



www.WuT.de

# Manual

Installation, Startup and Applications

## Web-IO Analog

valid for models:

#57161      Web-IO Analog 0-20mA

#57162      Web-IO Analog 0-10V

Release 1.78 12/2025

© 10/2025 by Wiesemann und Theis GmbH

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Errors and changes reserved:

As we may make mistakes, none of our statements may be used without verification. Please report any errors or ambiguities to us so that we can identify and correct them as quickly as possible.

Only perform work on or with W&T products if it is described here and you have read and understood the instructions completely. Unauthorized actions can cause hazards. We are not liable for the consequences of unauthorized actions. If in doubt, please check with us or your dealer!

# Content

<b>1. Legal notices</b> .....	<b>7</b>
Warning notice concept .....	7
Qualified personnel .....	7
Disposal.....	8
Symbols on the product .....	8
<b>2. Safety instructions</b> .....	<b>9</b>
General information .....	9
Intended use.....	9
Electrical safety.....	9
<b>3 Assembly and wiring</b> .....	<b>11</b>
3.1 Assembly.....	11
3.2 Wiring .....	12
Connection of the supply voltage.....	12
Wiring of the inputs/outputs.....	13
Terminal assignment 57161 .....	13
Current input 0/4-20mA, passive .....	13
Current output 0-20mA .....	14
Terminal assignment 57162.....	15
Voltage input, passive 0-10V .....	15
Voltage output 0-10V.....	16
3.3 Network connection .....	17
3.4 LED displays.....	17
<b>4 Power supply</b> .....	<b>20</b>
4.1 PoE supply.....	20
4.2 External power supply.....	20
<b>5 IP configuration</b> .....	<b>21</b>

- 5.1 IP configuration via WuTility ..... 21
  - 5.1.1 Possible applications and requirements..... 21
- 5.2 IP configuration via DHCP protocol ..... 24
  - 5.2.1 Manual activation of DHCP ..... 24
  - 5.2.2 System name ..... 24
  - 5.2.3 Lease time..... 25
- 5.3 IP configuration using the ARP command..... 25
- 6 Ethernet connection ..... 28**
  - 6.1 Link status..... 28
  - 6.2 10/100BaseT on RJ45 ..... 28
- 7 Online measurement data storage in the W&T Cloud..... 29**
  - 7.1 Automatic connection..... 29
  - 7.2 Create user account ..... 29
  - 7.3 Assign measurement data in the cloud using a code..... 29
  - 7.4 Assign measurement data from the device..... 30
- 8 Configuration via web-based management ..... 31**
  - 8.1 Home..... 31
  - 8.2 Visualization..... 32
  - 8.3 My web page ..... 33
  - 8.4 Log in..... 33
- 9 Basic settings..... 35**
  - 10 Network..... 35
    - 10.1 Sensors ..... 36
    - 10.3 Language/info..... 38
    - 10.4 Data storage..... 38
    - 10.5 Password ..... 38
    - 10.6 Certificates..... 39
- 11 Websites ..... 41**
  - 11.2 Home..... 41
  - 11.3 My Web Page ..... 41
- 12 Communication paths ..... 43**
  - 12.1 Mail..... 44

12.2 MQTT.....	44
12.3 REST.....	45
12.4 Cloud.....	48
12.5 Web-API.....	48
12.6 Modbus-TCP.....	48
12.7 Socket-API.....	57
12.8 RSS.....	57
12.9 OPC DA.....	57
12.10 OPC UA.....	58
Establishing an SNMP session.....	61
Access to inputs and outputs.....	62
12.12 FTP.....	62
<b>13 Alarms/Messages .....</b>	<b>63</b>
Trigger.....	63
<b>Actions .....</b>	<b>64</b>
E-Mail message.....	65
SNMP-Trap.....	65
MQTT-Publish.....	66
HTTP-Request.....	66
TCP messages.....	66
UDP messages.....	66
Syslog messages.....	67
FTP messages.....	67
Switching outputs.....	67
Switching own outputs.....	67
Switching the outputs of another Web-IO.....	67
<b>14 Diagnosis .....</b>	<b>69</b>
<b>15 Device information.....</b>	<b>70</b>
<b>16 Maintenance .....</b>	<b>71</b>
16.1 Reboot device.....	71
16.2 Restore device.....	71
16.3 Save configuration.....	71
16.4 Restore configuration.....	71

<b>17 Access from your own applications .....</b>	<b>72</b>
Access via TCP/IP sockets .....	72
Command strings ASCII.....	72
TCP server .....	74
UDP peer .....	75
BINARY binary structures.....	75
HTTP request .....	76
<b>18 Firmware update .....</b>	<b>77</b>
18.1 Where can I get the latest firmware??.....	77
18.2 Firmware update via the network under Windows.....	77
<b>19 Security information .....</b>	<b>79</b>
19.1 Function and typical application .....	79
19.2 Requirements for integrators and operators .....	79
19.3 Installation site.....	79
19.4 Commissioning.....	80
19.5 IP assignment .....	80
19.6 Password .....	80
19.7 Registration for security-related information .....	80
19.8 Operation and configuration .....	81
20.8.1 Configuration via HTTPS / PKI environments if possible.....	82
20.8.2 Encrypted communication .....	82
19.8.3 Isolation of the subnetwork via router/firewall.....	83
19.8.4 Updating the firmware .....	83
19.8.5 Service, maintenance, and decommissioning.....	84
19.9 Emergency access and factory settings.....	84
<b>21 Battery replacement and disposal.....</b>	<b>88</b>

# 1. Legal notices

## Warning notice concept

These instructions contain information that must be observed for your personal safety and to prevent damage to property. The information is highlighted by a warning triangle. Depending on the level of danger, the warnings are displayed in descending order as follows:

### DANGER

indicates a hazard that will result in death or serious injury if appropriate precautions are not taken.

### WARNING

indicates a hazard that could result in death or serious injury if appropriate precautions are not taken.

### CAUTION

indicates a hazard that may result in minor injury if appropriate precautions are not taken.

### ATTENTION

indicates a hazard that may result in damage to property if appropriate precautions are not taken.

If there are several hazard levels, the warning label with the highest level always applies. If a warning label with a warning triangle warns of personal injury, a warning of damage to property may also be included in the same warning label.

## Qualified personnel

The product described in this manual must only be installed and commissioned by personnel who are qualified for the task at hand.

The documentation relevant to the task at hand must be observed, in particular the



safety and warning instructions contained therein.

Qualified personnel are capable of recognizing risks and avoiding potential hazards when handling the products described due to their training and experience.

## Disposal

Electronic devices must not be disposed of with household waste, but must be disposed of properly as electronic waste.

## Symbols on the product

Symbol	Explanation
	CE labeling  The product complies with the requirements of the applicable EU directives.
	WEEE labeling  The product must not be disposed of with household waste, but must be disposed of in accordance with the disposal regulations for electrical waste applicable at the installation site.

## 2. Safety instructions

### General information

These instructions are intended for the installer of the Web-IO described in the manual and must be read and understood before work begins. The devices may only be installed and commissioned by qualified personnel.

### Intended use

#### DANGER

The Web-IO Analog devices from Wiesemann & Theis are devices for monitoring and controlling analog measured values via a network.

Any other use or modification of the described devices is not in accordance with their intended purpose.

### Electrical safety

#### WARNING

Before starting any work on the Web-IO, the power supply must be completely disconnected by taking appropriate measures. Make sure that the device cannot be accidentally switched on again!

The Web-IO may only be used in closed and dry rooms.

The device should not be exposed to high ambient temperatures or direct sunlight, nor should it be operated near heat sources. Please observe the restrictions regarding the maximum ambient temperature.

Ventilation openings must be free of any obstructions. A distance of 10-15 cm between the Web-IO and adjacent heat sources should be maintained.

The input voltage must not exceed the nominal values specified.

During installation, ensure that no loose wires protrude into the interior of the

housing through the ventilation slots of the Web-IO. Ensure that no individual wires protrude from the strands, that the entire strand is in the terminal, and that the screws of the connection terminals are tightened securely. Tighten the screws of unused connection terminals.

The power supply unit used to power the Web-IOs must ensure a safe separation of the low-voltage side from the supply network in accordance with EN62368-1 and have "LPS" properties.

## EMC

### ATTENTION

The Web-IOs comply with industrial immunity limits and the stricter emission limits for households and small businesses. Therefore, there are no EMC-related restrictions on the use of the devices in these environments.

*The complete declarations of conformity for the devices described in the manual can be found on the respective Internet data sheet page on the W&T homepage at <http://www.wut.de>.*

## 3 Assembly and wiring

Only a few steps are necessary to commission the W&T Web-IO Analog and make it visible in your network.

### Power over Ethernet

The Web-IO Analog devices can obtain their supply voltage via the network interface in accordance with IEEE802.3af/Power over Ethernet. Power can be supplied via the data pairs as well as via the unused wire pairs in 10/100BaseT (see PoE power supply).



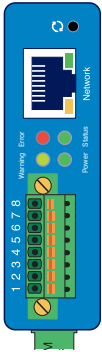
*The Web-IO Analog can also be used in networks without PoE supply. In this case, an external power supply must be used via the screw terminals, as described in the chapter on power supply. No further configurations or settings are necessary.*

The installation and wiring of the Web-IO should be carried out by qualified personnel. The generally applicable rules of technology and the applicable regulations and standards must be observed.

### 3.1 Assembly

The Web-IO Analog is designed for mounting in a control cabinet. For mechanical fastening, the Web-IO should be snapped onto a 35 mm DIN rail in accordance with DIN EN 50022. The Web-IO requires 22 mm of width.

## 3.2 Wiring



Ethernet connector (PoE)

Device status LED

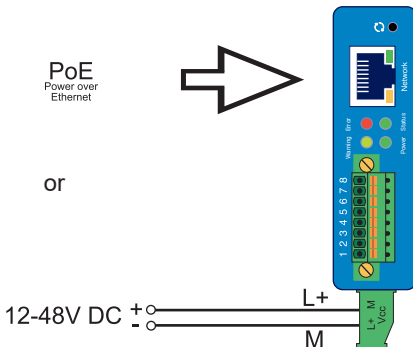
In-/Output wiring

### Connection of the supply voltage

The Web-IO is powered either via PoE (Power over Ethernet Class 2) or with a DC voltage between 12 and 48V. The supply voltage is connected via the green terminal on the bottom.

*Only potential-free power supplies may be used for the external power supply of the Web-IO Analog. Their reference ground for the output voltage must not have a direct connection to the protective earth conductor.*

*The simultaneous connection of an external power supply and a PoE infrastructure is not permitted.*



With a typical industrial power supply of 24V, the Web-IO consumes approx. 100mA of current.

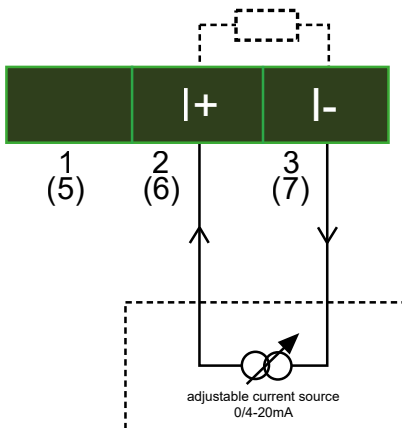
## Wiring of the inputs/outputs

Depending on the configuration, the Web-IO Analog can be wired as follows.

### Terminal assignment 57161

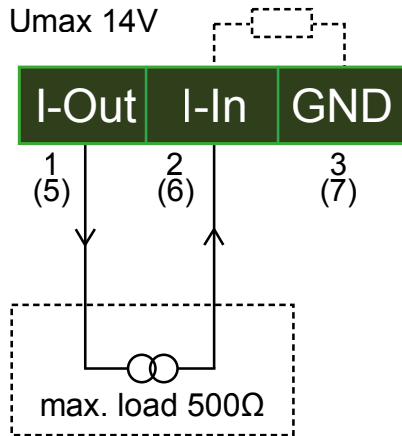
Terminal	Function
1	Current output
2	Current input
3	GND
4	-----
5	Current output
6	Current input
7	GND
8	-----

### Current input 0/4-20mA, passive

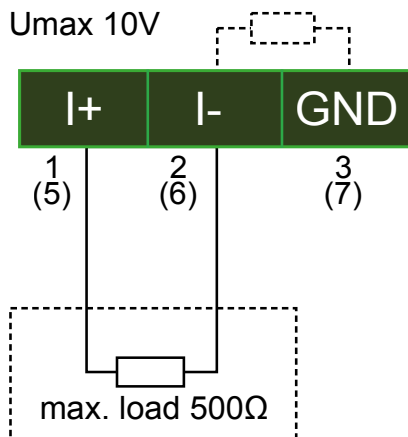


## Current input 0/4-20mA, active

With active current input, 14V is provided on pins 1 and 5.



