W&T

www.WuT.de

Manual

Startup and application

IP-Watcher

valid for:

#57955	IP-Watcher Digital 2xIn, 2xOut

Release 1.04 11/2024

Errors and omissions excepted:

Because we are subject to error, none of our statements should be used without verification. Please report any errors or misunderstandings that come to your attention so that we can identify and correct them as quickly as possible.

Only carry out work on or with W&T products if it is described here and you have read and understood the instructions in full. Unauthorized action can cause hazards. We are not liable for the consequences of unauthorized actions. In case of doubt, please contact us or your dealer again!

Content

1. Legal notes

Warning concept

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

⚠DANGER

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

⚠WARNING

indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠CAUTION

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

⚠ATTENTION

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

If there are several hazard levels, the warning notice of the highest level is always used. If the warning triangle is used in a warning against personal injury, then a warning against property damage can also be added to the same warning.

Qualified personnel

The product described in this manual may only be installed and started up by personnel qualified for the task in hand.

The documentation pertaining to the respective task must be observed, in particular the safety and warning instructions contained therein.

Due to their training and experience, qualified personnel are capable of recognizing risks and avoiding possible hazards when handling the described products.Entsorgung

Electronic equipment may not be disposed of with normal waste, but rather must be brought to a proper electrical scrap processing facility.

Symbols on the product

Symbol	Erklärung
CE	CE marking The product complies with the requirements of the applicable EU directives.
UK CA	UKCA marking The product complies with the requirements of the United Kingdom (GB)
	WEEE marking The product must not be disposed of with household waste, but in accordance with the disposal regulations for electrical waste applicable at the place of installation.

2. Safety instructions

General notes

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

Intended use

⚠DANGER

The IP Watchers from Wiesemann & Theis are devices for network monitoring with integrated web server and digital inputs and outputs. They serve as a monitoring unit for the accessibility of network nodes in the local network or Internet.

Not intended is any other use or modification of the described devices.

Electrical safety

⚠WARNING

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

The IP-Watcher may only be used in closed and dry rooms.

The device should not be exposed to high ambient temperatures and direct sunlight, and should not be operated near sources of heat. Please observe the restrictions with regard to the maximum ambient temperature.

Ventilation openings must be free of any obstacles. A distance of 10-15 cm should be maintained between the IP Watcher and adjacent heat sources.

Input voltage and output currents must not exceed the nominal values of the specification.

During installation, ensure that no vagrant wires protrude inside the enclosure through the IP Watcher's ventilation slots. Make sure that no individual wires are sticking out from strands, the complete strand is in the terminal and the terminal screws are screwed tight. Tighten the screws of unused terminals.

It is mandatory that the power supply used to power the IP Watchers ensures safe isolation of the low voltage side from the supply mains according to EN62368-1 and has „LPS“ property.

EMC

⚠ ATTENTION

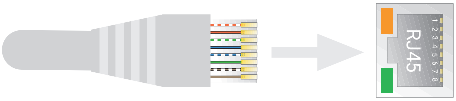
Only shielded network cables may be used to connect the IP-Watchers to the network.

In this case, the IP-Watchers meet the industrial immunity limits and the stricter emission limits for household and small business. Therefore, there are no EMC-based restrictions with regard to the usability of the devices in these environments.

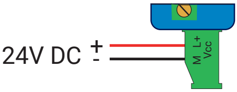
The complete declarations of conformity for the devices described in the instructions can be found via the respective Internet data sheet page on the W&T homepage at *https://www.wut.de*.

3. Quick startup

Network connection



Power supply



For the first test leave the inputs and outputs unconnected.

IP address assignment

Install the Wutility tool (Download: https://wut.de/wutility).

After starting Wutility, your IP Watcher will appear in the list. If multiple devices are displayed, identify your device by its Mac address
(white device label „EN = 00c0:3d......“").

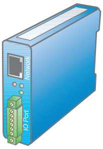
If there is a DHCP server in your network, you can use the assigned IP address for a first test. Alternatively, you can assign a free static IP address to the IP Watcher via the IP address icon in WuTility.

Function test

In the browser, open the IP Watcher web page using the address *http://<IP address of IP Watcher>.*

4. Product introduction

Hardware



Network interface:	RJ45 100/1000BaseT, Power over Ethernet - PoE
Power supply:	Screw terminal 24 ... 48V or PoE
Inputs:	2 Inputs -30 ... +30V DC Switching threshold +8V (+/-1,5V)
Outputs: 2 Outputs,	switching voltage Vdd min. +6V, max +30V DC current driving max. 500mA

Device status, error status and status of inputs/outputs are signaled via corresponding LEDs.

