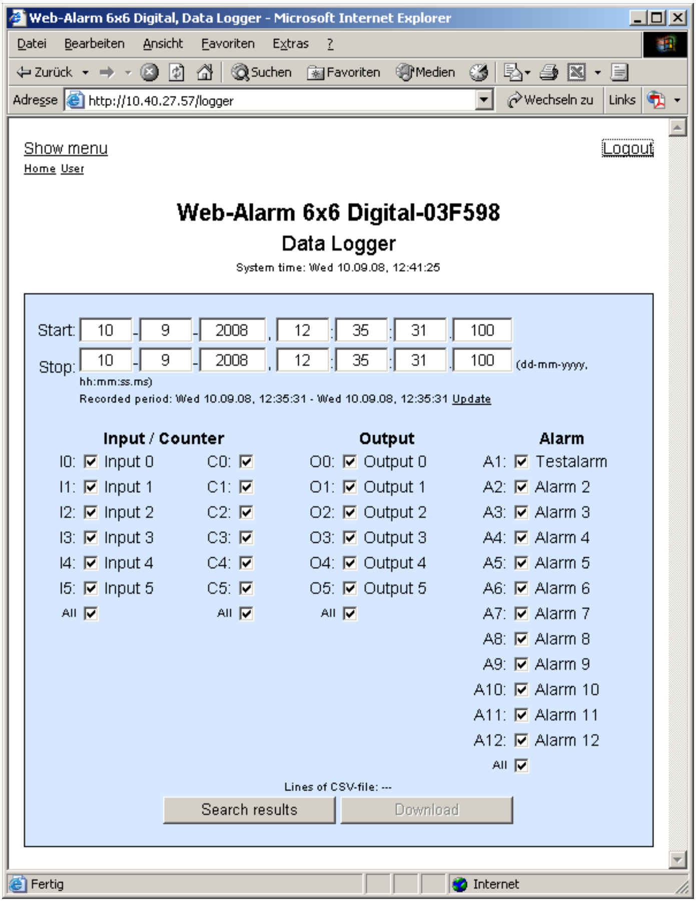
Lines of CSV-file: ---

Please log in to use this feature.

Data logger page with user logged out

Exporting data requires operator or administrator rights. If you are not logged in with the appropriate rights, all the control elements are greyed out.

When you log in, the greyed out buttons are enabled. In addition, the time points for the first and last memory event are read out and entered in the input screen. This information tells you about the time period in which the data logger was started up. This time is also indicated below the text fields for the start and stop time.


Web-Alarm 6x6 Digital, Data Logger - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://10.40.27.57/logger
Wechseln zu Links
Show menu
Logout
Home User
Fertig
Internet

Web-Alarm 6x6 Digital-03F598

Data Logger

System time: Wed 10.09.08, 12:41:25

Start: 10 - 9 - 2008 , 12 : 35 : 31 . 100

Stop: 10 - 9 - 2008 , 12 : 35 : 31 . 100 (dd-mm-yyyy, hh:mm:ss.ms)

Recorded period: Wed 10.09.08, 12:35:31 - Wed 10.09.08, 12:35:31 Update

Input / Counter		Output	Alarm
I0: ☑ Input 0	C0: ☑	O0: ☑ Output 0	A1: ☑ Testalarm
I1: ☑ Input 1	C1: ☑	O1: ☑ Output 1	A2: ☑ Alarm 2
I2: ☑ Input 2	C2: ☑	O2: ☑ Output 2	A3: ☑ Alarm 3
I3: ☑ Input 3	C3: ☑	O3: ☑ Output 3	A4: ☑ Alarm 4
I4: ☑ Input 4	C4: ☑	O4: ☑ Output 4	A5: ☑ Alarm 5
I5: ☑ Input 5	C5: ☑	O5: ☑ Output 5	A6: ☑ Alarm 6
All ☑	All ☑	All ☑	A7: ☑ Alarm 7
			A8: ☑ Alarm 8
			A9: ☑ Alarm 9
			A10: ☑ Alarm 10
			A11: ☑ Alarm 11
			A12: ☑ Alarm 12
			All ☑

Lines of CSV-file: ---

Data logger page following a search

The logger contents are exported in two steps. First a valid time period must be specified. This can either concentrate on a section of the data logger or include the entire recording time as is entered automatically after a login. In addition, you can use the check boxes to refine the trigger screens if you are not interested in all the event sources. Clicking on the *Find results* button starts the search, which searches the specified time period for events from the selected sources. The number of hits is shown in the input screen in parentheses behind the source name.

The progress of the search is indicated by a status bar at the bottom edge of the input screen. Clicking on the *Cancel search* button cyclically updates the line number of the loadable CSV file.

Once the search has been completed, you can refine your search criteria based on the found results or load a CSV file with the hits into your computer.

⚠ *If the loaded CSV file is going to be opened for analysis purposes for example using Microsoft Excel, note that some versions of the table processor can only open documents having a maximum of 65536 lines.*

A loaded CSV file contains a column each for:

- Date
- Time of day (without milliseconds)
- Milliseconds
- Each input, counter, output, alarm

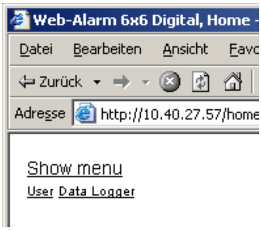
The search can be stopped at any time by clicking on the *Cancel search* button. The user interface then returns to the initial screen and is ready for new entries.

3.5 Hiding and showing the configuration menu

If the configuration menu is not visible, the pages

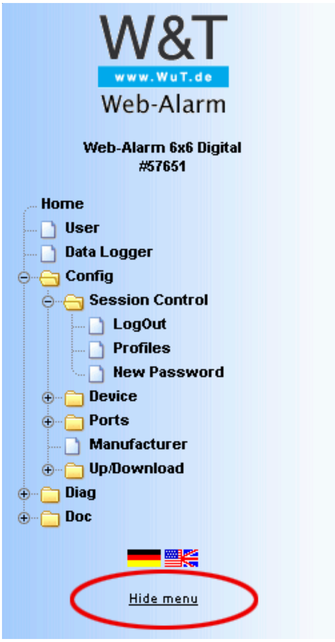
- Home (*home.htm*)
- User (*user.htm*)
- Data Logger (*logger.htm*)

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


Web-Alarm 6x6 Digital, Home -
Datei Bearbeiten Ansicht Favo
Zurück
Adresse http://10.40.27.57/home
Show menu
User Data Logger

Link for showing the configuration menu on the homepage

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



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 three main pages (*home.htm, user.htm, logger.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.

3.6 Login and Logout

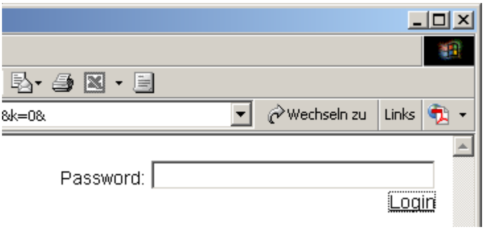
Depending on the login, the Web-Alarm distinguishes between three different access levels:

- *Default User*: Every user who accesses the device without a password has this status initially. The status of the Web-Alarm can now be read out and displayed. Acknowledging alarms, reading the data logger or changing the configuration is however not possible.
- *Administrator*: The administrator password provides full access to the device. Changing the configuration, acknowledging alarms and reading the data logger is now possible.
- *Operator*: Operator access rights are limited to acknowledging alarms, changing the alarm outputs, reading the data logger 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* and *logger.htm* pages or using the sub-item *Config* from the menu tree. The dialog box on the main pages is then only visible if the menu tree is hidden.

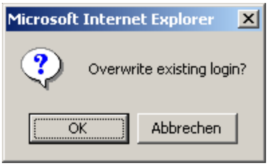


Password:

Login dialog on one of the three main pages

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

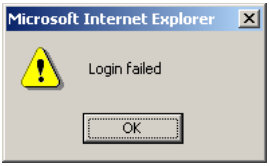
A login with administrator rights can overwrite an already existing login. In this case the user is prompted during the login to accept the existing login.



Overwrite existing login?

Prompt on a main page 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.