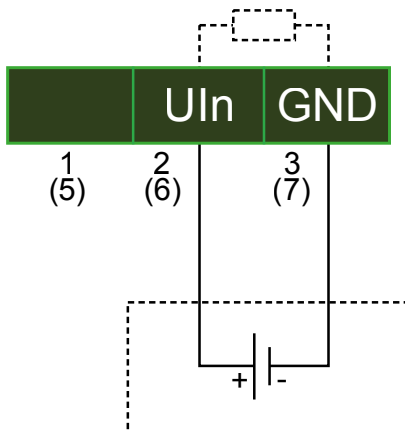
## Current output 0-20mA



## Terminal assignment 57162

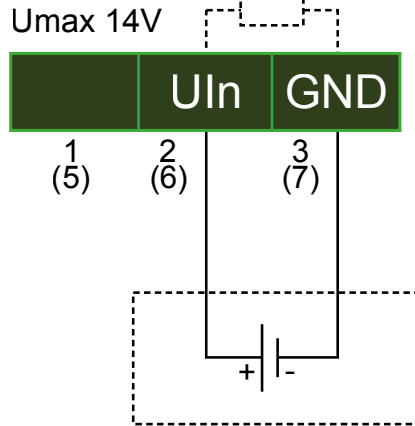
Terminal	Function
1	Voltage output
2	Voltage input
3	GND
4	-----
5	Voltage output
6	Voltage input
7	GND
8	-----

### Voltage input, passive 0-10V



## Voltage input, active 0-10V

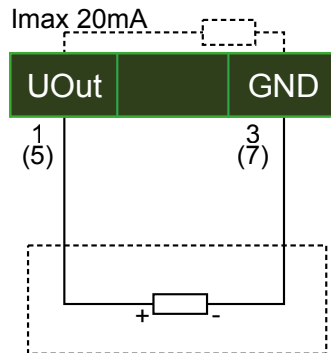
With active voltage input, 14V is provided on pin 1 or 5.



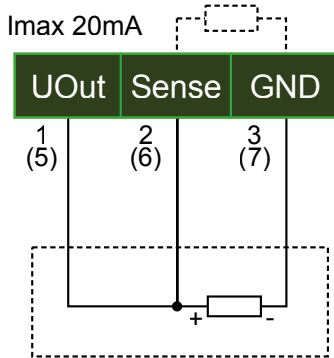
## Voltage output 0-10V

The device requires a sense line to measure the output signal in order to adjust the voltage output.

The device has an internal sense line for this purpose, which is used as standard.



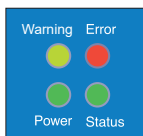
You also have the option of connecting the Sense cable externally. This is particularly recommended for longer cable runs.



### 3.3 Network connection

The Web-IO Analog has an IEEE 802.3-compatible network connection on a shielded RJ45 connector. The pin assignment corresponds to an MDI interface, so that the connection to the hub or switch is made with a 1:1 wired and shielded patch cable.

### 3.4 LED displays



#### Power LED

OFF: No power supply voltage is present. Check that the power supply voltage is correctly connected via PoE or the external power supply unit.

ON: The power supply voltage via PoE or the external power supply unit is present.

### *Status LED*

Fast continuous flashing = booting process, no IP

Fast continuous flashing (approx. 3x/s) indicates that the device is in the booting phase and/or has not yet been assigned an IP address. Please assign an IP address to the device, e.g., using WuTility.

Slow continuous flashing = Ready for operation

Slow continuous flashing (approx. 1x/s) indicates that the device is ready for operation. After configuring the IP address, the device's start page can be accessed by entering the IP address in a web browser.

### *Error LED*

The error LED indicates error conditions on the device.

All LEDs on = Self-test error

The self-test performed after each start or reset of the device could not be completed correctly. The device is no longer operational in this state.

This error can occur if a software update is interrupted prematurely and the operating software has not been transferred in its entirety. Repeat the software update via the network (see chapter Firmware Update) and address the device with the assigned IP address.

If the error cannot be resolved, there may be a hardware problem.

### *Warning-LED*

Displays internal configuration errors or communication problems. To analyze errors, open the page <http://xxx.xxx.xxx.xxx/diag> on the device.



### Speed (yellow)

OFF: When the Link/Activity LED is lit/flashing at the same time, there is a link to a device with 10 Mbit/s (10BaseT).

ON: When the Link LED is lit/flashing at the same time, there is a link to a device with 100 Mbit/s (100BaseT).



### Link/Activity (green)

OFF: The device does not detect a link pulse from a hub/switch. Check the cable or hub port.

ON: The device has a valid link to a hub/switch. In this case, the speed LED indicates the speed.

Flashing: The device is receiving/sending network packets.

## 4 Power supply

The Web-IO Analog can be powered either via PoE or with an external power supply.



The simultaneous connection of an external power supply and a PoE infrastructure is not permitted.

The power consumption can be found in the technical data in the appendix.

### 4.1 PoE supply

In PoE infrastructures (Power-over-Ethernet, IEEE802.3af), power is supplied via the network cabling. The Web-IO Analog supports both phantom power via the data lines and power supply via the unused wire pairs 4/5 and 7/8.

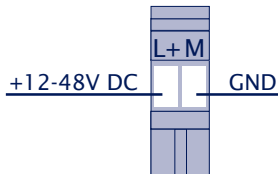
The Web-IO Analog is a PoE power class 1 device (power consumption 0.44 to 3.84W).

### 4.2 External power supply

As an alternative to PoE, power can be supplied externally via the pluggable screw terminal located on the underside of the housing. The input is reverse polarity protected by a single-way rectifier. DC voltages with the following limits can be used:

- DC voltage: 12V (-10%) - 48V (+10%)

When supplying DC voltage, the polarity must be observed:



## 5 IP configuration

### 5.1 IP configuration via WuTility

*WuTility* is the central inventory and management tool for all W&T network devices. In addition to convenient IP parameter assignment, *WuTility* offers quick access to device configuration, the ability to perform firmware updates, manage configuration profiles, etc.

The latest versions are always available on our website at <http://www.wut.de>. The easiest way to navigate the site is to use the menu tree on the left-hand side.

*Downloads -> Web-IO Analog -> WuTility*

The installation is performed by double-clicking on the file `e-5www-22-swww-***.exe`. *WuTility* is started via

*Start -> Programs -> W&T Software Toolkit -> WuTility*

#### 5.1.1 Possible applications and requirements

IP assignment with *WuTility* works independently of the current network parameters of the Web-IO Analog and the computer used. This means that even if the device has IP parameters that do not match the respective network, these can be overwritten with *WuTility*. Similarly, any values that do not match the PC's network can also be assigned to the Web-IO Analog with *WuTility*.

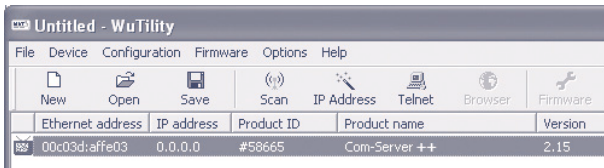
- The PC and Web-IO Analog must be located in the same physical network. This means that assignment across routers is not possible.
- Any firewalls and network security packages installed on the PC must allow UDP broadcast-based communication between *WuTility* and Web-IO Analog. If necessary, these must be configured accordingly or possibly temporarily disabled.
- If the Web-IO Analog is not set to its factory settings and has an administrator password, this must be known in order to make changes using *WuTility*.

## Step 1: Start the assignment dialog

After starting, *WuTility* automatically searches the local network for connected W&T network devices. The search process can be repeated as often as desired by pressing the Scan button.



Identify the Web-IO Analog in the inventory list using its MAC address. For initial installations, the IP address is 0.0.0.0.



Select the Web-IO Analog and press the IP Address button:



The screenshot shows a dialog box titled "Device Settings: Network Parameters". It has two radio buttons: "dynamic (DHCP)" and "static". The "static" option is selected. Below the radio buttons, there are several input fields:
 

- "IP address (must be unique):" with four spinners containing the values 10, 40, 21, and 12.
- "Address range:" with a dropdown menu showing "Subnet #0".
- A text box containing the message "This address might be unused."
- "Subnet mask:" with four spinners containing the values 255, 255, 0, and 0.
- "Default values from..." with a dropdown menu showing "Windows networking".
- "Default gateway:" with four spinners containing the values 10, 40, 250, and 252.
- An unchecked checkbox labeled "Enable Web-based management, on TCP port" followed by a text box containing the value "80".

 At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

## Step 2: Assigning the IP parameters

The static option allows you to assign fixed IP parameters while simultaneously deactivating the DHCP protocol. Enter the desired values for the IP address, subnet mask, and gateway address in the corresponding input fields. The DHCP option activates the DHCP protocol in the Web-IO Analog and operation with a static IP address is no longer possible (detailed information on *IP configuration via DHCP protocol*).

The Continue button transfers the entered values to the Web-IO Analog. If the assignment is successful, all columns of the WuTility inventory list are updated.

Further configuration of the Web-IO Analog is carried out via web-based management. To do this, click the *Browser* button.



For more information, see the chapter *Config. via Web-Based Management*.

## 5.2 IP configuration via DHCP protocol

With the factory settings, the DHCP protocol is activated in the Web-IO Analog, so that in DHCP environments it is sufficient to connect the device to the network.

The following parameters are assigned using DHCP:

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

### 5.2.1 Manual activation of DHCP

To prevent unwanted address assignments or address changes, the DHCP protocol is automatically deactivated for all other methods of assigning IP parameters. The following methods are available for subsequently activating DHCP:

- WuTility management tool

Select the desired Web-IO Analog in the device list and click the IP Address button. In the following dialog, activate the DHCP option and then click Next.

- WBM configuration

The DHCP protocol can be activated in the menu branch *Basic Settings* -> *Network* -> *TCP/IP Settings*.



*A configured static IP address is deleted after DHCP activation and the associated automatic reset. The Web-IO Analog automatically sets this to 0.0.0.0 and starts sending DCHP discover requests.*

### 5.2.2 System name

To support a possible automated update of the DNS system by the DHCP server, the Web-IO Analog identifies itself within the

DHCP protocol with its system name. The factory setting is WEBIO- followed by the last three digits of the Ethernet address. For example, the factory-set system name of a Web-IO Analog with the Ethernet address 00:c0:3d:01:02:03 is WEBIO-010203. The system name of the Web-IO Analog can be changed via configuration. For more information, refer to the chapter Menu: *Basic Settings* -> *Language/Info*.

### 5.2.3 Lease time

The lease time determined and transmitted by the DHCP server defines the validity period of the assigned IP address. After half of the lease time has expired, the Web-IO Analog attempts to extend the validity or update the address with the assigning DHCP server. If this is not possible before the lease time expires (for example, the DHCP server is no longer accessible), the Web-IO Analog deletes the IP address and starts a cyclical search for alternative DHCP servers in order to assign a new IP address.

The lease time associated with the current IP address is no longer available after a reset. After the restart, a corresponding update request is therefore sent to the original DHCP server. If this is not reachable at this point in time, the Web-IO Analog deletes the IP address and starts a cyclic search for alternative DHCP servers. Existing TCP/UDP connections between the Web-IO Analog and other network participants are interrupted as a result.

The remaining lease time can be read out together with the current IP address in the Device Information menu branch (hh:mm:ss).

## 5.3 IP configuration using the ARP command

### Requirements

Assigning the IP address using a static entry in the computer's ARP cache is only possible if the current IP address is 0.0.0.0 (= factory setting). If the Web-IO Analog has any other value, this access is deactivated.

With the factory setting and after a manual switch from *static* to *DHCP*, the method for assigning IP addresses described in this chapter only works with a delay of approx. 2 minutes after a reset or power-up.

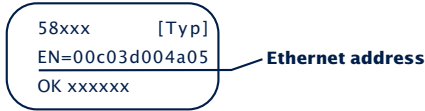
The method does not work across networks, e.g., across routers. This means that the PC used for assignment and the Web-IO Analog must be connected to the same physical network segment. Only IP addresses whose Net ID is identical to that of the assigning computer can be assigned.



*To prevent unwanted changes to the IP address, the DHCP client of the Web-IO Analog is automatically deactivated during IP assignment with the help of a static ARP entry.*

## Step 1

Read the Ethernet address of the Web-IO Analog from the label on the side of the housing.