Network Security

All available network accesses are configurable and must first be enabled by the administrator. Only the browser access, the inventory via Wutility and the port for initializing firmware updates are enabled in factory defaults. In addition, DHCP is enabled.

Access rights

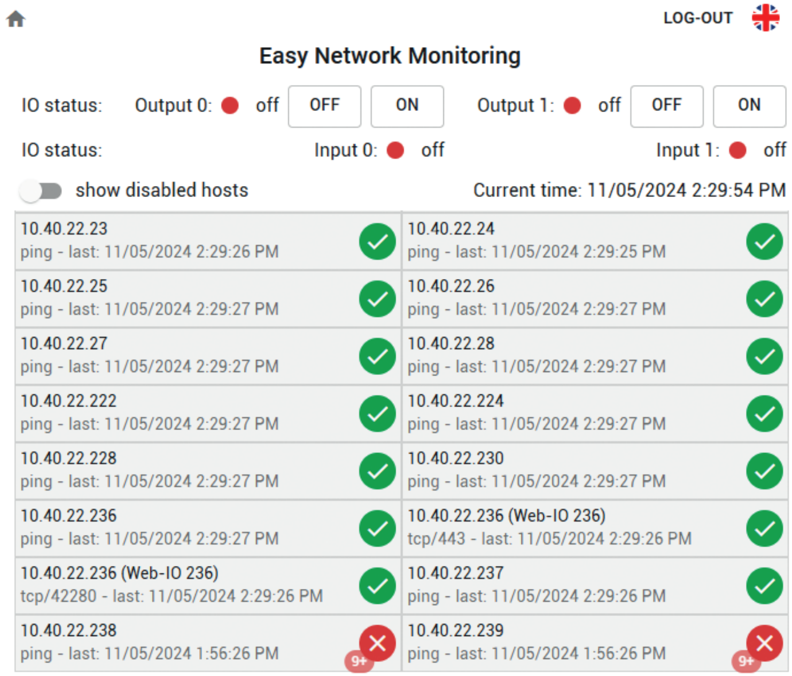
Configuration and operation of the IP-Watcher are done in the browser and are only possible after login as administrator.

Configuration changes will not take effect until they are confirmed by clicking the *Save* button.

Functionality

The IP Watcher allows the administrator to create an inventory list of network nodes to be monitored. Each entry includes the IP addresses or hostnames and the monitoring method. Monitoring can be done via ICMP (ping) or by checking the availability of certain TCP ports. The monitoring interval is configurable.

On the start page, the current status of all network nodes is displayed in the browser with the time stamp of the last availability or failure.



Easy Network Monitoring

IO status: Output 0: ● off OFF ON Output 1: ● off OFF ON

IO status: Input 0: ● off Input 1: ● off

show disabled hosts Current time: 11/05/2024 2:29:54 PM

10.40.22.23 ping - last: 11/05/2024 2:29:26 PM	✓	10.40.22.24 ping - last: 11/05/2024 2:29:25 PM	✓
10.40.22.25 ping - last: 11/05/2024 2:29:27 PM	✓	10.40.22.26 ping - last: 11/05/2024 2:29:27 PM	✓
10.40.22.27 ping - last: 11/05/2024 2:29:27 PM	✓	10.40.22.28 ping - last: 11/05/2024 2:29:27 PM	✓
10.40.22.222 ping - last: 11/05/2024 2:29:27 PM	✓	10.40.22.224 ping - last: 11/05/2024 2:29:27 PM	✓
10.40.22.228 ping - last: 11/05/2024 2:29:27 PM	✓	10.40.22.230 ping - last: 11/05/2024 2:29:27 PM	✓
10.40.22.236 ping - last: 11/05/2024 2:29:27 PM	✓	10.40.22.236 (Web-IO 236) tcp/443 - last: 11/05/2024 2:29:26 PM	✓
10.40.22.236 (Web-IO 236) tcp/42280 - last: 11/05/2024 2:29:26 PM	✓	10.40.22.237 ping - last: 11/05/2024 2:29:26 PM	✓
10.40.22.238 ping - last: 11/05/2024 1:56:26 PM	✗ 9+	10.40.22.239 ping - last: 11/05/2024 1:56:26 PM	✗ 9+

The state list of the monitored network nodes is visible even without login - but without the possibility of switching the outputs.

Actions or alarms can be created to monitor a subset of network nodes from the inventory list. For each alarm it can be defined whether a mail is sent or an output is switched if a monitored node is not available.