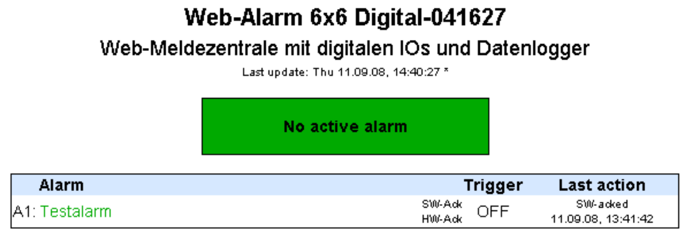
Login failed

Message for rejected login on a main page

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

3.7 Preconfigured example alarm

An example alarm is already preconfigured in the device as shipped from the factory. This is intended to demonstrate the functions and capabilities of the device right after startup.



Web-Alarm 6x6 Digital-041627

Web-Meldezentrale mit digitalen IOs und Datenlogger

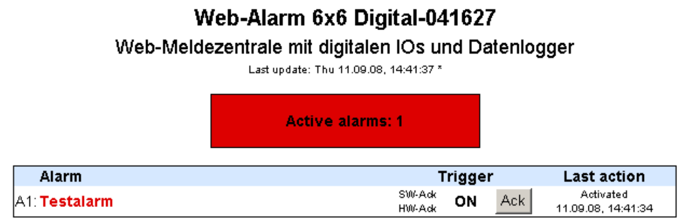
Last update: Thu 11.09.08, 14:40:27 *

No active alarm

Alarm		Trigger	Last action
A1: Testalarm	SW-Ack HW-Ack	OFF	SW-acked 11.09.08, 13:41:42

Inactive example alarm

The alarm is configured such that wiring Input 0 triggers a clearable (Ack) alarm. Switching Output 0 is set as a message type for this alarm. The acknowledgement can be done per button on the page *home.htm*. The output is cleared only after an acknowledgement has been performed, regardless of whether the alarm condition still exists or has already been cleared.



Web-Alarm 6x6 Digital-041627

Web-Meldezentrale mit digitalen IOs und Datenlogger

Last update: Thu 11.09.08, 14:41:37 *

Active alarms: 1

Alarm		Trigger		Last action
A1: Testalarm	SW-Ack HW-Ack	ON	Ack	Activated 11.09.08, 14:41:34

Triggered example alarm, user logged in

Note that administrator or operator rights are required to carry out software ACKs.

A fall and subsequent rise of the alarm condition does not change the alarm status if there has been no acknowledgement.

4 Alarms

The Web-Alarm allows up to 12 different alarms to be used which are tripped based on input states and/or counter states. 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 Web-Alarm 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.

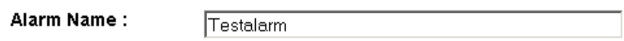
⚠ *If delays occur when sending messages, for example due to wait times in opening the connection, these delays also affect the as yet unsent messages.*

4.1 Configuring alarms

You can use the configuration menu to set parameters for the available alarms 1 - 12. To do this, open the configuration page

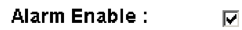
```
Config >> Device >> Alarm >> Alarm X
```

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



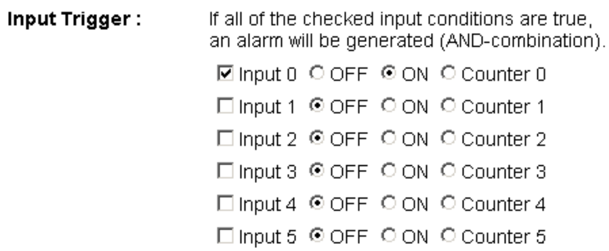
Alarm Name : Testalarm

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.



Alarm Enable : ☑

In the *Input Trigger* configure the conditions which must be met for the alarm to be triggered. Here you can activate the involved inputs and define the status which must exist at the moment of triggering. An input can be OFF or ON or the counter associated with the input can show a particular counter state.

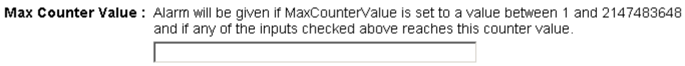


Input Trigger : If all of the checked input conditions are true, an alarm will be generated (AND-combination).

☑ Input 0 ○ OFF ● ON ○ Counter 0
□ Input 1 ● OFF ○ ON ○ Counter 1
□ Input 2 ● OFF ○ ON ○ Counter 2
□ Input 3 ● OFF ○ ON ○ Counter 3
□ Input 4 ● OFF ○ ON ○ Counter 4
□ Input 5 ● OFF ○ ON ○ Counter 5

Note that when selecting multiple inputs as triggers the configured condition of all the inputs must be met in order to trigger an alarm. This represents an AND operation of the individual events.

If in the Input Trigger area you have specified a counter state as the trigger condition for one or more counters, you can enter this value in the *Max Counter Value* field.



Max Counter Value : Alarm will be given if MaxCounterValue is set to a value between 1 and 2147483648 and if any of the inputs checked above reaches this counter value.

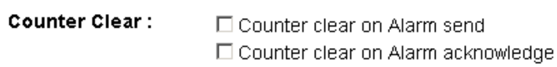
Even if multiple inputs have been set based on their counters, only one counter state can be specified as the trigger threshold.

To enable cyclical repeating of alarms whose trigger condition is based on counters, the counter states can be cleared for...

- ...Sending the alarm...
- ...Acknowledging the alarm

Otherwise the counter wsould be continuously incremented after triggering, which would cause the trigger condition to be never met.

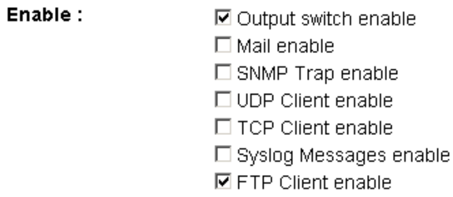
The parameter setting is made in *Counter Clear*.



Counter Clear :

□ Counter clear on Alarm send
□ Counter clear on Alarm acknowledge

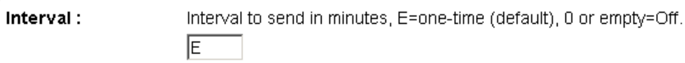
The *Enable* block contains all the message types. Here you select the communication path for reporting the alarm.



Enable :

☑ Output switch enable
□ Mail enable
□ SNMP Trap enable
□ UDP Client enable
□ TCP Client enable
□ Syslog Messages enable
☑ FTP Client enable

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.

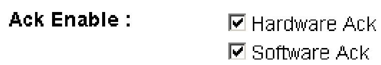


Interval : Interval to send in minutes, E=one-time (default), 0 or empty=Off.

E

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.

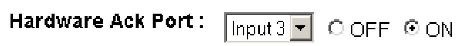
A possible acknowledgement can be set in the *Ack Enable* block. A hardware and/or software acknowledgement may be selected.



Ack Enable :

☑ Hardware Ack
☑ Software Ack

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.



Hardware Ack Port : Input 3 ○ OFF ● ON

Apply the changes by clicking on *Save*.

4.2 Formulating message texts

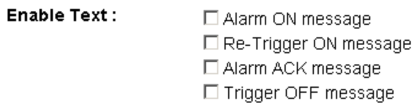
For the messaging types reporting over the network, three messages each can be formulated which are sent by the device depending on the alarm status:

- 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.



Enable Text :

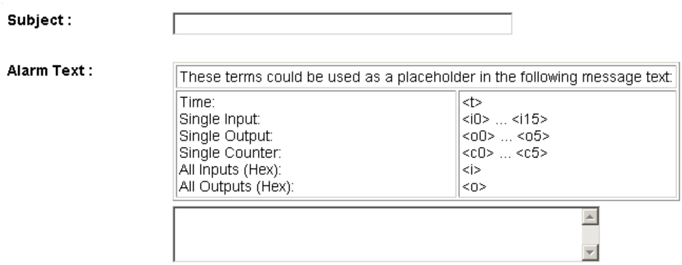
□ Alarm ON message
□ Re-Trigger ON message
□ Alarm ACK message
□ Trigger OFF message

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 :

Alarm Text :

These terms could be used as a placeholder in the following message text:

Time:	<t>
Single Input:	<i0> ... <i15>
Single Output:	<o0> ... <o5>
Single Counter:	<c0> ... <c5>
All Inputs (Hex):	<i>
All Outputs (Hex):	<o>

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.