Use the following command line to create a static entry in the computer's ARP table.

```
arp -s [IP-Adresse] [MAC-Adresse]
```

e.g.:

Command line in Windows:

```
arp -s 10.40.21.12 00-C0-3D-af-fe-01
```

Command line under UNIX/Linux:

```
arp -s 10.40.21.12 00:C0:3D:AF:FE:01
```

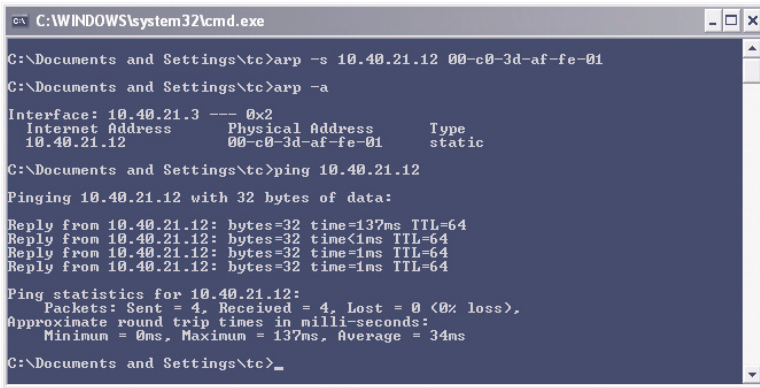


*In Windows environments, IP addresses must be entered without leading zeros. Otherwise, the system will misinterpret the entry and assign an incorrect IP address to the Web-IO Analog. The command prompt required to call the ARP command "cmd.exe" must be started with administrator rights.*

## Step 2

Start a ping to the Web-IO Analog with the desired IP address using the following command line:

```
ping 10.40.21.12
```



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\tc>arp -s 10.40.21.12 00-c0-3d-af-fe-01
C:\Documents and Settings\tc>arp -a

Interface: 10.40.21.3 --- 0x2
   Internet Address      Physical Address      Type
   10.40.21.12           00-c0-3d-af-fe-01   static

C:\Documents and Settings\tc>ping 10.40.21.12

Pinging 10.40.21.12 with 32 bytes of data:

Reply from 10.40.21.12: bytes=32 time=137ms TTL=64
Reply from 10.40.21.12: bytes=32 time<1ms TTL=64
Reply from 10.40.21.12: bytes=32 time=1ms TTL=64
Reply from 10.40.21.12: bytes=32 time=1ms TTL=64

Ping statistics for 10.40.21.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 137ms, Average = 34ms

C:\Documents and Settings\tc>_
```

The Web-I/O Analog adopts the target IP address of the first network packet addressed to it at MAC level as its own and stores it in non-volatile memory. It then responds to the ping requests from the PC.

It is not possible to configure the subnet mask and gateway address using a static ARP entry. These must be configured subsequently via the device's web interface.

## 6 Ethernet connection

The Web-IO Analog has an IEEE 802.3-compatible network connection.

### 6.1 Link status

The link status is indicated by the two LEDs integrated into the RJ45 socket.

- Link/Activity (green)

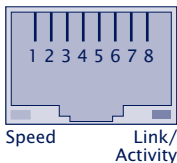
ON indicates a valid link to a hub/switch port. The LED flashes when data is being transmitted.

- Speed (yellow)

ON indicates a 100 Mbit/s link (100BaseT). OFF corresponds to 10 Mbit/s (10BaseT).

### 6.2 10/100BaseT on RJ45

The Web-IO Analog has a shielded RJ45 connector for network connection. The design corresponds to an Auto-MDI-X interface, allowing connection to the switch/hub with a shielded patch cable up to 100 m long.



The network connection is galvanically isolated from both the supply voltage and the measurement input with  $1,5kV_{rms}$ .

*Auto negotiation: 10/100BaseT, full/half duplex*

The Web-IO Analog operates in auto-negotiation mode ex works. Data transfer speed and duplex mode are automatically negotiated with the connected switch/hub and set accordingly.

## 7 Online measurement data storage in the W&T Cloud

With its cloud service, W&T offers a comprehensive solution that, in addition to long-term documentation of measurement data in the internal data logger, also enables data to be backed up in online storage. Measurement data is transmitted directly from the measuring point to the cloud and is thus available online.

### 7.1 Automatic connection

Cloud functionality is enabled by default when the device is delivered. If the device receives its network parameters via DHCP, or if you enable Internet access for the device by entering the network parameters, it will begin to connect to the cloud.

Measurement data transmission will only begin once the device has been assigned to a user account.

### 7.2 Create user account

To transfer the measured data, you must first create a user account for cloud access. To do this, go to the cloud homepage

<http://cloud.wut.de>

and click on the "Create account" link.

After entering your email address and a password, you will receive access to the cloud.

### 7.3 Assign measurement data in the cloud using a code

Log in with your access data at <http://cloud.wut.de> and enter the access code supplied with the device. The measurement data will now be transferred and is immediately available for you to use.

*Alternatively:*

## 7.4 Assign measurement data from the device

After creating a cloud user account, open the configuration menu of your device and log in as an administrator user. Navigate to the page

Communication paths -> Cloud

and enter your user data for cloud access. After clicking on the "Bind" button, all measurement data from this device will be stored for your user account from this point onwards.

By clicking on the "Unbind" button, the assignment of the measurement data will be disconnected from this point on and no further values will be added to your user account.

By clicking on "Bind" again, a new measurement series will be created in the cloud for your user account.



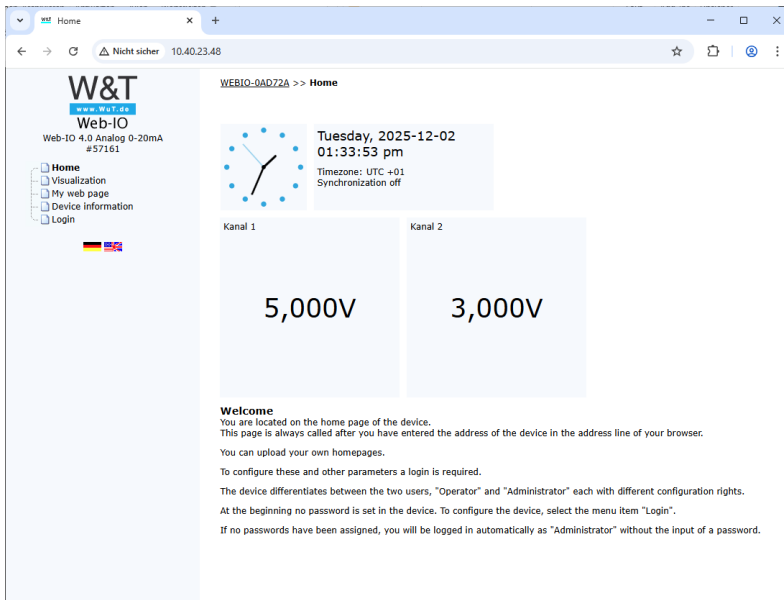
*For more information on how to use the cloud features, please refer to the instructions at <http://cloud.wut.de>.*

## 8 Configuration via web-based management

Further configuration of the device is carried out via the device's web page. To access this, enter the assigned IP address in the address bar of your web browser:

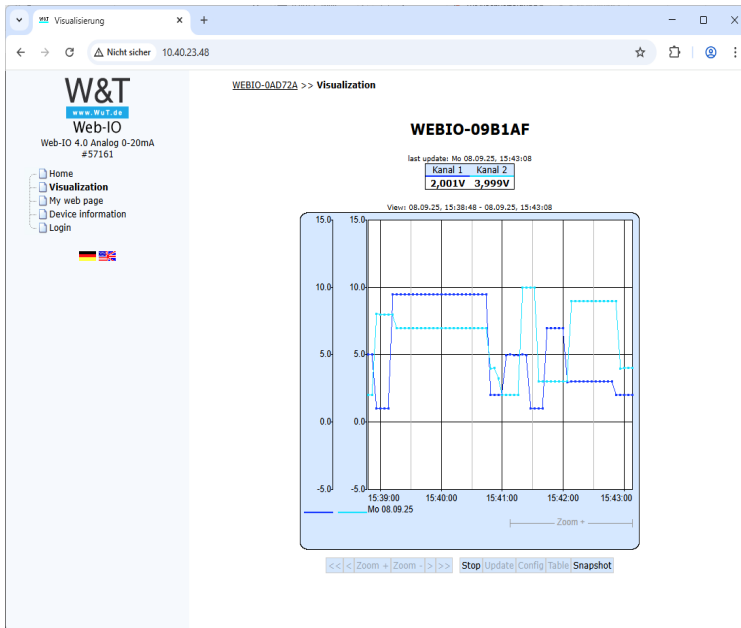
http://<IP address>

### 8.1 Home



The following pages are also available:

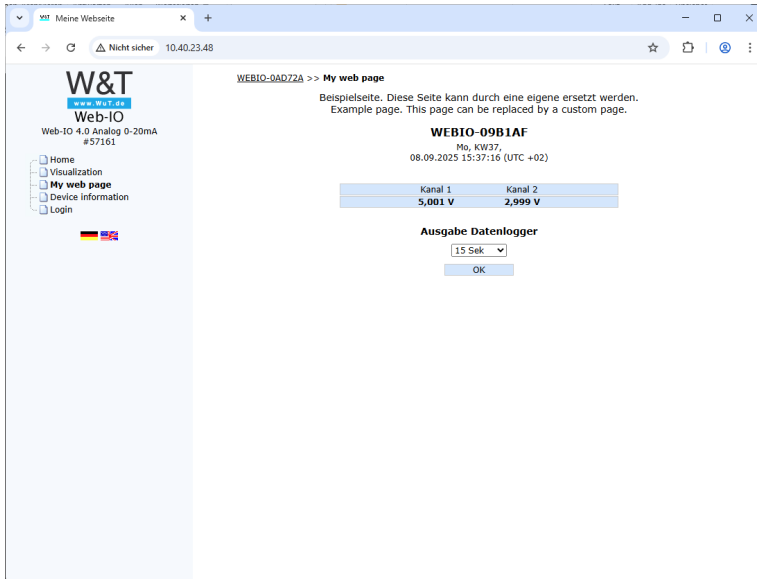
## 8.2 Visualization



This page shows you a graphical display of the stored measured values.

The controls displayed allow you to make temporary adjustments to this display while you are on this page. You can make permanent adjustments via the configuration menu (see *Web pages* -> *Home*).

## 8.3 My web page



This page can be customized or replaced and serves as an example. Here you also have the opportunity to take a look at the device's data logger.

## 8.4 Log in

[WEBIO-07255D](#) >> **Login**

### Login

The login dialog box is titled 'Login' and contains the following fields and options:

- User:** Radio buttons for 'Administrator' (selected) and 'User'.
- Password:** A text input field.
- An information icon (i) in the top right corner.
- A 'Login' button at the bottom right.

You can access the device configuration via the login dialog. The device distinguishes between an administrator and a standard user with different access rights.

No password is configured in the device at the start. Select the administrator user and click "Log in."

The menu tree with all configuration parameters is now displayed.

For more information on the respective configuration parameter, click the info button on the right-hand side of the corresponding parameter.



## 9 Basic settings

In this section of the configuration, you can make all the settings required for the various operating modes.

[WEBIO-0AD72A](#) >> **Basic-Settings**

### Basic-Settings

Here you are able to set the basic configuration.

<a href="#">Network</a>	Set the network basic parameters here.
<a href="#">Inputs/Outputs</a>	Here you will find all the sensor settings. For example, you can configure the name that appears, specify units, or adjust the measured value if necessary.
<a href="#">Date/time</a>	The device time is necessary to create a time stamp for data storage of the measured values. Enter the time of day manually or use the convenience of automatic time compensation using a time server.
<a href="#">Language/infos</a>	Select here the device language and enter additional device information such as its location or contact information. You may also upload your own logo.
<a href="#">Data storage</a>	Select which sensors should be stored and configure the storage interval. The default interval is 15 seconds. Note that changing these settings results in a memory deletion.
<a href="#">Password</a>	You may optionally set password protection for access to the configuration. You can set a password for an administrator user and for a standard user. The standard user has no access right to device system settings such as changing network parameters, etc.
<a href="#">Certificates</a>	Create Certificate Signing Requests that you can have signed by your certificate authority, upload certificates and certificate chains, or create a self-signed certificate by the device.

## 10 Network

Set the basic network parameters here. You can choose between automatic address assignment via DHCP and manual configuration of the parameters. If you want to configure communication parameters with names instead of IP addresses in the further configuration, you can configure additional DNS servers here, in addition to the DNS server assigned via DHCP, if applicable.

### *HTTP or HTTPS*

The browser access for HTTP is enabled for port 80 by default. To switch the access to HTTPS or to change the port, select Basic settings » Network in the navigation tree and then select Protocol in the Access for web services section. All other settings relating to the display in the browser can be made under *Web pages*.

## Setting the system ports and maintenance access

The ports activated here facilitate maintenance and configuration. The ports can be deactivated to meet specific security requirements.

## 10.1 Sensors

Here you have the option of configuring the names of the sensors and, in the case of temperature sensors, the unit.

If you want to adjust the sensors, you can choose between 1-point compensation, in which a correction value is added to or subtracted from the measured value, or 2-point compensation, in which a straight line is calculated across the measuring range.

Alternatively, a compensation file in JSON format with a maximum of 10 correction points per sensor can be uploaded to the device. However, at least two reference points must be available. If this function is activated, all other compensation settings mentioned above are ignored.

Compensationfile ▲

active

Save compensation file: ⓘ

Download

Restore compensation file: ⓘ

Select File Keine ausgewählt

Create a json file, e.g., "senscomp.json," in a text editor:

```
{„Sensor1“:
  [
    {„x1“: „y1“},
    {„x2“: „y2“}
    {„x3“: „y3“}
  ],
„Sensor2“:
  [
    {„x1“: „y1“},
```

```

    { „x2“: “y2” }
    { „x3“: “y3” }
  ]
}

```

The keyword is “Sensor” followed by the sensor number. The order corresponds to the order of the configuration parameters specified on the website.

“x1-xx” corresponds to the measured value to be corrected. One decimal place (with comma or period separator) is allowed. The values for x1-xx must be strictly monotonically increasing.

“y1-yy” corresponds to the correction value. This value is added to or subtracted from “x1-xx”.

A correction line is calculated between the successive measuring points. Example:

```

{ „Sensor1“:
  [
    { „15“: “0.2” },
    { „25“: “-0.1” }
  ],
  „Sensor2“:
  [
    { „50“: “-0.8” },
    { „75“: “0.2” }
  ]
}

```

## 10.2 Date/Time

The device time is necessary to obtain plausible time stamps for storing the measured values.

Enter the time manually or use the convenient automatic time synchronization feature with the help of a time server.

Daylight saving time can also be enabled or disabled here.

## 10.3 Language/info

Here you can configure the default language of the device. This language will be used automatically when the device pages are called up. The default language can be changed dynamically during operation using the flags below the configuration menu. This change is temporary and will not be saved.

On this page, you can change information and device names and upload a custom logo, which will be displayed above the configuration menu.

## 10.4 Data storage

Configure the time interval at which the measurement data is to be stored in the internal data logger and which sensors are to be included in the storage.



*Changing these settings will delete the entire data logger and measurement recording will start again from the beginning.*

You also have the option of downloading the contents of the data logger as a CSV file for further processing. The data logger can also be deleted on this page.

## 10.5 Password

Optionally, set up password protection for access to the configuration.

You have the option of specifying a password for an administrator user and for an operator user.

The operator user has no access rights to the device's system settings, such as changing the network parameters, etc.



*If you assign an administrator password, it must be stored when changing the IP address via WuTility or firmware updates.*

## 10.6 Certificates

On the network side, HTTPS is based on the TLS protocol, which encrypts communication and authenticates communication partners using certificates.

The device is factory-set to identify itself with a self-signed default certificate, which browsers generally consider a security risk. If the application requires secure authentication, the device must be equipped with an individual certificate signed by a trusted certification authority.

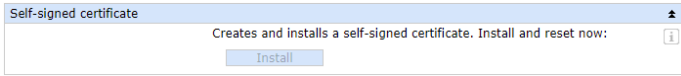
### *Certificate Signing Request (CSR)*

Certificate Signing Request (CSR)	
Specification for CSR:	in the installed certificate:
Common name:	webIO
Organization name:	Wiesemann & Theis
Organizational unit:	
City or Locality:	
State or province:	
Country code (2 letters):	DE
Email address:	
Alternative name:	webIO
Add OPC UA application URI:	<input type="checkbox"/>
<a href="#">Copy content of the installed certificate</a>	
CSR:	Generates a private key and checks the information. <span>?</span>
<input type="button" value="Check"/>	

Here you have the option of generating a CSR (Certificate Signing Request) with a new key pair and individual content.

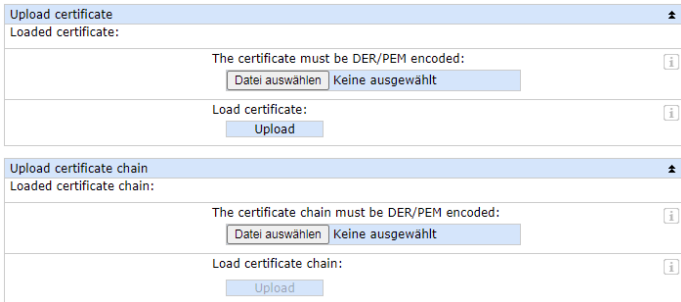
Clicking on the Verify button formally checks the values entered and generates the new key. The new CSR can be downloaded using the Download CSR button.

### Self-signed certificate



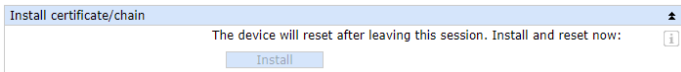
A previously generated individual CSR can be self-signed by the device using the private key associated with the CSR.

### Upload certificate/Upload certificate chain



A previously generated and downloaded CSR can be loaded into the device as a certificate after being signed by an external certification authority. If a certificate chain belonging to the certificate is not already part of the certificate file, it can be uploaded separately afterwards. The files can be in PEM or DER format.

### Install certificate/chain



A previously uploaded certificate, including the associated certificate chain, is installed on the device and, after being saved, is used as a certificate within TLS connections.

# 11 Websites

This device has three preset pages that can be selected as the start page.

The default home page shows you the current values of the individual sensors, which are updated cyclically.

The visualization page allows you to display the measured values graphically.

## 11.1 Browser access

Here you have the option to disable browser access and select the start page.



*Please note that you will no longer be able to make configurations via the web interface if you deactivate browser access. To reactivate it, you must first reset the device to factory settings using the jumper.*

## 11.2 Home

Here you can customize the appearance and access rights of the home page.

## 11.3 My Web Page

The user page can be customized. To do this, you can download it from the device, edit it, and upload it again.

To display the measured values on the user.htm page, you can use the following tags in the source code, which will be replaced with the corresponding values when the page is called up:

```
<w&t_tags=m1>
```

displays the current measured value of the first port.

```
<w&t_tags=m2>
```

displays the current measured value of the second port.

`<w&t_tags=time>`

inserts the current time.

`<w&t_tags=steps>`

inserts a list box for selecting the time periods to be displayed.

`<w&t_tags=ok_button>`

inserts an "OK" button that transfers the selected parameters to the device.

Background color:

For values shown in tables, corresponding background colors can be used, depending on the sensor status:

`<w&t_tag=bc1>`

describes a background color (BGColor) that depends on the alarm status of the first port. If a limit value is exceeded, this color is red. Otherwise, the tag does not describe an explicit color.

`<w&t_tag=bc2>`

Background color for the second port.

`<w&t_tags=sensorx>`

inserts the name of the sensor x into the page and includes a link to the complete sensor description.

`<w&t_tags=device_name>`

inserts the assigned device name.

`<w&t_tags=device_text>`

inserts the freely configurable descriptive text for the device.

`<w&t_tags=location>`

`<w&t_tags=contact>`

inserts the respective text modules, which can be configured under Language/Info.

This configuration page also contains the parameters for customizing the visualization.

## 12 Communication paths

This device can communicate via various network protocols and services. You can configure all necessary parameters here.

[WEBIO-078349](#) >> **Communication paths**

### Communication paths

Here you will find the settings for the network services used for enabling the device to communicate.

<a href="#">Mail</a>	The e-mail function allows you to forward messages to one or more recipients. Here you configure the access parameters for your mail server. SSL/TLS encrypted connections are usual.
<a href="#">MQTT</a>	The Web-Thermometer can send the measured values to an MQTT broker when there is a change or cyclically via MQTT as a topic.
<a href="#">REST</a>	The measured values as well as the device status can be queried using REST (Representational State Transfer). In the Rest query you specify whether the reply should be in JSON or XML format or as a raw text.
<a href="#">Cloud</a>	With the cloud service W&T offers a comprehensive solution that enables the backup of data in online storage in addition to the long-term documentation of temperature and humidity measurement data in the internal data logger. The measurement data will be sent directly from the measuring point to the cloud, and is available online.
<a href="#">Web API</a>	Here you specify whether access is permitted to device status and measurement values via HTTP requests (e.g. for dynamic websites that use AJAX but also to give third-party equipment such as web cameras access to the measurement values).
<a href="#">RSS</a>	The device provides an RSS feed that feed readers can subscribe to. Here you can configure the necessary channel settings.
<a href="#">SNMP</a>	Make the SNMP basic settings here. The device can be incorporated into your existing automation system via SNMP. Use corresponding OIDs to query device and sensor data, or send messages via SNMP trap. An MIB can be downloaded directly in the device at <a href="http://&lt;ip-adresse/mib.zip">http://&lt;ip-adresse/mib.zip</a> .
<a href="#">Syslog</a>	Make the syslog basic settings here. The device can be incorporated into your existing automation system via syslog.
<a href="#">FTP</a>	Messages can be stored directly on an FTP server for archiving and control. Here you configure the basic settings of the FTP client.
<a href="#">Socket API</a>	You can directly retrieve the measured data on a socket access from the device. In the simplest case, send the command "GET /Single" to the unit to get back the current measurement data from the device. The ASCII modes use readable GET commands based on HTTP protocol.

## 12.1 Mail

The email function allows you to send messages to one or more email recipients. Configure the access parameters for your mail server here.

## 12.2 MQTT

After activating MQTT and configuring it in the *Communication Paths » MQTT* menu branch, the Web-IO Analog supports the following options:

Transfer of individual measured values as MQTT topics to an MQTT broker via MQTT publish.

This function is managed in the Web-IO Analog as an alarm/message. A detailed description of the action philosophy applied in the Web-IO Analog can be found in the chapter *Alarms/Messages*.

### *Publish measured values*

To create a new MQTT publish, click the Add button under *Alarms/Messages*. The input mask for a new message appears.

Here you can specify the name of the message and what should trigger it.

For example, set the temperature sensor as the trigger.

Select MQTT Publish as the action. In the following menu, enter the path to which the topic should be written at the broker.

You can freely determine the text content of the topic, using the placeholders described in the info text.

## 12.3 REST

With REST (Representational State Transfer), the Web-IO Analog provides another web-based communication channel.

Communication takes place via specific HTTP requests via the HTTP or HTTPS port entered under *Basic settings » Network » Access for web services*.

In order to exchange data via REST, access must first be enabled via *Communication Paths » Rest*.

If you want to protect REST access against unauthorized access, you can enable digest authentication. Requests must then be made as the “Admin” user with the administrator password or as the “User” user with the user password.

*Read access*

REST uses the HTTP command GET for read accesses.

The Web-IO Analog supports three formats for responses to REST requests:

- JSON
- XML
- Text

The format of the response can be specified in the request. For example,

```
http://<ip-address>/rest/json
```

can be used to retrieve the entire process image of the Web-IO Analog in JSON format. The response would then look like this:

```
{
  <info>: {
    <request>: </rest/json>,
    <time>: <2018-01-01,15:15:58>,
    <ip>: <192.168.0.123>,
    <devicename>: <WEBIO-07DD3A>
  },
  <iostate>: {
    <output>: [{
      <name>: <Output 1>,
      <number>: 0,
      <unit>: <V>,
      <value>: 0.0
    }, {
      <name>: <Output 2>,
      <number>: 1,
      <unit>: <V>,
      <value>: 0.0
    }
  ]
},
  <system>: {
    <time>: <2018-01-01,15:15:58>,
    <diagnosis>: [{
      <time>: <01.01.2018 12:00:00>,
      <msg>: <Gerätstatus: OK>
    }],
    <diagarchive>: [{
      <time>: <01.01.2018 15:15:58>,
      <msg>: <Gerätstatus: OK>
    }
  ]
}
}
```

To query only specific areas or points, the request can be formulated in more detail:

```
http://<ip-adresse>/rest/json/iostate
```

This causes the Web-IO Analog to return the status of all sensors:

```
{
  "iostate": {
    "output": [
      {
        "name": "Kanal 1",
        "number": 0,
        "unit": "V",
        "value": 0.000
      }, {
        "name": "Kanal 2",
        "number": 1,
        "unit": "V",
        "value": 0.000
      }
    ]
  }
}
```

With

```
http://<ip-adresse>/rest/json/iostate/sensor/0
```

the status of the first sensor can be queried specifically.