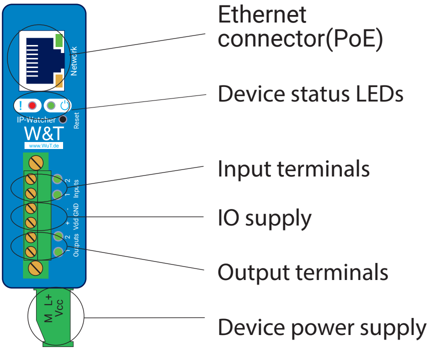
5. Mounting and wiring

The IP Watcher should be installed and wired by qualified personnel. The generally applicable rules of technology and the relevant regulations and standards must be observed.

Mounting

The IP-Watcher is intended for mounting in the control cabinet. For mechanical fixation the IP-Watcher should be snapped onto a 35mm top hat rail according to DIN EN 50022. Thereby the IP-Watcher takes up 22mm width.

Connections

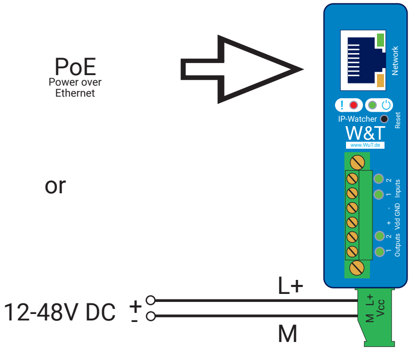


Connection of the supply voltage

The IP-Watcher is supplied either via PoE (Power over Ethernet Class 2) or with a DC voltage between 24 and 48V. The supply voltage is connected via the green terminal on the bottom.

For the external power supply of the IP-Watcher #57955 only potential-free power supplies may be used. The reference ground for the output voltage must not have a direct connection to the protective earth conductor.

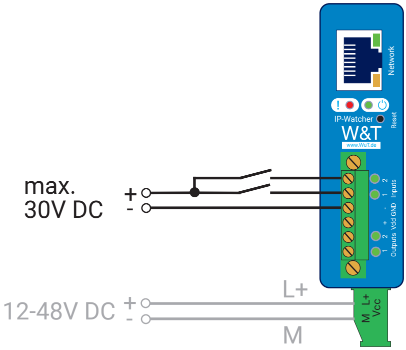
Simultaneous connection of an external supply and a PoE infrastructure is not permitted.



With a typical industrial power supply of 24V, the IP-Watcher draws approximately 140mA of current.

Input wiring

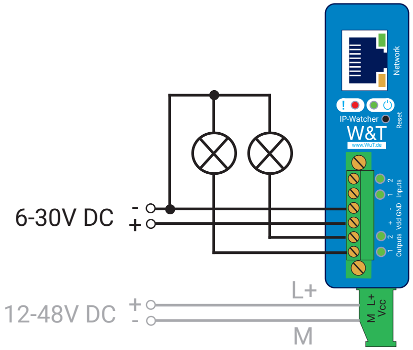
The inputs of the IP-Watcher are wired via the terminals labeled Input 0 and Input 1. The inputs are designed for voltages between -30V and +30V and are galvanically isolated from the internal circuitry via optocouplers with 1kV.



Positive voltages above 8V, referring to the terminal - GND, are recognized as ON signal and signaled via the corresponding LED.

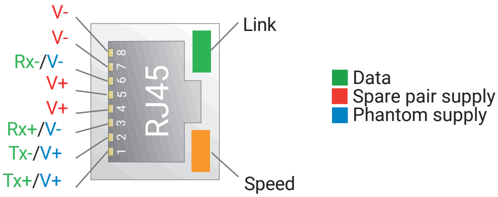
Output wiring

The outputs work current driving and can be loaded with max. 500mA each. The voltage Vdd is switched, which is applied to the terminals + Vdd and - GND.



Network connection

A common Ethernet patch cable (min. CAT5) with RJ45 connectors can be used for the network connection.



With PoE-capable (Power over Ethernet) infrastructure, the IP-Watcher can be supplied via the network connection.

6. Startup

After the IP-Watcher has been properly mounted and wired, the supply voltage can be switched on. During the first boot phase, the green power LED flashes in rapid succession. Subsequently, the red status LED briefly turns on and immediately turns off again. After another phase of slow blinking, the green power LED remains permanently on, signaling that the boot process has been completed.

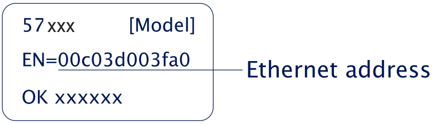
If the network connection is working, the green/orange Speed LED signals the network speed (green = 1000BaseT, orange = 100BaseT). The yellow LED provides information on whether communication is taking place in full or half duplex.

IP address assignment

In the delivery state, the IP Watcher has the IP address 190.107.233.110 and DHCP is enabled.