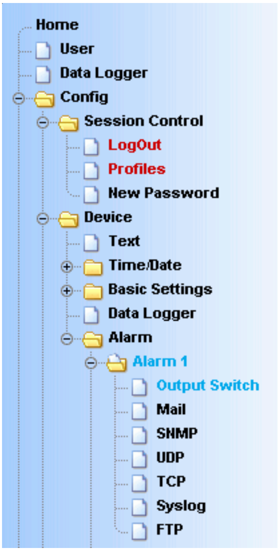
Alarm Variable	Beschreibung
<dn>	Device Name (Config >> Device >> Text)
<i>	Input state, hex
<i**x**>	State of input no. **x** (ON / OFF)
<in**x**>	Name of input no. **x**
<o>	State of outputs, hex
<on**x**>	Name of output No. **x**
<c**x**>	Counter value of counter no. X
<t>	Time of event (TT.MMM.YYYY hh:mm:ss)
<$y>	Yeay (YYYY)
<$m>	Month (MM)
<$d>	Day (DD)
<$h>	Hour (hh)
<$i>	Minute (mm)
<$s>	Second (ss)
x is value from 0 to 5	

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

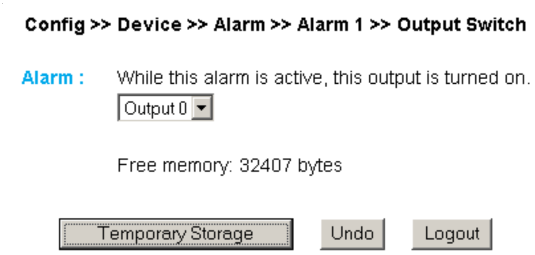
To switch a digital output when there is an alarm, open the profile *Local Alarming*.



„Local Alarming“ 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.


Config >> Device >> Alarm >> Alarm 1 >> Output Switch

Alarm : While this alarm is active, this output is turned on.
Output 0

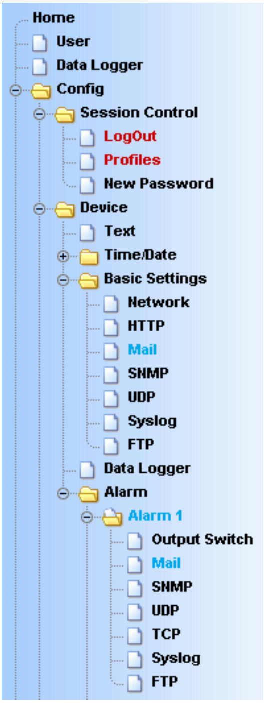
Free memory: 32407 bytes

Definition of the switching output

Apply the changes by clicking on *Save*.

4.4 Alarming per e-mail

Open the profile *Alarming per e-mail* .



„Alarming per e-mail“ profile

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

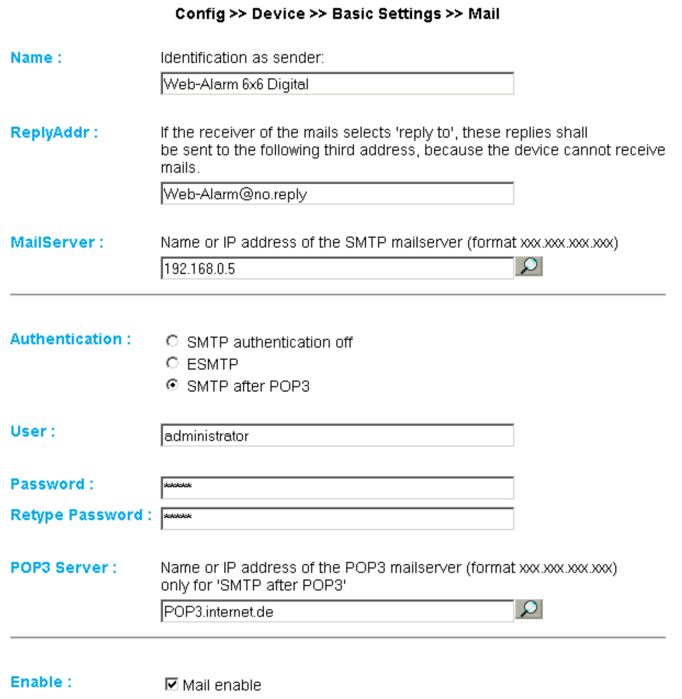
4.4.1 General settings

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.



Config >> Device >> Basic Settings >> Mail

Name : Identification as sender:
Web-Alarm 6x6 Digital

ReplyAddr : If the receiver of the mails selects 'reply to', these replies shall be sent to the following third address, because the device cannot receive mails.
Web-Alarm@no.reply

MailServer : Name or IP address of the SMTP mailserver (format xxx.xxx.xxx.xxx)
192.168.0.5

Authentication :
○ SMTP authentication off
○ ESMTP
● SMTP after POP3

User : administrator

Password : *****

Retype Password : *****

POP3 Server : Name or IP address of the POP3 mailserver (format xxx.xxx.xxx.xxx) only for 'SMTP after POP3'
POP3.internet.de

Enable : ☑ Mail enable

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 *Save*.

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

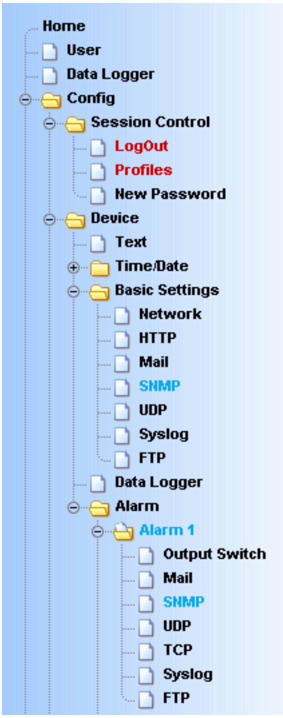
```
Config >> Device >> Alarm >> Alarm X >> Mail
```

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.alarming per trap*.



„Alarming per 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 *Save*.

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

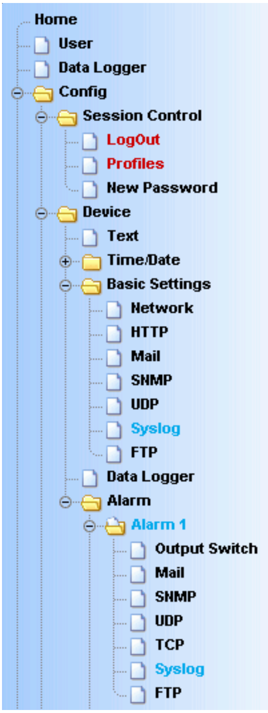
```
Config >> Device >> Alarm >> Alarm X >> SNMP
```

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. alarming*.



Profile „Syslog Messages incl. alarming"

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 Web-Alarm 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.

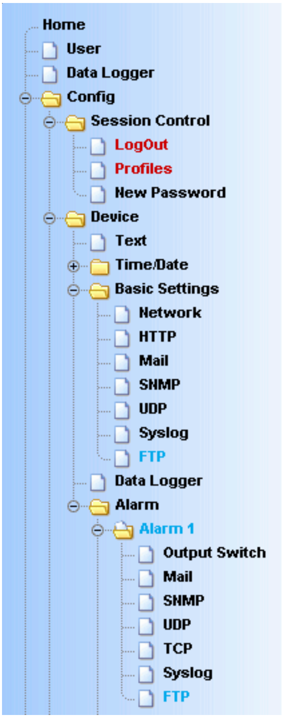
Finally, configure the require message texts as described in the section *Formulating message texts* and save the changes by clicking on *Save*.

4.7 Alarming per FTP

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

Open the profile *Alarming per FTP (Client Mode)*.

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



„Alarming per FTP“ profile

4.7.1 General settings

On the page

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

specify the basic parameters for message sending per FTP.