```
{
  „iostate“: {
    „sensor“: [
      {
        „name“: „Temperatur“,
        „number“: 0,
        „unit“: „ C“,
        „value“: 23.2
      }
    ]
  }
}
```

## 12.4 Cloud

With its cloud service, W&T offers a comprehensive solution that, in addition to long-term documentation of measurement data in the internal data logger, also enables data to be backed up in online storage.

Measurement data is transmitted directly from the measuring point to the cloud and is thus available online.

A user account is required to use the W&T Cloud. You can create one on the Cloud website at:

<http://cloud.wut.de>

## 12.5 Web-API

Another possible action is to send an HTTP request, as required by some devices, such as cameras, in order to query measured values, for example.

Enter the complete URL with all parameters expected by the receiving device as the HTTP request.

e.g.:

`http://<IP/Hostname>/single`

## 12.6 Modbus-TCP

The Web-IO can be activated for Modbus slave operation via the menu item *Communication Paths » Modbus TCP*. Here you can also specify whether the outputs may be switched via Modbus TCP.

The following tables show which function codes and register addresses are supported by the Web-IO.

All addresses are hexadecimal.

The Web-IO has various Modbus memory areas:

- Bit range (starting at address 1000 or 1800),

- 16-bit range (from address 2000),
- 32-bit range (starting at address 5000, 6000, or 7000),
- 8-bit range (exception status, no address).

Addressing is performed bit by bit in the bit range, i.e., 1 bit requires one address. In the 16-bit and 32-bit ranges, addressing is performed word by word (2 bytes).

The analog inputs are located in the 32-bit range starting at address 5036 (example 5716x: 5036 and 5038). The values are given in percent with 3 decimal places and are to be understood as relative.

Value	dez.	hex.	4-20mA	0-10V
0%	0	0x0000 0000	4	0
1°%	10	0x0000 000A	4,0016	0,001
1%	1.000.	0x0000 03E8	4,16	0,1
10%	10.000	0x0000 2710	5,6	1
65,5%	65.535	0x0000 FFFF	14,4856	6,55
65,5%	65.536	0x0001 0000	14,4857	6,55
100%	100.000	0x0001 86A0	20	10
120%	120.000	0x0001 D4C0	23,2	12

The analog outputs are located in the 32-bit range starting at address 5046 (example 5716x: 5046 and 5047). The values (see above) are given as percentages with 3 decimal places.

The alarms are located in the bit range starting at address 1040 (example 5716x: 1040 to 1048), in the 16-bit range at 2004, and in the 32-bit range at address 5004. The alarm trigger bits are located in the bit range starting at address 1800.

The exception status is located in the bit range starting at address 1060, in the 16-bit range at 200D (low byte). Alternatively, the exception status can be read out with function code 0x07.

The configuration status is located in the bit range at address 1068, in the 16-bit range at 200D (high byte).

The diagnostic status (number of errors) is located in the 16-bit range at 2006, in the 32-bit range at 504A.

The diagnostic status bits are in the 16-bit range from 2007 and in the 32-bit range from 504C. With the #5716x, 64 error messages are possible.

The device is identified by its serial number (from 6000) and Mac address (from 6004).

The free memory area that the device provides for any Modbus participants is located in the 32-bit range starting at address 7000.

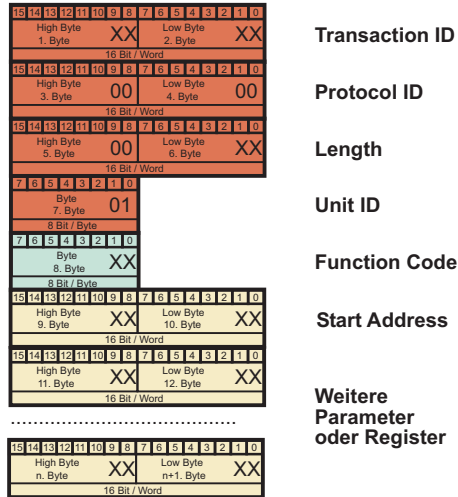
Memory-region	Definition	MB-Start-address [hex]	Read m. FC / Port access	Read m. FC / Block access	Write m. FC / Port access	Write m. FC / Block access	5766x
Bit	Alarm- / Report-Status (1-8)	1040	1,2	-	-	-	1-8
Bit	Alarm- / Report-Status (9-16)	1048	1,2	-	-	-	9
Bit	Exception-Status	1060	1,2	-	-	-	Exc. 0-7
Bit	Conf.-Status	1068	1,2	-	-	-	Conf-St. 0-7
Bit	Alarm-Trigger 1	1800	1,2	-	5	15	1
Bit	Alarm-Trigger 2	1801	1,2	-	5	15	2
Bit	Alarm-Trigger 3	1802	1,2	-	5	15	3
Bit	Alarm-Trigger 4	1803	1,2	-	5	15	4
Bit	Alarm-Trigger 5	1804	1,2	-	5	15	5
Bit	Alarm-Trigger 6	1805	1,2	-	5	15	6
Bit	Alarm-Trigger 7	1806	1,2	-	5	15	7
Bit	Alarm-Trigger 8	1807	1,2	-	5	15	8
8Bit	Exception-Status	-	-	7	-	-	x
16Bit	Alarm- / Report-Status (1-16)	2004	-	3, 4	-	-	1-9
16Bit	Diagnose-Status (Anzahl Fehler)	2006	-	3, 4	-	6, 16	0-x
16Bit	Diagnose-Status (0-15)	2007	-	3, 4	-	-	0-15
16Bit	Diagnose-Status (16-31)	2008	-	3, 4	-	-	16-31
16Bit	Diagnose-Status (32-47)	2009	-	3, 4	-	-	32-47
16Bit	Diagnose-Status (48-63)	200A	-	3, 4	-	-	48-63
16Bit	Diagnose-Status (64-79)	200B	-	3, 4	-	-	64
16Bit	Exception-Status (low byte) + Conf.-Status (high byte)	200D	-	3, 4	-	-	0-7, 8-15

Memory-region	Definition	MB-Start-address [hex]	Read m. FC / Port access	Read m. FC / Block access	Write m. FC / Port access	Write m. FC / Block access	5766x
32Bit	Alarm-/Report-St.(1-32)	5004	-	3, 4	-	-	1-9
32Bit	AI 1	5036	-	3, 4	-	-	1
32Bit	AI 2	5038	-	3, 4	-	-	2
32Bit	AO 1	5046	-	3, 4	-	6, 16	1
32Bit	AO 2	5048	-	3, 4	-	6, 16	2
32Bit	Diagnose-Status (Error quantity)	504A	-	3, 4	-	6, 16	0-x
32Bit	Diagnose-Status (0-31)	504C	-	3, 4	-	-	0-31
32Bit	Diagnose-Status (32-63)	504E	-	3, 4	-	-	32-63
32Bit	Diagnose-Status (64-95)	5050	-	3, 4	-	-	64
32Bit	Serial number	6000	-	3, 4	-	-	OK-Nr.
32Bit	Mac-address	6004	-	3, 4	-	-	Eth-Nr.
32Bit	Memory 0	7000	-	3, 4	-	6, 16	0
32Bit	Memory 1	7002	-	3, 4	-	6, 16	1
32Bit	Memory 2	7004	-	3, 4	-	6, 16	2
32Bit	Memory 3	7006	-	3, 4	-	6, 16	3
32Bit	Memory 4	7008	-	3, 4	-	6, 16	4
32Bit	Memory 5	700A	-	3, 4	-	6, 16	5
32Bit	Memory 6	700C	-	3, 4	-	6, 16	6
32Bit	Memory 7	700E	-	3, 4	-	6, 16	7
32Bit	Memory 8	7010	-	3, 4	-	6, 16	8
32Bit	Memory 9	7012	-	3, 4	-	6, 16	9
32Bit	Memory 10	7014	-	3, 4	-	6, 16	10
32Bit	Memory 11	7016	-	3, 4	-	6, 16	11
32Bit	Memory 12	7018	-	3, 4	-	6, 16	12
32Bit	Memory 13	701A	-	3, 4	-	6, 16	13
32Bit	Memory 14	701C	-	3, 4	-	6, 16	14
32Bit	Memory 15	701E	-	3, 4	-	6, 16	15
32Bit	Memory 16 .. 31	7020	-	3, 4	-	6, 16	16-31

When reading data (memory areas) that have not been defined for the device, the device returns "0".

Modbus data packets always consist of a header, the function code, the start address, and other parameters or registers.

The MSB of the WORD or DWORD determines whether the value is positive (0) or negative (1).



### Transaction Identifier

Used to assign the response of the Web-IO Analog to the client's request. The client normally increments the ID by 1 with each new data transmission. The Web-IO Analog always returns the received value 1:1.

### Protocol Identifier

Irrelevant for communication with the Web-IO Analog and always 0x0000

### Length

Number of bytes sent after Length (total bytes sent).

### Unit identifier

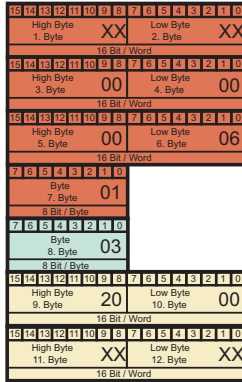
Always 0x01 for Modbus TCP

### Function Code

The function code determines how the Modbus memory of the Web-IO Analog is accessed.

#### *Function Code 0x03 Read Holding Registers*

Function code 0x03 is intended for reading multiple registers (16-bit values). Depending on the start address used, FC 0x03 can be used to query the values of various measurement inputs on the Web-IO Analog.



**Transaction ID**

**Protocol ID**

**Length**

**Unit ID**

**Function Code**

**Start Address**

**Number of Registers**

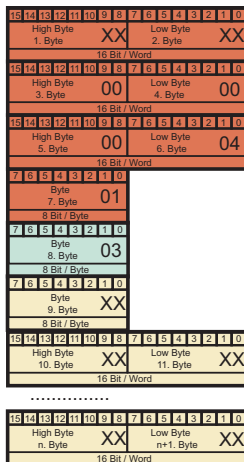
*Start Address*

Specifies the memory location from which registers are to be read.

*Number of Registers*

The number of registers to be read is passed here.

The Web-IO Analog responds with the following packet:



**Transaction ID**

**Protocol ID**

**Length**

**Unit ID**

**Function Code**

**Byte Count**

**Register Value**

*Bytes Count*

contains the number of bytes transferred as registers (2 bytes per 16-bit register).

*Register Value*

One or more 16-bit register values. The first 16-bit register begins with the high byte at the position of the 10th byte.

Depending on the start address (from 0x5000), two 16-bit values—i.e., 4 bytes—are transferred for a requested 32-bit register. In this case, too, the value begins with the highest byte at the position of the 10th byte, and the first low byte is at the position of the 13th byte of the data packet.

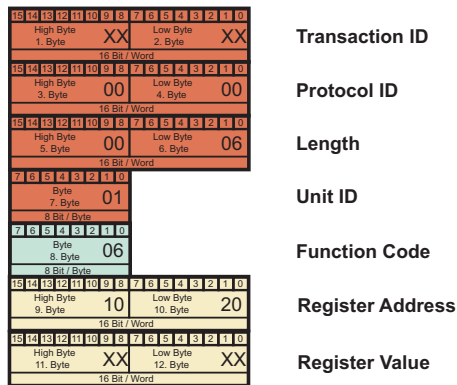
*Function Code 0x04 Read Input Registers*

Function code 0x04 is specifically intended for reading the status of the measured values as a 16-bit register.

The packet structure of the request and response with function code 0x04 is identical to that of function code 0x03.

*Function Code 0x06 Write Single Register*

Function code 0x06 is intended for setting any register (from address 0x7000).



### Register Address

Register Address is used to specify the memory location to which data should be written.

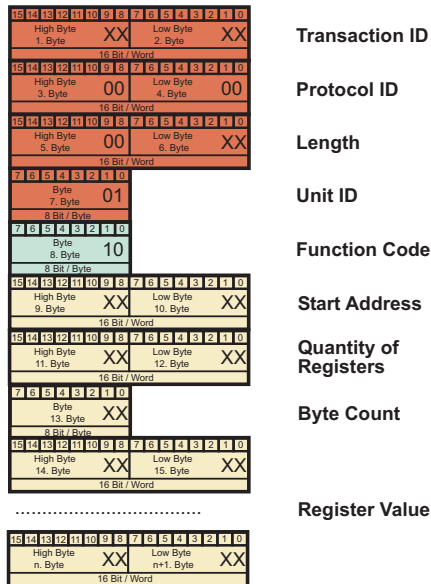
### Register Value

is a 16-bit register value that is written to the Modbus memory of the Web-IO Analog.

The Web-IO Analog responds with a data packet that has exactly the same structure.

### Function Code 0x10 Write Multiple Registers

Function code 0x0F is intended for writing multiple 16-bit register values.



### Start Address

specifies the memory location from which registers are to be written.

### Quantity of Registers

The number of 16-bit registers to be written is transferred here. When writing to the 32-bit range of the Web-IO Analog, two 16-bit registers must be calculated for each 32-bit value.

### Bytes Count

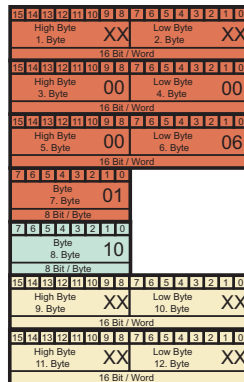
contains the number of bytes to be transferred. Two bytes are calculated for each 16-bit register to be sent.

### Register Value

The 16-bit registers are transferred here. The first high byte is placed as the 14th byte in the data packet. The first low byte is placed as the 15th byte, etc.

When writing to the 32-bit range of the Web-IO Analog (from address 0x7000), two 16-bit registers must be written for each 32-bit value, starting with the highest byte of the 32-bit value.

The Web-IO Analog responds with a data packet with the following structure:



**Transaction ID**

**Protocol ID**

**Length**

**Unit ID**

**Function Code**

**Start Address**

**Quantity of Registers**

### Start Address

specifies the memory location from which the 16-bit registers were written.

### *Quantity of Outputs*

Here, the number of written 16-bit registers is transferred.

## 12.7 Socket-API

You can retrieve measurement data directly from the device via socket access.

In the simplest case, send the command "GET /Single" to the device to receive all measurement data from the device.

Configure the settings for access via HTTP and UDP here.

## 12.8 RSS

The device provides an RSS feed that can be subscribed to by feed readers. Configure the necessary channel settings here.

## 12.9 OPC DA

The Web-IO Analog is preset for OPC DA operation at the factory. If you want to use OPC DA, you only need to activate the Web API function under Communication Channels.

The W&T OPC server must be installed so that your OPC DA client can communicate with the Web-IO Analog. Access via third-party OPC servers is not provided.

In the OPC server, select the menu item Devices » New I/O Device. Enter the IP address and password of your Web-IO Analog and select the device type. Confirm with OK. Finally, you must apply the new entries via the menu item File » Save as active configuration.

The measured values are then provided as OPC-DA items.

## 12.10 OPC UA

The device provides you with OPC UA via a binary TCP protocol. The default port for the server service is the standard port for this application: 4840.

Your client establishes the connection with the following call:

```
opc.tcp://<ip-address>:4840
```

The device provides several authentication methods with corresponding security policies. You can choose between:

- No authentication

  - No security policy

- Sign

  - Security policies:

    - Basic128 - RSA15

    - Basic265

    - Basic265-SHA256

    - AES128-SHA256 RsaOaep

- Sign & Encrypt

  - Security policies:

    - Basic128 - RSA15

    - Basic265

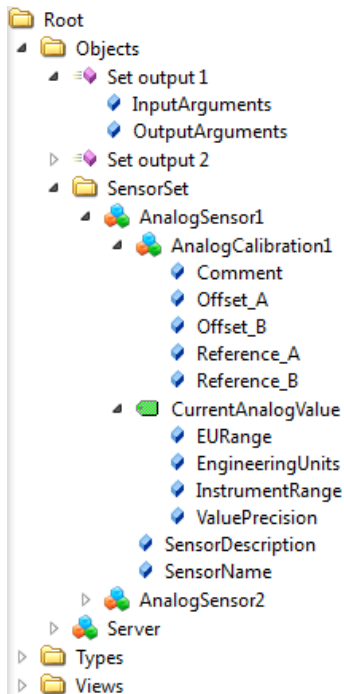
    - Basic265-SHA256

    - AES128-SHA256 RsaOaep

Also configure a UPC UA user name and password. If you select “No authentication,” this is not necessary.

The device provides you with the variable “EURange” for each channel. With the help of this variable, you can specify preconfigured min. and max. values for display instruments in your UPC UA client, within which the display moves. You can configure these values separately for each channel in the device.

The device provides you with the following OPC UA tree:



## Historizing

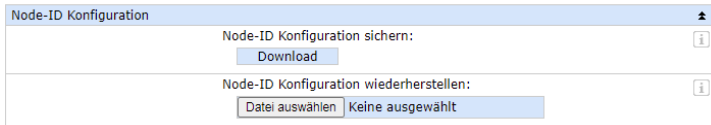
The device supports historizing via OPC UA, i.e., in addition to the current measured value, it can retrieve the measured values stored in the device.

The device can process four parallel OPC UA connections.

### Custom numbering of NodeIDs

The NodeIDs configured ex works for the OPC UA endpoints can be changed to suit customer requirements.

To do this, download the list of preconfigured IDs via the OPC UA configuration page and the “Download” button.



You will receive a file named “nodecfg.json,” which you can open in a text editor.

This file contains the preconfigured NodeID in JSON format, one entry per line, an empty entry for alternative numbering, and the display name of the OPC UA node, named with the letter “T.”

To assign an alternative number, enter your desired NodeID in the free field instead of the placeholder.

Example:

Original entry: { „15284“: “”, “T“: “CurrentAnalogValue” },

modified entry: { „15284“: “12345”, “T“: “CurrentAnalogValue” },

The NodeID of the entry “CurrentAnalogValue” is changed from the original ID 15013 to 12345.

Save the file and upload it back to the device using the “Upload” button on the OPC UA configuration page.

After clicking “Apply,” all changed IDs are applied.

You then need to rebrowse the nodes in your OPC UA client.

The output states are changed using the following method:

- Set output - sets the output defined by the index parameter to the specified value.

## 12.11 SNMP/Syslog

Both the IOs and the configuration of the Web-IO can be accessed via SNMP. Which parameter, which status, and which value can be retrieved under which OID is stored in the private MIB, which can be downloaded directly from the *Web-IO Communication Paths » SNMP* (alternative download at <http://www.WuT.de>).

The MIB can be conveniently viewed with one of the common MIB browsers. This is the fastest way to get an overview of the assignment of the OIDs.

All SNMP-related settings can be made under *Communication Paths » SNMP*. If the outputs are to be settable via SNMP, this must be enabled here.

### Establishing an SNMP session

Read access is possible immediately via SNMP-GET after activating SNMP under *Communication Paths » SNMP*. For write/modify access, you must first log in to the session and enter the system password.

This is done using SNMP-SET via the OID, which you can find in the MIB branch of your Web-IO under

```
wtWebGraphAnalog...SessCntrl » wtWebGraphAnalog...SessCntrlPassword
```

You can check whether a valid session exists by sending a GET query to the OID

```
wtWebGraphAnalog...SessCntrl » wtWebGraphAnalog...SessCntrlConfigMode
```

(Return 1 = valid session, 0 = no session.)

An existing session can be closed via a SET on the OID

```
wtWebGraphAnalog...SessCntrl » wtWebGraphAnalog...SessCntrlLogout
```

During an SNMP session, login attempts via the browser are rejected.

## Access to inputs and outputs

The input/output can be queried or set directly using SNMP Get commands. You can access the respective port via the following paths:

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.3.1.1.1 = Output value 1 as an octet string with comma separators. (Read/Write)

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.4.1.1.1 = Output value as an integer value in thousandths, without comma separation. (Read/Write)

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.8.1.1.1 = Output value 1 as octet string with period separator. (Read/Write)

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.3.1.1.2 = Output value 2 as octet string with comma separator. (Read/Write)

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.4.1.1.2 = Output value 2 as an integer value in thousandths, without comma separators. (Read/Write)

<IP address> 1.3.6.1.4.1.5040.1.2.**28**.1.8.1.1.2 = Output value 2 as octet string with period separator. (Read/Write)

The IDs of the different device versions are:

#57161: 1.3.6.1.4.1.5040.1.2.**28**...

#57162: 1.3.6.1.4.1.5040.1.2.**29**...



*Specify the configured SNMP read or read/write community for the query.*

## 12.12 FTP

For archiving and control purposes, measurement data can be stored directly on an FTP server. Configure the basic settings for the FTP server here.

## 13 Alarms/Messages

With alarms/messages, the Web-IO offers the option of sending individual messages and also setting outputs. This happens depending on defined IO states or other events.

Up to 12 messages can be created and managed, whereby an individual name must be specified for each message.

### Trigger

#### Channel X

One of the two channels can be designated as the trigger. After entering the limit values, specify whether you want to monitor the range outside or inside the configured limit values. If monitoring inside the limit values, it is mandatory to enter both the minimum and maximum values. For monitoring outside the limit values, it is sufficient to enter a single limit.

#### Intervall timer

With the appropriate configuration, the Web-IO can execute actions at specified times. The times are entered in "cron format."

Valid characters are:

- \* represents all valid values in the respective input field (e.g., every minute or every hour)
- specifies a range from...to (e.g., weekday "2-4" stands for Tuesday to Thursday, while entering "\*" triggers the timer on all weekdays).
- / Interval within the entered range (e.g., minute "0-45/2" triggers the timer every two minutes between the 0th and 45th minute (0, 2, 4, 6, 8, 10, ... , 44)).
- , Specifies an absolute value (e.g., minute "0, 15, 30" triggers the timer at the top of the hour, at the 15th minute, and at the 30th minute).

Example:

An action should be performed every Monday at 8:00 a.m. from April to October.

Minute: 0  
 Hour: 8  
 Day of month: \*  
 Month: 4-10  
 Weekday: 1

### Restart device

If a restart is to trigger an action, the Web-IO distinguishes between two variants:

- Cold start

If the restart is triggered by hardware access (supply voltage applied or interrupted, or reset button pressed), the Web-IO evaluates this as a cold start.

- Warm start

A warm start can be triggered via the website under Maintenance using the Restart button. Furthermore, connecting to port 8888 TCP and entering the system password will trigger a restart if the reset port is enabled.

### Sensor lost

In the event of a sensor malfunction, i.e., if values can no longer be received, this can also be used as a trigger for a message.

## Actions

For actions that allow the sending of alarm, notification, and other texts, placeholders can be used within the text, which are replaced with actual content, such as IO states, time, etc., when an action is executed.

Placeholder	Description
<Mx>	Measurement value Channel 1 (commas)
<mx>	Measurement value Channel 1 (decimal points)
<RCx>	Change rate in the last 5 minutes (commas)

Placeholder	Description
<rcx>	Change rate in the last 5 minutes (decimal points)
<Z>	Date/time as string
<\$y>	Year (####)
<\$m>	Month (##)
<\$d>	Day (##)
<\$h>	Hour (##)
<\$i>	Minute (##)

In addition to the actual message that is sent when triggered, a clear message can also be stored for text messages. The clear message is sent when the trigger for the action no longer exists—i.e., when the normal state returns. Depending on the protocol, sending messages takes varying amounts of time. If the triggering condition only exists for such a short time that the corresponding message could not be sent, only the clear message is sent.

## E-Mail message

The recipient, subject and contents of the e-mail can be freely configured.

To be able to send e-mail messages, access to the mail server must be configured and Mail enabled as the communication channel. All the necessary settings can be made under *Communication paths » Mail*. In the information area you can find the general access data for the most common e-mail providers.

## SNMP-Trap

The IP address and Host Name of the SNMP server as well as the message texts can be freely configured.

To be able to send SNMP traps, SNMP must be enabled under *Communication paths » SNMP*. All other parameters that can be set there are not relevant to sending SNMP traps.

## MQTT-Publish

The Web-IO can write any information as an MQTT Topic on a configurable path to an MQTT Broker.

This requires access to the MQTT Broker be configured under *Communication paths* » *MQTT*.

## HTTP-Request

Another possible action is sending of an HTTP request such as required by some devices such as cameras in order to trigger certain functions.

As the HTTP request enter the complete URL with all the parameters expected by the receiving device.

Format:

```
http://<Ip/Hostname>/<request>?Parameter1&Parameter2&ParameterN
```

For devices which require authentication with username and password, enable *Use authentication* and fill in the corresponding fields.

## TCP messages

When sending TCP messages the Web-IO works as a TCP client. When initiating an action it opens a TCP connection to the specified TCP server address on the specified port, transmits the message or clear text and then closes the connection. Any replies from the server are ignored and rejected.

## UDP messages

To be able to send UDP messages, enable UDP Sockets in the UDP-Sockets AS-CII-Mode area under *Communication paths* » *Socket-API*.

When sending UDP messages the Web-IO acts as a UDP peer. The message is transmitted in the form of a UDP datagram to the specified UDP peer address on the specified port. Any replies from the other end are ignored and rejected.

## Syslog messages

IP Address and host name of the syslog server as well as the message texts can be freely configured.

To be able to send syslog messages, Syslog must be enabled under *Communication paths* » *Syslog*. All other parameters there are not relevant to sending syslog messages.

## FTP messages

The Web-IO can save message texts to a file via FTP.

Under *Communication paths* » *FTP*, FTP support must first be enabled and access to the FTP server configured.

The file name, message and clear texts can be formulated as desired.

The options are used to distinguish whether STOR can be used for each initiated action to completely overwrite the file or APPEND is used to append the message and clear texts continuously to the file.

## Switching outputs

When switching outputs the Web-IO distinguishes between switching its own outputs of those of another Web-IO.

### Switching own outputs

When selecting an individual output it can be switched to ON or OFF. Another possibility is to change the existing state.

Alternately multiple outputs can be switched at the same time. You can specify for each selected output whether it is turned ON or OFF.

### Switching the outputs of another Web-IO

Here again either one particular or multiple outputs can be switched.

Enter the IP address to specify which Web-IO to switch the outputs for. For the TCP port enter which one is set for the target Web-IO as access for the browser. If the

target Web-IO is password protected, the password must be entered as well.

For the target Web-IO access for AJAX and HTTP requests must be enabled (*Communication paths » Web-API*) and the controlled outputs must be enabled for switching using HTTP requests.

The outputs on older model Web-IOs (#57661, #57662, #57630, #57631, #57634 and #57637) can also be switched. In this case specify the HTTP port of the Web-IO as the TCP port. In Output Mode Menu the outputs must be set to *HTTP*.

# 14 Diagnosis

Here you will find all runtime error messages generated by the device.

WEBIO-07255D >> **Diagnosis**

**Diagnosis**

18.09.2015 10:18:07: DNS: server reply not recognized

**Diagnosis Archive**

18.09.2015 10:17:46: System: Network malfunction or bad configuration.

18.09.2015 10:17:46: Time Server synchronisation not successful

Clear Report

Errors that have occurred but are no longer current can be found in the diagnostics archive.

Errors that occur during the entry of parameters do not appear on this page but are displayed directly on the parameter.

<b>Invalid value</b>
Alert name: <input type="text"/>

# 15 Device information

Here you will find descriptive information about your device and manufacturer details. You can change the content of this information in the basic settings under Language/Info.

[WEBIO-07255D](#) >> **Device information**

## Device information

Manufacturer and hardware information

Web-Thermo-Hygrobarometer ▲

Hersteller:  
Wiesemann & Theis GmbH

Address:  
Porschestr. 12  
42279 Wuppertal  
Germany

Support Hotline:  
+49-(0)202-2680-0

Internet:  
<http://www.wut.de>

Type:  
Web-Thermo-Hygrobarometer

Article Number:  
#57713

System Name:  
WEBIO-07255D

Description:

IP-address:  
10.40.23.27

Datasheet:  
<http://www.wut.de/57713>

Software revision:  
1.0

Sensor type temperature:  
W&T Temp

Sensor type humidity:  
W&T rH

Sensor type air pressure:  
W&T hPa

MAC address:  
00:C0:3D:07:25:5D

DHCP: DNS Server:  
0.0.0.0

DHCP: Lease Time:  
00:00:00

# 16 Maintenance

[WEBIO-078349](#) >> **Maintenance**

## Maintenance

Device reboot, reset, backup and restore.

Maintenance		▲
Reboot device:	<input type="button" value="Reboot"/>	<input type="button" value="i"/>
Restore device:	<input type="button" value="Factory defaults"/>	<input type="button" value="i"/>

Config		▲
Save configuration:	<input type="button" value="Download"/>	<input type="button" value="i"/>
Restore configuration:	<input type="button" value="Datei auswählen"/> <input type="button" value="Keine ausgewählt"/>	<input type="button" value="i"/>

## 16.1 Reboot device

The device will restart and all network connections will be reset.

## 16.2 Restore device

The device is reset to factory settings. All configuration parameters and passwords are deleted. After the reset, you must start assigning IP addresses again.

## 16.3 Save configuration

After clicking on the download button, a file containing the entire configuration of the device will be downloaded. This can be edited in a text editor.

## 16.4 Restore configuration

Select a configuration file and upload it to the device. After a restart, all configuration parameters will be applied by the device.

## 17 Access from your own applications

In addition to the numerous standardized access options, the Web-IO also offers the option of addressing it from your own application.

This can be done via TCP/IP sockets from common high-level languages. However, it is also possible to use common web technologies such as AJAX or PHP to communicate with the Web-IO.

### Access via TCP/IP sockets

The Web-IO offers three access points for access via TCP/IP sockets.

Access via:

- Command strings      ASCII
- Binary structures      BINARY
- HTTP requests      AJAX

### Command strings ASCII

The inputs can be read and the outputs set by exchanging simple command strings.

Depending on the configuration, the Web-IO operates as a TCP server or as a UDP peer in this mode.

Use the following expression to set the values:

```
GET /outputaccessX?PW=<password>&State=<value>&
```

X: Number of the output: 1=Port 1, 2= Port 2

password: If an Admin password is assigned, it must be entered here in order to be able to set the output value. If no password is assigned, leave this place blank (...?PW=&...)

value: Here you enter the value you want to set on the respective output. The unit of the value corresponds to the scale settings you configured.

To set a value of 50 on Channel 2 without an assigned password, use for example the expression:

```
GET /outputaccess2?PW=&State=50&
```

Response: <Header>;<Sensor-Name>;output2;<value> <unit>

example:

```
„http://<IP address>/outputaccess1?PW=&State=10.5&“
```

Response:

```
„<IP address>;WEBIO-xxxxxx;Sensor 1 4-20mA;output1;10,5 Unit“
```

With „NA=ON“ it is optionally achieved that no response to the outputaccess command is sent by the Web IO.

Example:

```
GET /outputaccess2?PW=&State=50&NA=ON&
```

Similar to setting the output, both input channels can also be polled using command strings.

The expression for polling the respective port is:

```
GET /SingleX
```

X: Number of the Inputs: 1=Port 1, 2= Port 2

Example:

```
10.40.42.44;WEBIO-046EE9;Sensor 1 0-20mA;14,300 mA
```

When entering the command string

```
GET /Single
```

without a port number the device outputs the values for both ports separated by semicolons:

```
10.40.42.44;WEBIO-046EE9;12,000 mA;5,000 mA
```

or

```
12,000 mA;5,000 mA
```

It is also possible to download the data logger content of the device via a socket command. Here you also have the possibility to specify a start and end time for the output:

To download the logger content, send:

```
ET /logger.csv
```

This expression can also include additional parameters which determine the contents:

```
start=ttmmmyyyyThhmmss
```

Start-date and -time for the measurement data to be loaded

```
end=ttmmmyyyyThhmmss
```

End-date and -time for the measurement data to be loaded

```
DTb=x&
```

Output interval, where x =

- 1 -> 15 Sek.
- 2 -> 30 Sek.
- 3 -> 1 Min.
- 4 -> 5 Min.
- 5 -> 15 Min.
- 6 -> 60 Min.

The expression must begin with “?” after the file name, where the individual variables are separated by a “&”.

Example:

```
http://<ip-address>/logger.csv?start=01012022T123000&end=03032022T200000&DTb=3&
```

The above expression generates a CSV file which contains the measurement data from 01.01.2022, 12:30 p.m. until 03.30.2022 8:00 p.m. in 1 minute intervals.

## TCP server

To access the Web-IO as a TCP server using ASCII sockets, enable TCP ASCII-Sockets under *Communication paths* » *Socket-API*. Specify which server port the Web-

IO should accept connections on. The Web-IO can simultaneously provide up to four TCP connections on the specified port – any additional connection attempt is rejected.

If the Web-IO does not receive a valid command within 30 seconds, it closes the connection and is then ready again for a new connection attempt. The Web-IO behaves in the same way when a defective or unknown command is received.

The inputs are generally read using polling. Event-driven evaluation is only possible if the input triggers are correspondingly configured.

### UDP peer

To access the Web-IO via UDP using ASCII sockets, enable UDP ASCII-Sockets under *Communication paths* » *Socket-API*. Specify on which local UDP port the Web-IO should accept datagrams.

Use Remote UDP-Port to specify at which UDP port of the requestor the replies should be sent from the Web-IO. Entering AUTO specifies that the replies go to the port which is entered in the receiving datagram as the sending port.

The inputs can only be read using polling. Event-driven evaluation is possible by adding a corresponding action (see *Actions* section).

### BINARY binary structures

The Web-IO specifies binary structures for various functions such as reading the inputs, setting the outputs etc. Access is exclusively by exchanging these structures.

In this mode the Web-IO can operate as a TCP client, TCP server or UDP peer. Access can be password protected.

Four binary accesses are available which can be configured independently of each other under *Communication paths* » *Socket-API*.

In TCP server mode only one client at a time can connect to the corresponding binary access. Any other connection attempt is rejected.

A detailed description of the supported binary structures and other details about access using BINARY sockets can be found in the Web-IO programming manual.

(Download at <http://www.WuT.de>). From the data sheet page of your Web-IO following the Manual link.

## HTTP request

In addition to the traditional socket accesses, the Web-IO can also be accessed directly via HTTP using HTTP requests.

By default this access is disabled and must first be enabled at *Communication paths* » *Web-API*.

A detailed description of the supported HTTP requests and other details about access using Web techniques such as AJAX or PHO can be found in the Web-IO programming manual. (Download at <http://www.WuT.de>). From the data sheet page of your Web-IO following the Manual link.

## 18 Firmware update

The operating software of the Web-IO Analog is constantly being further developed. For this reason, the following chapter describes the procedure for uploading the firmware.

- Where can I get the latest firmware?
- Firmware update via the network under Windows

### 18.1 Where can I get the latest firmware??

The latest firmware, including the available update tools and a revision list, is published on our website at the following address: <http://www.wut.de>

Before downloading, please note the 5-digit type designation on the Web-IO Analog. From the homepage, you can now access the product overview sorted by item numbers, which will take you directly to the device data sheet. Follow the link to the latest version of the firmware.

### 18.2 Firmware update via the network under Windows

The prerequisite is a PC running Windows XP/Vista/7/8/8.1/10/11 with a network connection and activated TCP/IP stack. For the update process, you need two files, which are available for download from the homepage <http://www.wut.de> as described above:

- The executable tool WuTility for transferring the firmware to the Web-IO Analog
- The file with the new firmware to be transferred to the device

No special preparation of the Web-IO Analog is required for the firmware update.

The WuTility used for the update recognizes all WuT devices in your network and is largely self-explanatory. If you have any questions or uncertainties, please refer to the accompanying documentation or online help.



*Never interrupt the update process yourself by disconnecting the power supply or pressing the reset button, if available. After an incomplete update, the Web-IO Analog will be inoperable.*

*Never mix files with different version numbers in the file name. This will cause the device to malfunction.*

*The Web-IO Analog automatically detects when the transfer of the new operating software is complete and then performs a reset on its own.*

# 19 Security information

The following sections contain relevant information and recommendations from an IT security perspective for commissioning, configuration, operation, and maintenance of the Web-IO Analog.

## 19.1 Function and typical application

The Web-IO Analog from Wiesemann & Theis are devices for temperature and climate monitoring via network.

Measurement data is transmitted via the network as TCP payload and optionally also within higher protocol instances.

Web-IO Analog devices are not designed for operation in a secure network environment. The factory settings focus on the most convenient transmission of measurement data and uncomplicated commissioning and configuration. In insecure network environments and/or in cases of increased security requirements, additional measures must be taken to prevent unauthorized access.

## 19.2 Requirements for integrators and operators

Depending on the individual network environment and security requirements, the factory settings for operational use must be reviewed from a security perspective. Changes and/or additional measures may be required by the integrator or operator. These include in particular:

- Choosing a secure password in terms of length and composition.
- Deactivation of unnecessary services and/or access restrictions by means of an upstream, external firewall.

## 19.3 Installation site

The installation location of the Web-IO Analog must ensure that no unauthorized physical access is possible (e.g., suitably secured room, control cabinet, etc.). Physical access to the Web-IO Analog carries the following risks, for example:

- Decommissioning of the device (removal of the power supply, etc.) and loss of all connections to communication partners.

## 19.4 Commissioning

The commissioning of the Web-IO Analog is divided into the web configuration and the subsequent assignment of the IP address (DHCP, WuTility), as well as the subsequent further configuration via web-based management. With the factory settings, all configuration services are freely accessible. Commissioning must therefore be carried out in such a way that no unauthorized access can occur until the system password has been assigned and a secure configuration has been established.

## 19.5 IP assignment

During initial commissioning, ensure that there is no unauthorized access to the Web-IO Analog until a system password has been assigned. A suitable measure is, for example, commissioning via a point-to-point connection. Only then should the Web-IO Analog be connected to the actual target network.

## 19.6 Password

The Web-IO Analog should not be used without a password. The password is the central protection against unauthorized access to the configuration and management of the Web-IO Analog. We recommend using a secure password with a length of at least 15 characters, consisting of upper and lower case letters, numbers, and special characters.

During normal operation, the system password is not transmitted to the Web-IO Analog in plain text. For password-protected access from potentially insecure or public networks, additional measures such as the use of a VPN tunnel must be taken.

## 19.7 Registration for security-related information

Devices can be registered with W&T using the WuTility inventory tool. In the event of security-related updates and/or information, we will notify you immediately by email. In addition to the personal data provided, device-specific data is also stored during registration.

## 19.8 Operation and configuration

All access points and communication channels except browser access are disabled by default.

We recommend only enabling the communication channels and services that are actually required for operation.

The following table provides an overview of the available communication channels.

Communication path/protocol	Connection type	Active by default	Local port	Configurable	Remote port	Configurable	Password protected	Plain text transmission
Utility inventory	UDP	X	8513	X	dynamic			
Utility IP assignment	UDP	X	68		67		X	X
DHCP	UDP	X	68		67			
HTTP	TCP-Server	X	80	X	dynamic		X	X
HTTPS	TCP-Server		443	X	dynamic		X	
DNS	UDP	X	dynamisch		53			
NTP	UDP	X	dynamisch		123			
Geräte-Reset	TCP-Server	X	8888	X	dynamic		X	X
Device update initialization	TCP-Server	X	8002	X	dynamic		X	X
Device update Firmware data	UDP		69		dynamic		X	X
Mail	TCP-Client		dynamisch		587	X	X	
MQTT	TCP-Client		dynamisch		1883	X	X	X
SMQTT	TCP-Client		dynamisch		8883	X	X	
REST (HTTP)	TCP-Server		80	X	dynamic		X	X
REST (HTTPS)	TCP-Server		443	X	dynamic		X	
Web-API (HTTP)	TCP-Server		80	X	dynamic		X	X
Web-API (HTTPS)	TCP-Server		443	X	dynamic		X	
TCP-ASCII-Socket Server	TCP-Server		42280	X	dynamic		X	X
UDP-ASCII-Socket Peer	UDP-Peer		42279	X	dynamic	X	X	X
Modbus-TCP	TCP-Server		502	X	dynamic			

Communication path/protocol	Connection type	Active by default	Local port	Configurable	Remote port	Configurable	Password protected	Plain text transmission
OPC UA	TCP-Server		4840	X	dynamic		X	
SNMP V1	UDP-Peer		161		dynamic		X	X
SNMP V2	UDP-Peer		161		dynamic		X	X
SNMP V3	UDP-Peer		161		dynamic		X	
SNMP-Trap	UDP-Peer		161		162	X		
SYSLOG	UDP-Peer		dynamic		514	X		
FTP control connection	TCP-Client		dynamic		21	X	X	X
FTP data connection (active)	TCP-Server		dynamic		dynamic			
FTP data connection (passive)	TCP-Client		dynamic		dynamic			
HTTP request (action)	TCP-Client		dynamic		80	X	X	X
HTTPS request (action)	TCP-Client		dynamic		443	X	X	
TCP message (action)	TCP-Cleint		dynamic		8000	X		
UDP message (action)	UDO-Peer		dynamic		8500	X		
W&T Cloud	TCP-Client	X	dynamic		443			

### 20.8.1 Configuration via HTTPS / PKI environments if possible

The TLS protocol used by HTTPS provides encrypted and authenticated access to the web interface of the Web-IO. This also applies to access via the web API and REST access. To protect the configuration data, commands, and system password that are exchanged, we recommend activating HTTPS, especially in unsecure network environments. To protect against man-in-the-middle attacks, the self-signed default certificate should also be replaced with an individual, custom certificate.

### 20.8.2 Encrypted communication

The hardware platform of the Web-IO combines low latency with low power consumption. This limits the key length of possible certificates to 2048 bits. The Web-IO supports TLS1.2 at most. In applications with higher requirements, additional measures may be necessary (e.g., VPN).

TLS-encrypted communication is possible in the following operating modes:

- HTTPS (browser)
- HTTPS (web API)
- HTTPS (REST)
- MQTT (SMQTT)
- Mail delivery
- OPC UA

The computationally intensive TLS encryption functions can affect data transfer latencies. For time-critical switching and detection tasks, compatibility with HTTPS access should therefore be tested. This includes, in particular, any security scans in the network. These sometimes open a large number of TLS connections within a short period of time and can therefore lead to interruptions or timeouts in data traffic.

### 19.8.3 Isolation of the subnetwork via router/firewall

For applications that communicate with the Web-IO without encryption, the communication partners (e.g., Web-IO and PC) should be isolated in a separate network segment via a firewall to protect them from espionage. With the help of a W&T Microwall, for example, the communication partners are also protected from harmful events (broadcast storms, overload, etc.) in the main network.

Appropriate firewall rules restrict cross-network access to the minimum necessary.

### 19.8.4 Updating the firmware

W&T releases firmware updates for the Web-IOs to fix functional errors, any vulnerabilities that may have been discovered, or to extend functionality.

The updates are uploaded to the device using the WuTility management tool.

Update files always contain the entire firmware or the entire system of the Web-IO. For this reason, firmware updates always require a restart of the Web-IO and thus also an interruption of operation. Individual configuration data (IP parameters, firewall rules, etc.) are not affected by a firmware update and are retained.

The Web-IOs are based on W&T's own operating system and do not contain any third-party components (e.g., Linux, external TCP stacks, etc.). Compromise with common malware existing for these systems is therefore not possible.

The firmware is uploaded via TFTP (UDP) and the system password is transmitted in plain text on the network side. In unsecure networks or in environments with in-

creased security requirements, additional external measures are therefore necessary (e.g., VPN).

Further details on firmware updates can be found in the Firmware Update chapter.

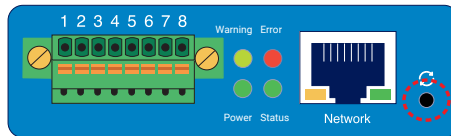
### 19.8.5 Service, maintenance, and decommissioning

Despite high quality standards, electronics can fail at any time, e.g. due to external events. Depending on the availability requirements of the respective application, we recommend taking appropriate precautions.

- Backup/storage of the device configuration
- If necessary, provision of a replacement device
- Documentation of the procedure for replacing the device

When taking the device out of service, the Web-IO should be reset to the factory settings to protect all confidential information stored in the device (IP ranges, external access data, etc.). This can be done either via web-based management or via hardware by pressing and holding the reset button.

## 19.9 Emergency access and factory settings



The reset button, which is recessed in the device, is used for emergency access.

#### *Deleting the password*

Using a pointed object, press the reset button recessed into the front of the Web-IO Analog 8x housing. Hold down the reset button until the status, warning, and error LEDs begin to flash slowly. Now release the reset button.

By entering the IP address of the Web-IO Analog as a URL in the browser, you will be taken to an emergency access web page where you can reset the passwords.

### Reset to factory settings

Press the reset button on the Web-IO Analog 8x with a pointed object. Hold down the reset button until the status, warning, and error LEDs start to flash slowly and then quickly after a while. Now release the reset button.

The configuration of the Web-IO Analog now corresponds to the factory settings.

## 20 Technical specifications

### 20.1 Technical data for item #57161

Terminals and Indicators	
Current input passive	0/4..20mA, 1000hm
Current input active	0/4..20mA, burden max. 5000hm, active voltage U <sub>max</sub> 14V / 40mA
Current output	0/4..20mA, burden max. 5000hm, supply 10V guaranteed
Analog in-/output	8-pin terminal block Conductor cross-section 0.2-1.3mm <sup>2</sup> Strip to 6-8 mm
Current loop monitor	Short-circuit protected and open-loop detection
Network	10/100BaseT autosensing RJ45
Galvanic isolation	Measuring inputs-network: min. 1500 V
Supply voltage	Power-over-Ethernet (PoE) or on screw terminal with DC 12V .. 48V (+/-10%)
Current consumption	typ. 75mA @24VDC, 60mA @48VDC max. 90mA @24VDC, 70mA @48VDC PoE Class 1 (0,44 - 3,84W)
Displays	1 LED Power 2 LEDs Network status 4 LEDs Status and error 1 LED Warning

Measuring Unit	
Resolution	Current input: 2.5µA
Measuring error	max. 0.5% FSR (Full Scale Range 0..20mA) TA = 0-60°C
Sample rate	15, 30 sec, 1, 5, 15, 60 min
Memory depth	min. 150 days, max. 99 years
Data logging (can be queried over the network or alarm triggering)	2 / second
Housing and other data	
Housing	Compact plastic housing for DIN rail mount 105x22x-75mm (LxWxH)
Protection class	IP20
Ambient temperature, storage	-40..+70°C
Ambient temperature, operating	0 .. +60°C

## 20.1 Technical data for item #57162

Terminals and Indicators	
Current input passive	0/4..20mA, 1000hm
Current input active	0/4..20mA, burden max. 5000hm, active voltage U <sub>max</sub> 14V / 40mA
Current output	0/4..20mA, burden max. 5000hm, supply 10V guaranteed
Analog in-/output	8-pin terminal block Conductor cross-section 0.2-1.3mm <sup>2</sup> Strip to 6-8 mm
Current loop monitor	Short-circuit protected and open-loop detection
Network	10/100BaseT autosensing RJ45
Galvanic isolation	Measuring inputs-network: min. 1500 V

Supply voltage	Power-over-Ethernet (PoE) or on screw terminal with DC 12V .. 48V (+/-10%)
Current consumption	typ. 75mA @24VDC, 60mA @48VDC max. 90mA @24VDC, 70mA @48VDC PoE Class 1 (0,44 - 3,84W)
Displays	1 LED Power 2 LEDs Network status 4 LEDs Status and error 1 LED Warning
<b>Measuring Unit</b>	
Resolution	Voltage input: 1.25mV
Measuring error	max. 0.5% FSR (Full Scale Range 0..20mA) TA = 0-60°C
Sample rate	15, 30 sec, 1, 5, 15, 60 min
Memory depth	min. 150 days, max. 99 years
Data logging (can be queried over the network or alarm triggering)	2 / second
<b>Housing and other data</b>	
Housing	Compact plastic housing for DIN rail mount 105x22x-75mm (LxWxH)
Protection class	IP20
Ambient temperature, storage	-40..+70°C
Ambient temperature, operating	0 .. +60°C

## 21 Battery replacement and disposal

The Web-IO Analog contains a 3V lithium manganese dioxide button cell battery of type CR 1632 for buffering the internal clock. This battery has a service life of 10 years and may only be replaced with a battery of the same type.

When operating the Web-IO Analog in a network environment with access to a time server, the battery is not essential for the correct functioning of the device and can be removed.

### **ATTENTION**

The battery may only be replaced or removed by a qualified electrician. Disconnect the power supply before opening.

To remove the battery, open the device housing as follows:

First remove the green power supply terminal. Press the narrow sides of the housing together slightly to create a small gap and pull out the green IO terminal.

The battery is located on the side opposite the network connection.

### **Note according to the Battery Act (BattG):**

Batteries and rechargeable batteries must not be disposed of in household waste; you are legally obliged to return used batteries and rechargeable batteries. Old batteries may contain harmful substances that can damage the environment or your health if not stored or disposed of properly.

However, batteries also contain important raw materials such as iron, zinc, manganese, or nickel and are recycled. After use, you can either return the batteries to us or return them free of charge in your immediate vicinity (e.g., in stores or at municipal collection points). Returns to retail outlets are limited to quantities that are typical for end users and to used batteries that the distributor carries or has carried in its range as new batteries.

The complete declaration of conformity for the device described can be found on the

Internet data sheet page on the W&T homepage at <http://www.wut.de/<item number>>.



Wieseemann & Theis GmbH  
Porschestraße 12  
D-42279 Wuppertal

Mail [info@wut.de](mailto:info@wut.de)  
Web [www.wut.de](http://www.wut.de)

Tel. +49 (0)202 2680-110  
Fax +49 (0)202 2680-265