Networks with DHCP

If a DHCP server is active in the network where the IP-Watcher is connected, an IP address should be assigned to the IP-Watcher automatically. To be able to address the IP-Watcher specifically, you should configure a reservation in the DHCP server so that the IP-Watcher can always be reached under the same address. The Ethernet address required for this can be found on the white sticker on the device.



If in doubt, ask the responsible network administrator.

Networks without DHCP
On a Windows PC, install the program WuTility (Download on *https://www.WuT.de*).

When WuTility is started, the local subnet is searched and all W&T network components found are listed. Select your IP watcher and click the IP address icon. WuTility will suggest the network parameters (subnet mask, gateway, DNS server) that also apply to the PC. If you want the IP-Watcher to work in the same subnet as the PC, you only need to adjust the IP address.

If you select > *any subnet* under Address range, you can also enter parameters that differ from your local network, e.g. to preconfigure the IP Watcher for another network.

Changing the IP parameters

To change IP address, subnet mask, gateway or DNS server afterwards, you can either use Wutility again or adjust the parameters in the browser under *Basic Settings >> Network.*

7. Basic setting

The further configuration of the IP Watcher is done in the browser. Enter the IP address of the IP Watcher as the address or URL. Click on *Login* in the upper right corner of the browser window. No password is assigned in factory defaults, so that a click on the *login* button in the subsequent dialog is sufficient to configure the IP Watcher with administrator rights.

Network

The basic network settings can be entered or changed here. In addition to the IP settings, you can also specify whether browser access is to take place classically via HTTP or encrypted via HTTPS.

Certificate

The browser access to the IP-Watcher is preset to HTTP in factory defaults. If access is switched to HTTPS, the IP-Watcher initially works with a certificate self-signed by W&T.

This factory pre-installed, self-signed certificate of the IP-Watcher generates corresponding security warnings for current browsers. These must be acknowledged for WBM accesses and/or confirmed with suitable exception rules.

In network environments with increased security requirements where these exceptions are not desired/permitted, the factory certificate can be replaced by an individual certificate.

The generation, signing and installation of an individual certificate are divided into the following rough steps:

- Generation of a CSR (Certificate Signing Request) with the associated private key of the IP Watcher
- Download of the CSR and external signature to a certificate by a trusted certification authority
- Upload and installation of the certificate into the IP-Watcher

Generating a Certificate Signing Request (CSR)

Enter all required information in the CSR form. The only mandatory field is the common name under which the IP Watcher web pages will later be called up in the browser. Additional names, IP addresses and wildcard names can be entered under Alternative Names. The name entered in Common Name is automatically transferred to the Alternative Names.

By clicking Create, the IP Watcher generates a key pair and creates a CSR from the information provided.

Installation of a self-signed certificate

By clicking *Install* under Self-signed certificate, the previously generated signing request can be provided with a self-signature. Browsers will report a corresponding security warning when the web pages are accessed.

Externally signed certificate

The generated Signing Request can be downloaded from the IP Watcher via the *Download* button for external signature. The download is in PEM format.

After the signature by a trusted certification authority (CA), the certificate as well as a possibly required certificate chain can be uploaded to the IP-Watcher via the corresponding Upload buttons. All files must be in PEM format.

After a formal check, the certificate is integrated into the system by clicking *Install* under Externally signed certificate and used for all web accesses.

Information and expiration of certificates

Under *Current information* you will find the file information of the current certificate and the certificate chain as well as the validity date.

Date and time

Specify here whether a cyclic adjustment is to be performed with a configured time server. Alternatively, date and time can also be configured manually. The internal clock is buffered by a special capacitor so that the date and time are retained even after an interruption in the supply voltage.

Especially with activated time server adjustment it is important to set the correct time zone. This is the only way to ensure that the local time of a ping loss is entered in alarm messages, for example.

Information

The device and manufacturer information pre-entered ex works, such as the product name, can be adapted here according to your own requirements. In addition, the W&T logo can be exchanged for your own.

The Description parameter has a special feature. The text entered here is displayed on the home page above the monitored inventory list. For example, a location or department can be configured to indicate which monitoring is being carried out. This simplifies the overview if several subareas are each monitored with their own IP Watcher.

Password

Ex works, access to the configuration interface in the browser is possible without entering a password. Assign a login password here to protect the IP Watcher from non-legitimate access.

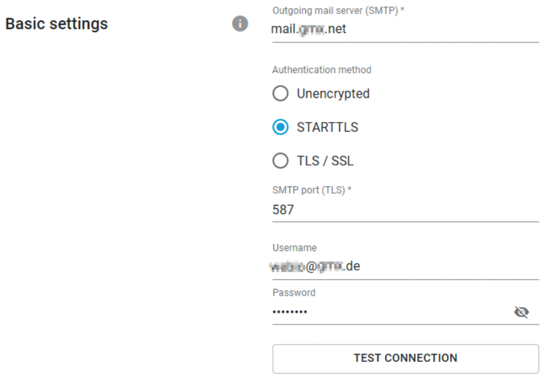
8. Mail Server

In order to send mail messages, some basic settings are necessary first.