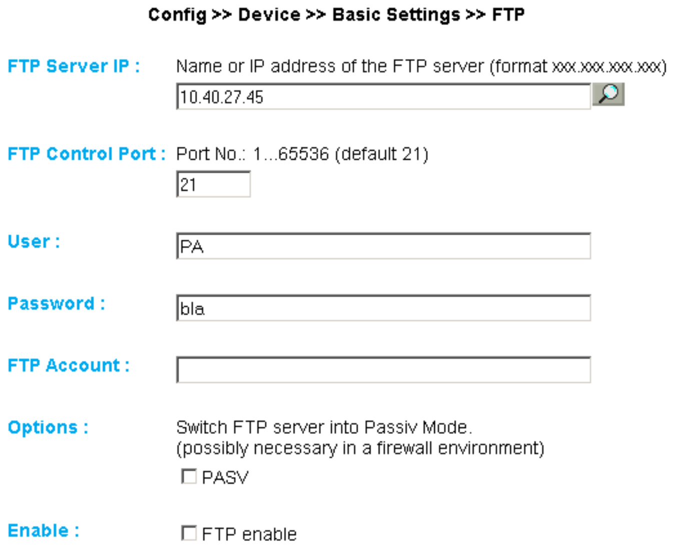
For *FTP Server IP* enter the IP address or host name (only for configured DNS servers) of your FTP server you want to receive the data.

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 Web-Alarm. 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.



Config >> Device >> Basic Settings >> FTP

FTP Server IP : Name or IP address of the FTP server (format xxx.xxx.xxx.xxx)
10.40.27.45

FTP Control Port : Port No.: 1...65536 (default 21)
21

User : PA

Password : bla

FTP Account :

Options : Switch FTP server into Passiv Mode.
(possibly necessary in a firewall environment)
□ PASV

Enable : □ FTP enable

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 Web-Alarm. 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.

Options : ○ STORE
● APPEND

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 Data Logger

The device features an internal data logger which records status changes in the

- Alarms
- Alarm acknowledgements
- Digital inputs
- Counters
- Digital outputs

in addition to all alarm outputs, visualizations and user entries. The logging routine runs at a frequency of 100 Hz, which enables writing of 100 logger entries per second. One entry may contain status changes from multiple event sources.

There are two types of entries which are stored in the data logger: *Alarm* and *IO Events*. The occurrence of an alarm involves significantly more information, including a complete map of the IO states, than a simple IO event. This also means that alarm events are considerably more memory-intensive. Taking this fact into account, the data logger can store a maximum of 130,000 alarm events or 1,000,000 of the less memory-intensive IO events. Depending on how the device is used, various mixes of these two entry types are possible.

The data logger memory consists of an 8MB flash memory which works as a ring memory. Once the memory is completely filled, the oldest data are replaced (overwritten) by the new events.

The logger entries are stored non-volatile, so that the data are retained even after a loss of power.

The data logger is ready immediately after the device is supplied with power. It records the usual events even when there is no active network connection.

5.1 Clearing the memory

If the memory is cleared using the option *Clear data memory* on the

`Config >> Device >> Data Logger`

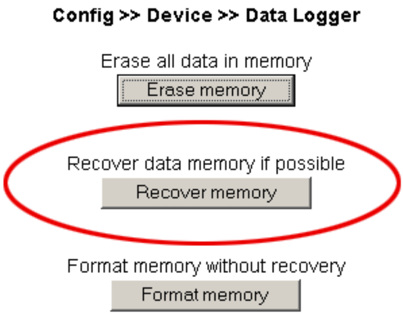
page, this is done by clearing the table of contents of the data logger. The actual, physical data contents is not deleted..

5.2 Restoring data

If you have cleared the data logger using the option *Clear data memory*, it is still possible to reconstruct contents which have not in the meantime been overwritten with new events.

If it is possible to reconstruct a memory, the *Restore data memory* button will be shown on the page

`Config >> Device >> Data Logger`



Config >> Device >> Data Logger

Erase all data in memory

Recover data memory if possible

Format memory without recovery

Option for reconstructing the memory contents

The restoring process reconstructs the table of contents based on the not yet overwritten memory entries.

Note that only the contents can be restored which have not yet been overwritten with more recent events.

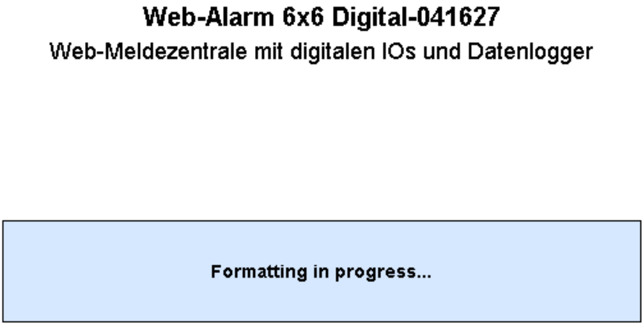
5.3 Formatting the memory

To perform a final, no longer restorable clearing of data you must format the memory. This can also be done on the

```
Config >> Device >> Data Logger
```

page using the option *Format memory*.

Clearing takes approximately 1 minute. The ongoing process is indicated by a message on the *home.htm*, *user.htm* and *logger.htm* pages. The data logger is disabled during formatting. Incoming alarms and IO events are not stored, and will be lost.



Web-Alarm 6x6 Digital-041627

Web-Meldezentrale mit digitalen IOs und Datenlogger

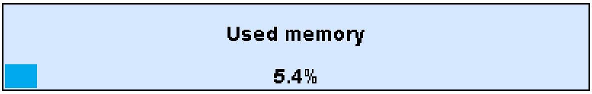
Formatting in progress...

Message for running memory formatting

The information logged in the data memory are permanently deleted by a formatting.

5.4 Memory utilization

The memory utilization of the data logger can be viewed on the *user.htm* page. The status bar shown there indicates the percent of memory capacity already used.



Used memory

5.4%

Graphical representation of the memory utilization

Like the rest of the page, the information about memory utilization is refreshed once a second.

⚠ *Even if the memory is already full and the oldest data are being overwritten with the new data, the ring structure means that the status bar never reaches the value 100%. This is because old data are always deleted in blocks and before the available memory space is consumed.*

6 Basic settings

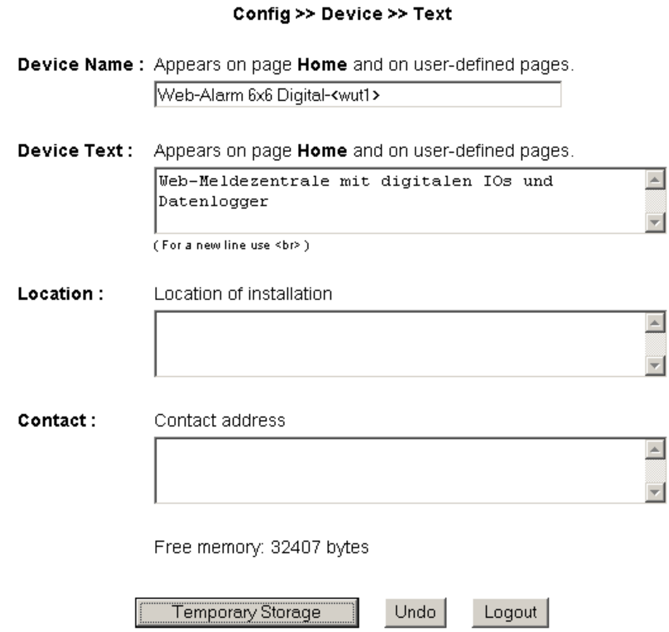
6.1 Device name

From the configuration menu open the page

```
Config >> Device >> Text
```

to edit the following texts:

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



Config >> Device >> Text

Device Name : Appears on page **Home** and on user-defined pages.
Web-Alarm 6x6 Digital-<wut1>

Device Text : Appears on page **Home** and on user-defined pages.
Web-Meldezentrale mit digitalen IOs und Datenlogger
(For a new line use
)

Location : Location of installation

Contact : Contact address

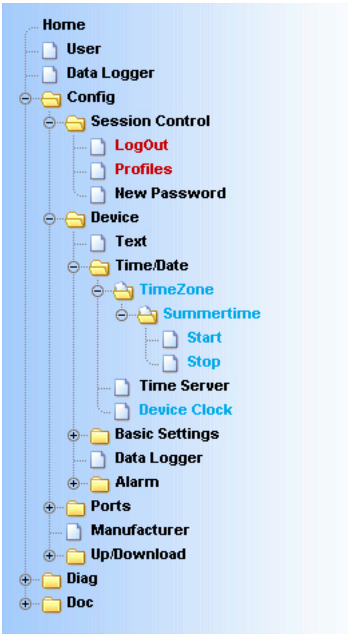
Free memory: 32407 bytes

Configuration page for device texts

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

6.2 Local time setting

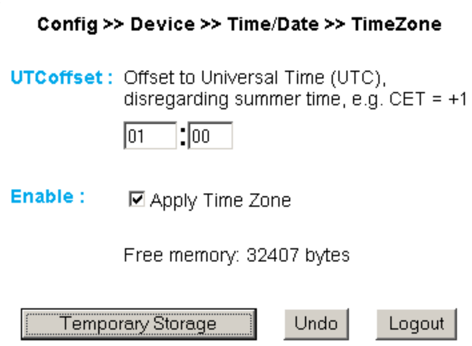
To manually set the system clock, the device provides a guided procedure using the profiles. To do this, open the profile *Local time setting*.



Configuration tree with selected profile for local time setting

6.2.1 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*.



Config >> Device >> Time/Date >> TimeZone

UTCoffset : Offset to Universal Time (UTC), disregarding summer time, e.g. CET = +1

01 : 00

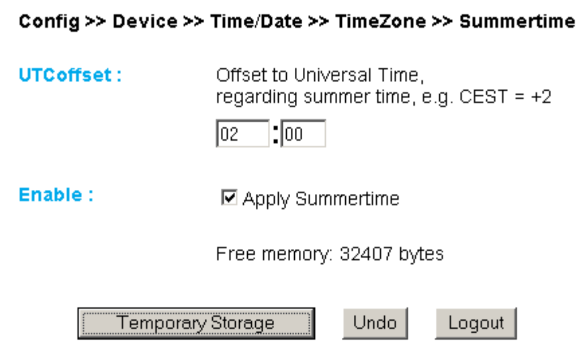
Enable : ☑ Apply Time Zone

Free memory: 32407 bytes

Time zone configuration

6.2.2 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.



Config >> Device >> Time/Date >> TimeZone >> Summertime

UTCoffset : Offset to Universal Time, regarding summer time, e.g. CEST = +2

02 : 00

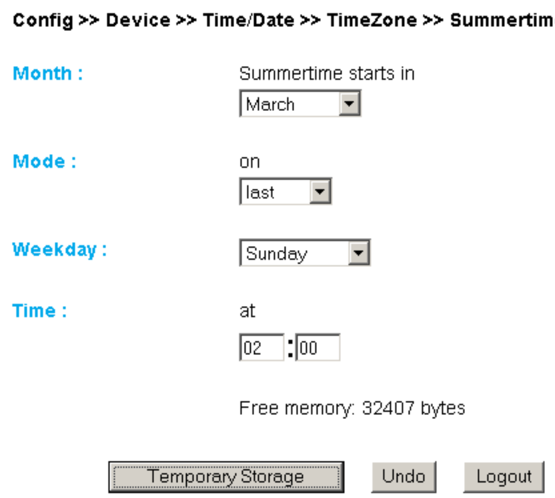
Enable : ☑ Apply Summertime

Free memory: 32407 bytes

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.



Config >> Device >> Time/Date >> TimeZone >> Summertime >> Start

Month : Summertime starts in March

Mode : on last

Weekday : Sunday

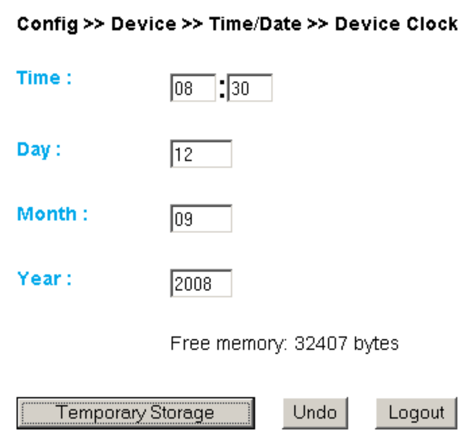
Time : at 02 : 00

Free memory: 32407 bytes

Rule for beginning daylight saving time

6.2.3 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.



Config >> Device >> Time/Date >> Device Clock

Time : 08 : 30

Day : 12

Month : 09

Year : 2008

Free memory: 32407 bytes

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.

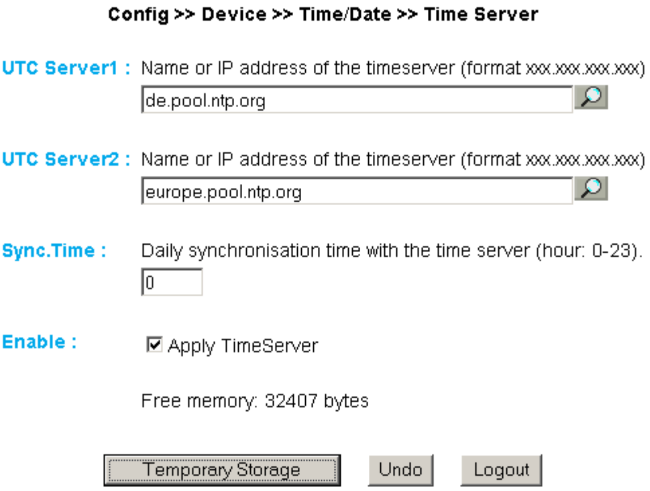
6.3 Automatic time setting using a network service

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 *Timezone*, *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*.



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

UTC Server1 : Name or IP address of the timeserver (format xxx.xxx.xxx.xxx)
de.pool.ntp.org

UTC Server2 : Name or IP address of the timeserver (format xxx.xxx.xxx.xxx)
europe.pool.ntp.org

Sync.Time : Daily synchronisation time with the time server (hour: 0-23).
0

Enable : ☑ Apply TimeServer

Free memory: 32407 bytes

Options for time servers

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

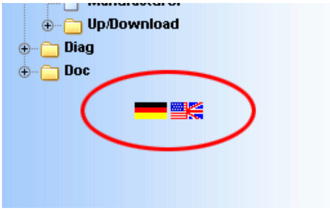
If you enter a name as the time server address, be sure that you have first configured both a gateway and a DNS server. Otherwise the address cannot be resolved. .

Click on *Logout* and save your settings.

6.4 Language

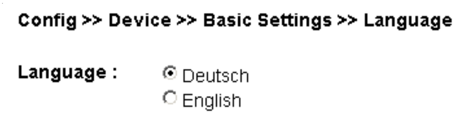
You can use the configuration menu to specify the system language. This can be done either using the flag link below the configuration menu, or navigate to:

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 *Save*.



Config >> Device >> Basic Settings >> Language

Language : ● Deutsch
○ English

Language selection

Changing the language requires operator or administrator rights.