If the mail is to be sent via a mail server on the Internet, it is important that the basic network settings are correct. Check under *Basic Settings* >> *Network* in particular whether *Gateway* and *DNS server* are specified correctly.

Basic settings

Here you can make all mail server specific settings.



Basic settings

Outgoing mail server (SMTP) *
mail.[redacted].net

Authentication method
○ Unencrypted
● STARTTLS
○ TLS / SSL

SMTP port (TLS) *
587

Username
[redacted]@[redacted].de

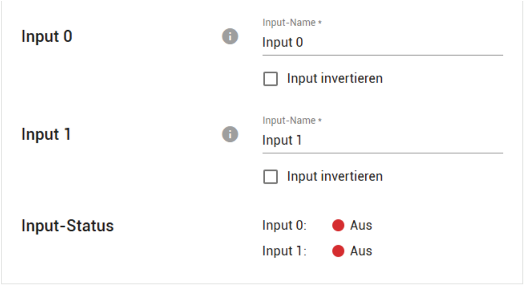
Password
••••••••

The authentication methods commonly used today are *STARTTLS* or *TLS/SSL*.

Using the TEST CONNECTION button, you have the possibility to check whether the configured access data are correct.

Input settings

The *invert input* checkbox can be used to configure whether a physical signal greater than 8V is evaluated as an ON or OFF state for each of the two inputs.



Input 0

Input-Name *
Input 0

□ Input invertieren

Input 1

Input-Name *
Input 1

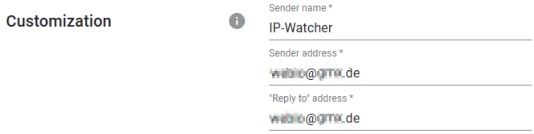
□ Input invertieren

Input-Status

Input 0: ● Aus
Input 1: ● Aus

Individualization

This area allows you to enter an individual sender name or the sender or reply address.



Customization

Sender name *
IP-Watcher

Sender address *
[redacted]@[redacted].de

"Reply to" address *
[redacted]@[redacted].de

Some mail servers only allow mails to be sent if a mailbox address valid on the server is specified as the reply address.

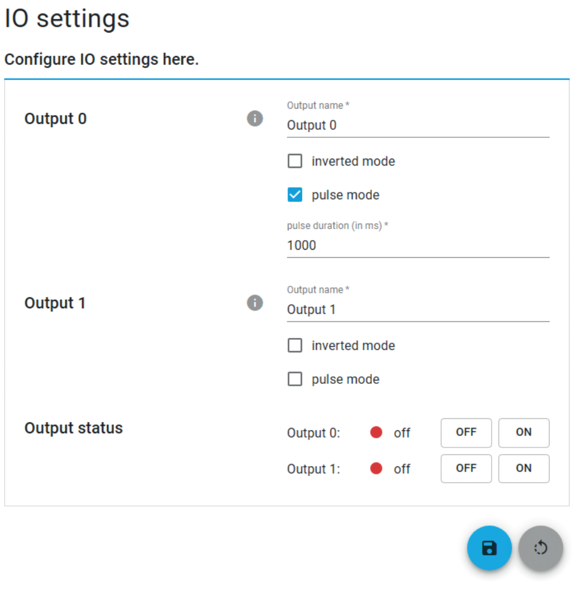
9. IO Ports

The inaccessibility of a monitored network node can trigger an alarm or an action (see Alarms / Actions). Here, among other things, an output can be switched.

Output-Konfiguration

For each of the two outputs it can be configured whether it is to be switched to a static state for the duration of the alarm or whether only a short switching pulse of configurable length is to be output.

Furthermore, it can be defined whether an output is to be switched on or off in the event of an alarm (output inversion).



IO settings

Configure IO settings here.

Output 0

Output name * Output 0

☐ inverted mode

☑ pulse mode

pulse duration (in ms) * 1000

Output 1

Output name * Output 1

☐ inverted mode

☐ pulse mode

Output status

Output 0: ● off

Output 1: ● off

The outputs can also be set or reset manually via the *Output status* menu item.

Switching states - logic and physics

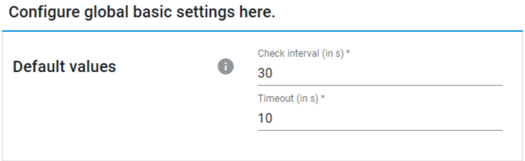
In the event of an alarm, the selected output is always switched to the logical ON state. Whether the output is physically switched on or off in this case depends on whether the menu item Switch output inverted has been activated.

As a general basic rule:
The display in the browser always shows the logical state of the respective output. The LED display on the IP Watcher shows the actual switching state.

10. IP Inventory

Global basic settings

First of all, it should be defined at which interval the network nodes from the inventory list should be checked for reachability and how long to wait for a response.



Configure global basic settings here.

Default values

Check interval (in s) * 30

Timeout (in s) * 10

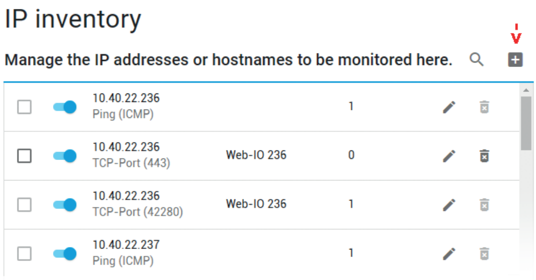
The interval and timeout specifications apply globally to all entries in the inventory list.

Creating the IP address inventory list

Under IP Inventory, up to 100 IP addresses or host names can be added to the list of network nodes to be monitored. There are two basic options here:

Adding individual IP addresses

To add a single address or host name to the inventory list click the plus icon.

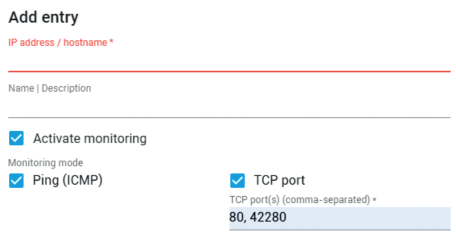


IP inventory

Manage the IP addresses or hostnames to be monitored here.

□	●	10.40.22.236 Ping (ICMP)		1
□	●	10.40.22.236 TCP-Port (443)	Web-IO 236	0
□	●	10.40.22.236 TCP-Port (42280)	Web-IO 236	1
□	●	10.40.22.237 Ping (ICMP)		1

The following dialog will open:



Add entry

IP address / hostname *

Name | Description

☑ Activate monitoring

Monitoring mode

☑ Ping (ICMP)

☑ TCP port

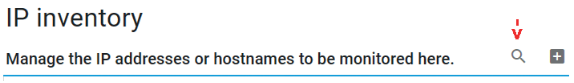
TCP port(s) (comma-separated) *

80, 42280

EEnter an IP address or a host name here and give the entry a custom name. You can also specify the monitoring type here. When monitoring TCP ports, multiple ports can be entered separated by commas. After clicking the *ADD* button, an entry for each selected monitoring type is added to the inventory list.

Scanning IP ranges

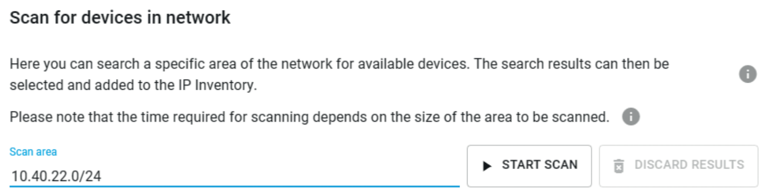
Click on the magnifying glass icon.



IP inventory

Manage the IP addresses or hostnames to be monitored here.

The following dialog will open



Scan for devices in network

Here you can search a specific area of the network for available devices. The search results can then be selected and added to the IP Inventory.

Please note that the time required for scanning depends on the size of the area to be scanned.

Scan area

10.40.22.0/24

Enter the IP range to be scanned here. This is possible in different notations:

CIDR notation

This notation is normally used to define subnets.

Example: 192.168.27.0/24 corresponds to a Class C network and includes all valid IP addresses between 192.168.27.0 and 192.168.27.255, where 192.168.27.0 and 192.168.27.255 are excluded from monitoring as network and broadcast addresses.

IP ranges

Geben Sie hier einfach Start- und End-IP mit Bindestrich getrennt ein

Example: 192.168.27.15-192.168.27.100

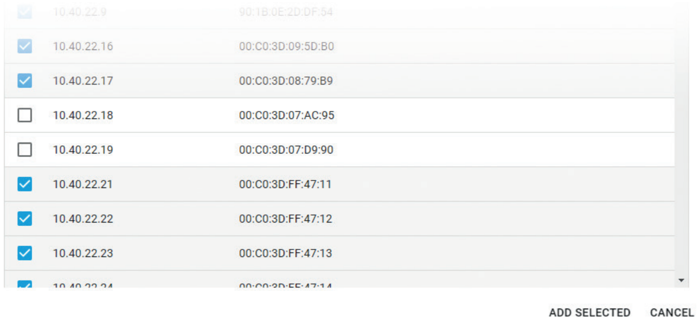
The search for IP addresses present in the range is performed via ICMP, i.e. by pinging all specified IP addresses.