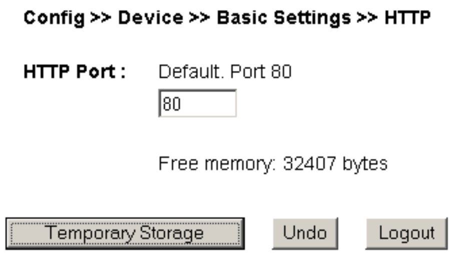
6.5 HTTP port

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 Web-Alarm>/home.htm:<portnumber>
```



Config >> Device >> Basic Settings >> HTTP

HTTP Port : Default. Port 80

80

Free memory: 32407 bytes

Configuring the port number

6.6 System traps per SNMP and SNMP basic configuration

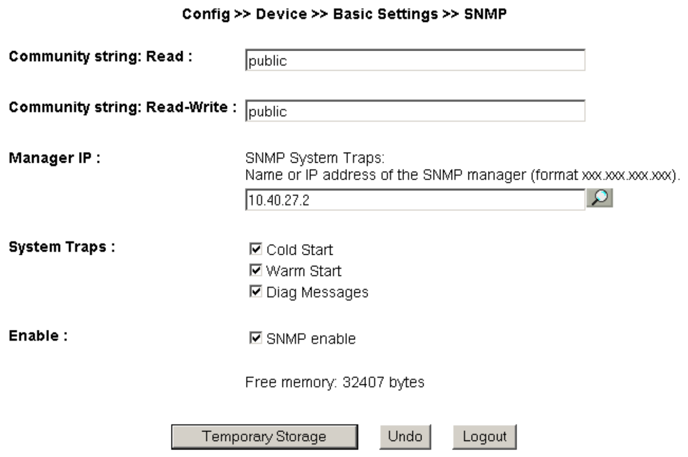
The following traps can be sent to an SNMP manager using SNMP protocol:

- 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



Config >> Device >> Basic Settings >> SNMP

Community string: Read : public

Community string: Read-Write : public

Manager IP : SNMP System Traps:
Name or IP address of the SNMP manager (format xxx.xxx.xxx.xxx).
10.40.27.2

System Traps :
☑ Cold Start
☑ Warm Start
☑ Diag Messages

Enable : ☑ SNMP enable

Free memory: 32407 bytes

SNMP configuration

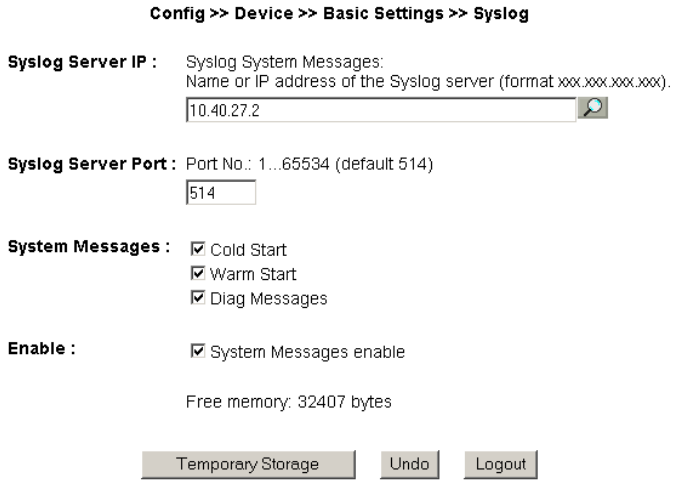
As opposed to the other messaging procedures, SNMP is activated by default.

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. Web-Alarm SNMP messages are sent to this address.
- System Traps: Select the messages you want to send.
- Enable: Enable the SNMP function

6.7 System Messages per syslog

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



Config >> Device >> Basic Settings >> Syslog

Syslog Server IP : Syslog System Messages:
Name or IP address of the Syslog server (format xxx.xxx.xxx.xxx).
10.40.27.2

Syslog Server Port : Port No.: 1...65534 (default 514)
514

System Messages : ☑ Cold Start
☑ Warm Start
☑ Diag Messages

Enable : ☑ System Messages enable

Free memory: 32407 bytes

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*.

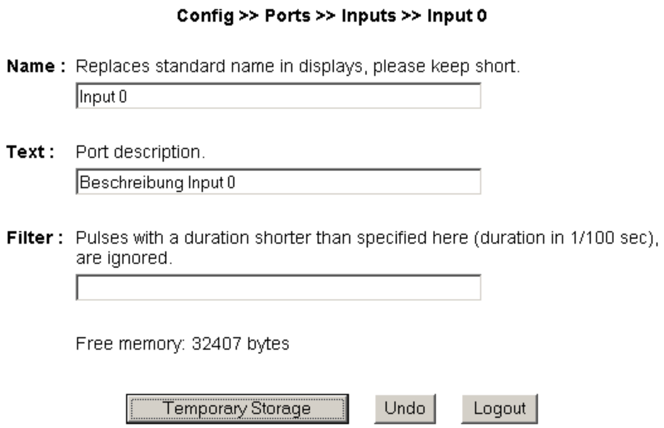
Save your settings by clicking on *Save*.

6.8 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
```



Config >> Ports >> Inputs >> Input 0

Name : Replaces standard name in displays, please keep short.
Input 0

Text : Port description.
Beschreibung Input 0

Filter : Pulses with a duration shorter than specified here (duration in 1/100 sec), are ignored.

Free memory: 32407 bytes

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 1/100 seconds. If no value is entered here, this function is disabled.

On the sub-page *Counter Mode:*

```
Config >> Ports >> Inputs >> Input X >> Counter Mode
```

you specify which edge of a pulse is used to increment the counter.

The second sub-page *Counter Set:*

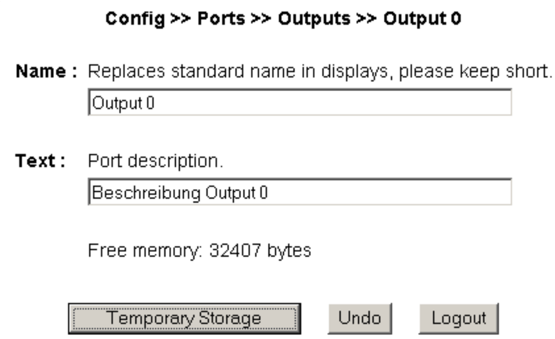
```
Config >> Ports >> Inputs >> Input X >> Counter Set
```

allows you to set the counter to a desired value.

6.9 Port settings - Outputs

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

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



Config >> Ports >> Outputs >> Output 0

Name : Replaces standard name in displays, please keep short.
Output 0

Text : Port description.
Beschreibung Output 0

Free memory: 32407 bytes

Settings„Output 0“

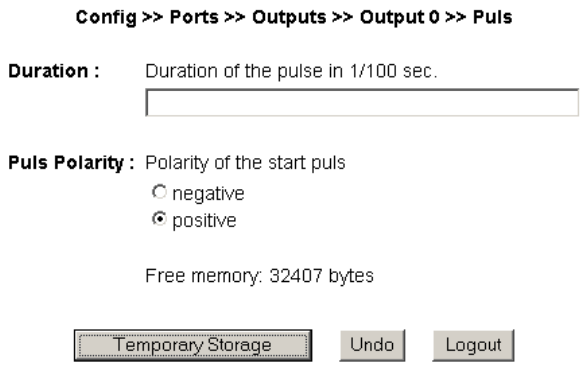
In this field you enter a name for the output. This name is then displayed in the browser for Output 0.

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 Web-Alarm 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 >> Pulse
```



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

Duration : Duration of the pulse in 1/100 sec.

Puls Polarity : Polarity of the start puls

○ negative
● positive

Free memory: 32407 bytes

Pulse configuration for outputs

For Duration enter the desired pulse length in 1/100‘s of seconds. A value of 100 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 Web-Alarm 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.

7 Troubleshooting and Testing

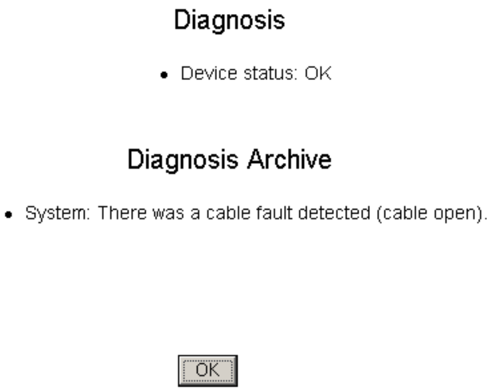
The Web-Alarm uses internal error management and diagnostics. This can be found in the configuration tree under the heading

```
Diag
```

7.1 Report

If an error occurs, this is indicated on the Web-Alarm itself by flashing of the *Diag* LED. In addition, any occurring errors are documented in a Diagnostic 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.



Diagnosis

- Device status: OK

Diagnosis Archive

- System: There was a cable fault detected (cable open).

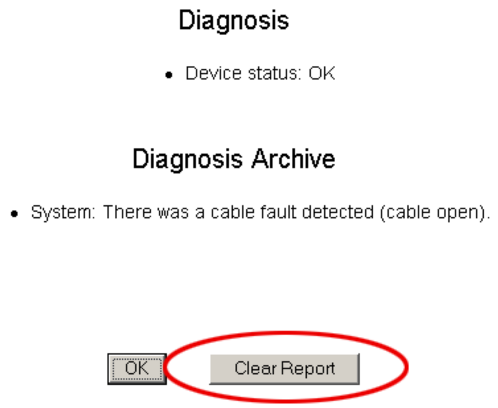
Diagnostic Report and Diagnostic Archive

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.



Diagnosis

- Device status: OK

Diagnosis Archive

- System: There was a cable fault detected (cable open).

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*.

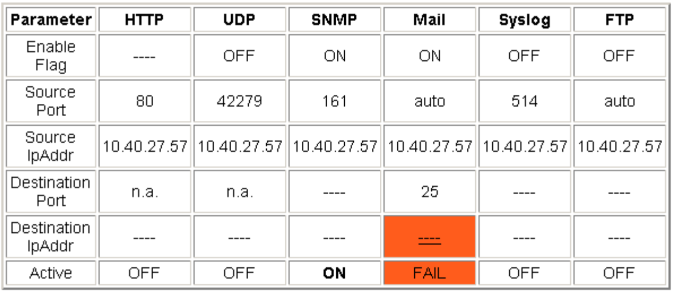
7.2 Check Config

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`

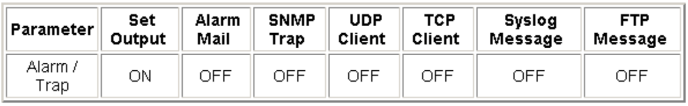
This Web page shows which access and message types are enabled with which parameters. The device performs a plausibility check of the settings. If missing parameters are detected which prevent proper operation of the access type, the corresponding fields are highlighted in orange. Clicking on the link 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

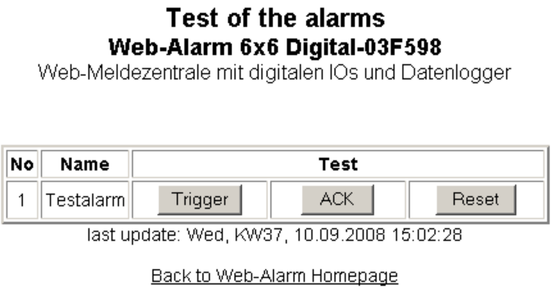
7.3 Check Alarm

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.



Test of the alarms

Web-Alarm 6x6 Digital-03F598

Web-Meldezentrale mit digitalen IOs und Datenlogger

No	Name	Test		
1	Testalarm	Trigger	ACK	Reset

last update: Wed, KW37, 10.09.2008 15:02:28

Back to Web-Alarm Homepage

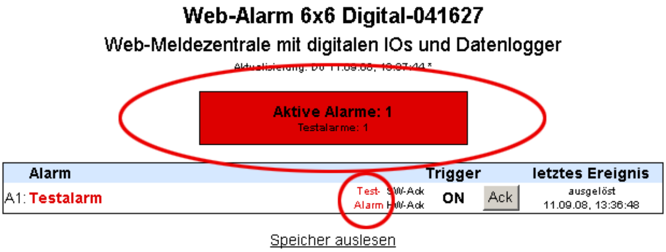
Test of the alarms-site

Clicking on the *Trigger* button tells the device that the triggering condition for the alarm has been met. The status of the inputs is irrelevant here, but the actual trigger condition should not in fact be met. This is to be considered a virtual alarm trigger.

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.



Web-Alarm 6x6 Digital-041627

Web-Meldezentrale mit digitalen IOs und Datenlogger

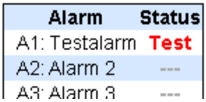
Aktualisierung: DO 11.09.08, 13:37:44 *

Aktive Alarme: 1
Testalarme: 1

Alarm		Trigger		letztes Ereignis
A1: **Testalarm**	Test-Alarm SW-Ack HW-Ack	ON	Ack	ausgelöst 11.09.08, 13:36:48

Speicher auslesen

„home.htm“ page with triggered test alarm



Alarm	Status
A1: Testalarm	**Test**
A2: Alarm 2	---
A3: Alarm 3	---

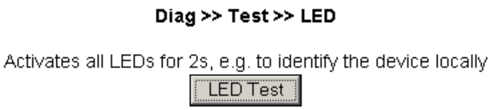
„user.htm“ page with triggered test alarm

7.4 LEDs

On the page

```
Diag >> Test >> LED
```

you can use the *LED Test* button to activate all the LEDs on the device for two seconds. This function simplifies identification of the device and helps to check the functionality of the LEDs.



Diag >> Test >> LED

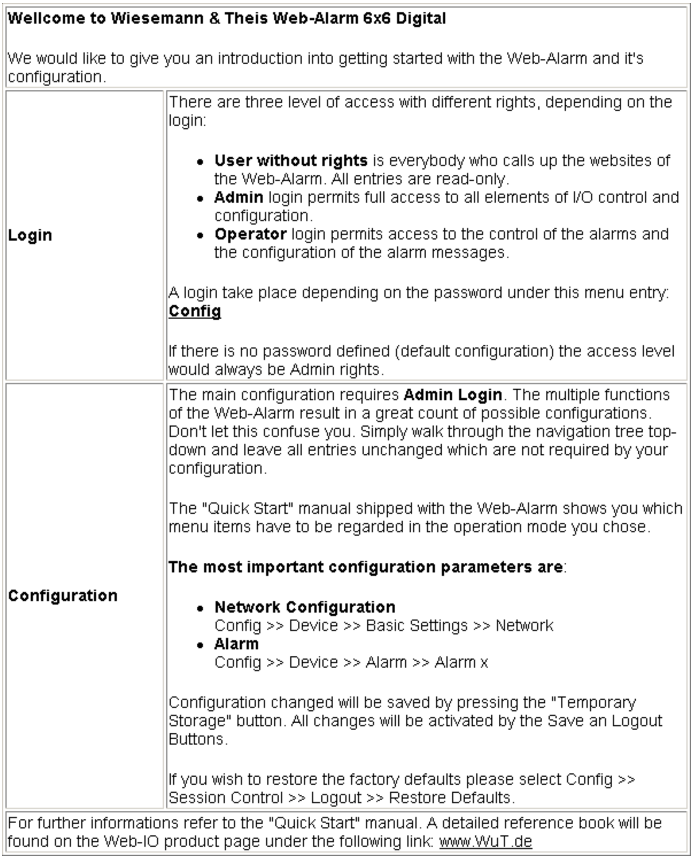
Activates all LEDs for 2s, e.g. to identify the device locally

Test page for the device LEDs

8 Documentation

8.1 Manual

Explanation of the login levels and important configurations.



Wellcome to Wiesemann & Theis Web-Alarm 6x6 Digital

We would like to give you an introduction into getting started with the Web-Alarm 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 Web-Alarm. All entries are read-only.
- **Admin** login permits full access to all elements of I/O control and configuration.
- **Operator** login permits access to the control of the alarms 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 Web-Alarm 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 Web-Alarm 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
- **Alarm**
  Config >> Device >> Alarm >> Alarm x

Configuration changed will be saved by pressing the "Temporary Storage" button. All changes will be activated by the Save an Logout Buttons.

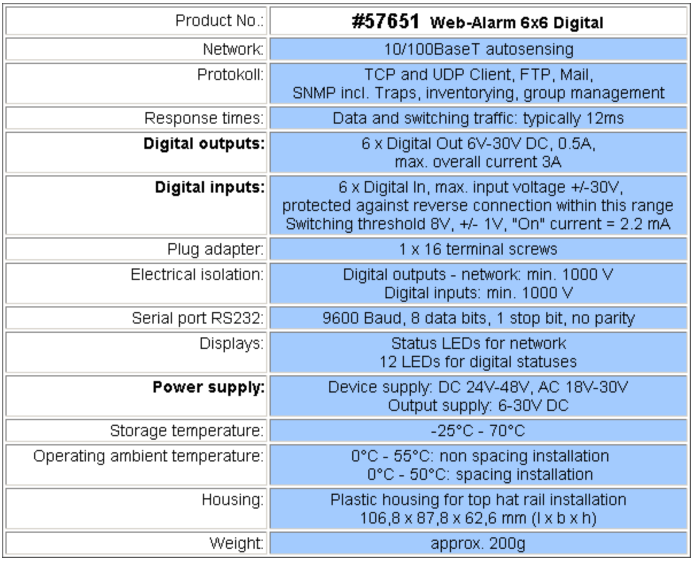
If you wish to restore the factory defaults please select Config >> Session Control >> Logout >> Restore Defaults.

For further informations refer to the "Quick Start" manual. A detailed reference book will be found on the Web-IO product page under the following link: www.WuT.de

Abbreviated „Manual“

8.2 Data sheet

The data sheet provides information about the key properties and technical data for the Web-Alarm.

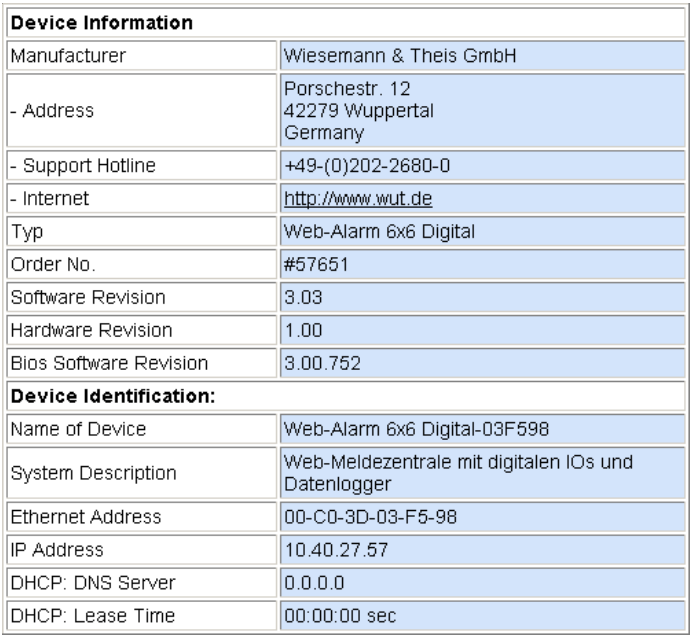


Product No.:	**#57651 Web-Alarm 6x6 Digital**
Network:	10/100BaseT autosensing
Protokoll:	TCP and UDP Client, FTP, Mail, SNMP incl. Traps, inventorying, group management
Response times:	Data and switching traffic: typically 12ms
Digital outputs:	6 x Digital Out 6V-30V DC, 0.5A, max. overall current 3A
Digital inputs:	6 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 16 terminal screws
Electrical isolation:	Digital outputs - network: min. 1000 V Digital inputs: min. 1000 V
Serial port RS232:	9600 Baud, 8 data bits, 1 stop bit, no parity
Displays:	Status LEDs for network 12 LEDs for digital statuses
Power supply:	Device supply: DC 24V-48V, AC 18V-30V Output supply: 6-30V DC
Storage temperature:	-25°C - 70°C
Operating ambient temperature:	0°C - 55°C: non spacing installation 0°C - 50°C: spacing installation
Housing:	Plastic housing for top hat rail installation 106,8 x 87,8 x 62,6 mm (l x b x h)
Weight:	approx. 200g

Web-Alarm data sheet

8.3 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	http://www.wut.de
Typ	Web-Alarm 6x6 Digital
Order No.	#57651
Software Revision	3.03
Hardware Revision	1.00
Bios Software Revision	3.00.752
Device Identification:	
Name of Device	Web-Alarm 6x6 Digital-03F598
System Description	Web-Meldezentrale mit digitalen IOs und Datenlogger
Ethernet Address	00-C0-3D-03-F5-98
IP Address	10.40.27.57
DHCP: DNS Server	0.0.0.0
DHCP: Lease Time	00:00:00 sec

„Property“ page

9 Appendix

9.1 LEDs

In the following the meaning and function of the LEDs on the front panel of the Web-Alarm is explained

9.1.1 Power-LED

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

9.1.2 Status-LED

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

9.1.3 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 Web-Alarm 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 Web-Alarm is no longer operable in this state. Please return the unit through your dealer to W&T for inspection*

9.1.4 Diag-LED

Indicates internal configuration errors. For error analysis open the page