Therefore, when specifying the range to be scanned, it should be noted that checking each individual IP address may take a long time.

- 256 Hosts -> approx. 4 Sec.
- 4096 Hosts -> approx. 70 Sec.
- 65536 Hosts -> approx. 20 Min.

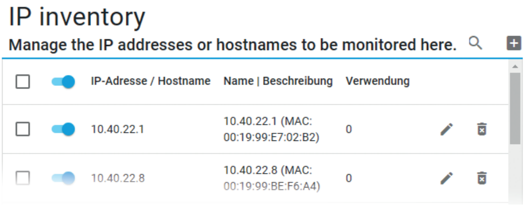
The final inventory list is limited to 100 IP addresses anyway. Although all found network nodes are listed first, only 100 entries can be taken over.

When scanning is complete, the IP addresses found are listed and it is possible to select which IP addresses are to be transferred to the IP inventory list:



☑	10.40.22.9	90:1B:0E:2D:DF:54
☑	10.40.22.16	00:C0:3D:09:5D:B0
☑	10.40.22.17	00:C0:3D:08:79:B9
□	10.40.22.18	00:C0:3D:07:AC:95
□	10.40.22.19	00:C0:3D:07:D9:90
☑	10.40.22.21	00:C0:3D:FF:47:11
☑	10.40.22.22	00:C0:3D:FF:47:12
☑	10.40.22.23	00:C0:3D:FF:47:13
☑	10.40.22.24	00:C0:3D:FF:47:14

Before finally saving the inventory list, the entries can be edited by clicking on the pencil icon, e.g. to enter a meaningful name.



IP inventory

Manage the IP addresses or hostnames to be monitored here.

□		IP-Adresse / Hostname	Name | Beschreibung	Verwendung		
□		10.40.22.1	10.40.22.1 (MAC: 00:19:99:E7:02:B2)	0		
□		10.40.22.8	10.40.22.8 (MAC: 00:19:99:BE:F6:A4)	0		

The blue *switch* icon allows to temporarily exclude IP addresses from monitoring.

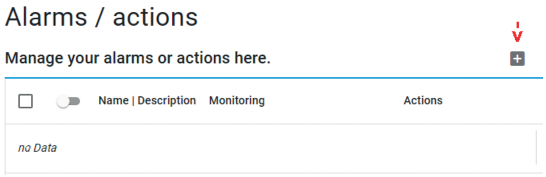
Finally, the list must be saved so that the entries are available in the further configuration.

11. Alarms / Actions

The IP Watcher allows to combine subsets of the IP inventory list as triggers of an alarm. The alarm is triggered even if only one of the associated IP addresses or network nodes is unreachable.

Creating an alarm

To add a new alarm click the *plus* icon.

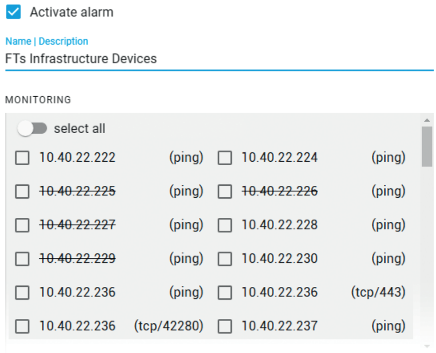


Alarms / actions

Manage your alarms or actions here.

□	Name | Description	Monitoring	Actions
no Data			

In the subsequent dialog you can select which network nodes should be considered for triggering the alarm.



☑ Activate alarm

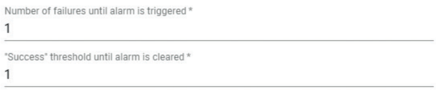
Name | Description: FTs Infrastructure Devices

MONITORING

select all

□ 10.40.22.222	(ping)	□ 10.40.22.224	(ping)
□ ~~10.40.22.225~~	(ping)	□ ~~10.40.22.226~~	(ping)
□ ~~10.40.22.227~~	(ping)	□ 10.40.22.228	(ping)
□ ~~10.40.22.229~~	(ping)	□ 10.40.22.230	(ping)
□ 10.40.22.236	(ping)	□ 10.40.22.236	(tcp/443)
□ 10.40.22.236	(tcp/42280)	□ 10.40.22.237	(ping)

For each alarm, it is possible to specify how many times the response to the ping request to a network node must remain unanswered before the alarm state is set.