```
http://<IP-Adresse des Web-Alarm>/diag
```

from the device.

9.1.5 System-LED

Indicates an internal communications error. Try to restart the device by momentarily interrupting power. If the condition remains, please return the unit through your dealer to W&T for inspection.

⚠ *If the Web-Alarm has no IP address or address 0.0.0.0, the Diag LED and the System LED will remain on after a reset or new start. The LEDs will turn off only if an IP address is assigned.*

9.1.6 Input 1-6

Indicates the status of the digital inputs. If the LED is on, the input is switched and is treated internally as high/logical 1.

9.1.7 Output 1-6

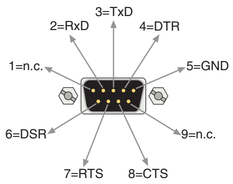
Indicates that an output is switched. If the LED is out, there is no voltage on the output.

9.2 Emergency access

The Web-Alarm has a serial port which can be used as an emergency access. This allows you to:

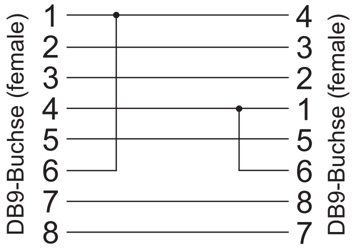
- Assign an IP address
- Restore the factory default settings
- Delete all passwords
- Open a port for a firmware update
- Format the data logger

The pin configuration for the serial port is shown in the following illustration.



Pin configuration for the serial port

Since the pin configuraiton of the RS232 port is identical to that of a PC, standard cables may be used.



Assignments for a null modem cable

Communication with the emergency access of the device is handles without handshake signals. This means a cable carrying only RxD, TxD and GND is sufficient for use

To enable the emergency access, use a null model cable to connect the device to a PC and start a serial terminal program. Set the connection settings to *9600baud, no parity, 8 bits, 1 stop bit, no handshake.*

If the device is connected to the power supply, disconnect it. Turn the supply voltage back on and immediately press the following letters on your keyboard *three times* to open the desired access:

u: Opens an update port. YOu can now load firmware.

f: Restores the device to its factory default settings. All previously made user settings are lost.

p: Deletes all assigned passwords.

Successful opening of the selected emergency access is indicated by flashing of the System and Diag LEDs.

x: For assigning or changing the IP adderess. An entry prompt appears. Enter the desired IP address and confirm by pressing *Enter*.

d: Deletes the contents permanently by formatting. During this process the *System* and *Diag* LEDs flash.

9.3 Factory defaults

Some situations require that the Web-Alarm be restored to its factory default settings. There are three ways to do this:

- Using Web-Based Management
- Using the serial emergency access
- 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.*

9.3.1 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.

9.3.2 Serial emergency access

Connect the Web-Alarm to a PC using a null modem cable and, as soon as you have turned the power on, press the *f* key on your keyboard three times.

9.3.3 Reset jumpers

If you are unable to restore the factory default settings using the Web interface or the serial emergency access, 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 Web-Alarm could be damaged.*

You will see four open jumper contacts on the lower board. Use two jumpers to close these contacts. The orientation of the jumpers corresponds to the two contact pairs on the lower board.

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

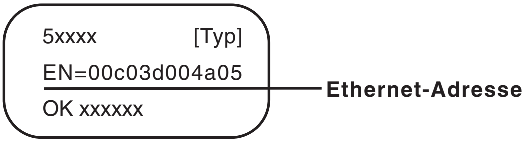
Once the factory default settings have been restored, disconnect the unit from power, remove the jumpers and close up the unit. Now proceed to startup.

9.4 Alternative IP address assignment

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

9.4.1 ARP command

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

9.4.2 Serial port

In contrast to the procedures described above, you can use the serial port to change an already existing IP address for the Web-Alarm.

Connect the RS232 port on the device to a PC and start a terminal program (e.g. Hyperterminal). In the program create a direct connection through your COM port and set the serial properties to *9600 baud, no parity, 8 bits, 1 stop bit, no handshake.*

Interrupt power to perform a reset while holdilng down the *x* key until the reply

```
IPno.+<Enter>
```

appears. Enter the IP address using the usual point notation (xxx.xxx.xxx.xxx) and finish your entry by pressing *Enter*. You can also enter the subnet mask and gateway and turn off the BootP client directly by using the following syntax after the entry prompt:

```
<IP address>,<subnet mask>,<gateway>-0
```

⚠ *If you make a typing mistake, you cannot correct it using Text Backspace. The procedure must be repeated.*

If the entry was correct, an acknowledgment follows with the assigned parameters; otherwise the current IP address appears on the monitor together with the message *FAIL*. This procedure can be repeated as often as desired or necessary.

To turn off the DHCP and BootP functionality directly, directly enter the expression *0* directly after the parameters (e.g. 192.168.1.2-0). The possible options must be separated from the other parameters by a hyphen. The following entries are possible:

- *0*: Disables DHCP and BootP
- *1*: Enables BootP/RARP
- *2*: Enables DHCP

9.4.3 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 Web-Alarm 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 Web-Alarm 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*.

9.5 Firmware update

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

9.5.1 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 Web-Alarm. 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.

9.5.2 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 Web-Alarm
- The file with the new firmware to be sent to the Web-Alarm

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

9.5 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 Web-Alarm 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 Web-Alarm must begin with the expression

```
<io-WebAlarm6x6.1>
```

and end with the expression

```
</io-WebAlarm6x6.1>
```

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.

9.6 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