Number of failures until alarm is triggered *
1

"Success" threshold until alarm is cleared *
1

Also how often a response must be detected before the alarm status is reset is adjustable.

The logic behind the alarms

Lists within the alarms

The IP-Watcher works internally with three lists per configured alarm:

newFailList

IP addresses that exceeded the failed attempts threshold in the last scan interval are included here.

oldFailList

If an IP address from the newFailList is still unreachable in the next interval, the entry changes from the new-FailList to the oldFailList and remains there until the threshold of the reaccessibility takes effect.

newGoodList

IP addresses that have responded accordingly often after failure change to the newGoodList and are deleted from the list they were in before.

Alarm management

When dealing with alarms, the IP-Watcher works with three definitions:

Alarm Event

An alarm event is triggered when one of the IP addresses selected for the alarm is added to the newFailList. Even if other IP addresses are already entered in the oldFailList, an alarm event is triggered again when a new address is added to the newFailList.

Clear Event

If an IP address changes from the newFailList or oldFailList to the newGoodList, a clear event is triggered even if there are still other entries in one of the two fail lists.

Alarm-Status

The alarm status is set as long as there are entries in one of the two fail lists. Only when both the newFailList and the oldFailList are empty, the alarm status is reset.

Home page display and alarm status

On the start or home page of the IP Watcher, the current status of all network nodes is displayed in the browser with the time stamp of the last availability or failure.

This display does not necessarily reflect the alarm status, since here - in contrast to the alarms - the first unreachability already indicates the failure. However, the alarm status is only set when the configured number of failed attempts is reached.

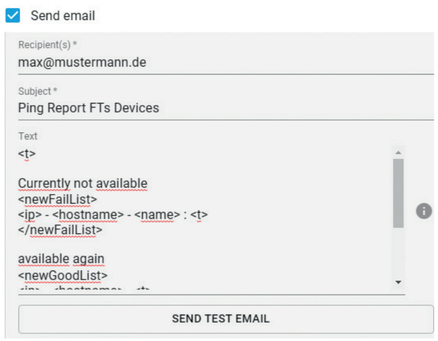
Actions

For each alarm an action can be configured individually, which is triggered by an occurring alarm event.

As an action either a mail can be sent or it is possible to switch an output.

Mail - Alarm message

As an action in consequence of an alarm event the sending of a mail can be configured.



☑ Send email

Recipient(s) *
max@mustermann.de

Subject *
Ping Report FTs Devices

Text

```
<t>

Currently not available
<newFailList>
<ip> - <hostname> - <name> : <t>
</newFailList>

available again
<newGoodList>
```

Recipient and subject

In order to send a mail in case of an alarm, at least one recipient and the subject must be entered.

The specification of several recipients is possible, separated by semicolons, written one after the other.

Mail text

The mail text can be individually designed. To include information about the status of the monitored network nodes, placeholders or tags are available, which are exchanged for real information when the mail is sent.

The following tags help to transfer the contents of the corresponding lists into the mail:

Tag	Description
<newFailList> <.....> </newFailList>	Placeholders can be used between the opening and closing tags to reproduce the existing list entries (see below)
<oldFailList> <.....> </oldFailList>	Placeholders can be used between the opening and closing tags to reproduce the existing list entries (see below)
<newGoodList> <.....> </newGoodList>	Placeholders can be used between the opening and closing tags to reproduce the existing list entries (see below)

The tags themselves do not appear in the sent mail.

Within the list areas the listed placeholders can be used

Placeholders	Description
<t>	Timestamp with date and time
<tDe>	Date and time country specific German
<tEn>	Date and time country specific English
<$y>	Year in format "JJJJ“
<$m>	Month in format "MM“
<$d>	Day in format "TT“
<$h>	Hour in format "hh“

Placeholders	Description
<$i>	Minute in format "mm“
<$s>	Second in format "ss“
<ip>	IP addresse
<hostname>	Hostname if specified, otherwise IP address
<name>	Name configured by the user in the inventory
<mode>	Test mode (ping or TCP port)
<errMsg>	Error message

Time specifications within the list tags reflect the time at which the entry was added to the list. Time specifications in the normal text stand for the time of the mail dispatch.

All information about a network node should be summarized in one line. When the mail is sent, this line is then written one below each other as often as there are entries in the respective list.

Example:

```
<newFailList>
<name>, <ip> <mode> failed since <t>
</newFailList>
```

could look like this for two entries in the mail:

```
PC Office, IP: 192.168.27.13 ping failed since 05.07.2023 08:24:28
PC Store, IP: 192.168.27.145 TCP port 80 failed since 05.07.2023 08:24:28
```

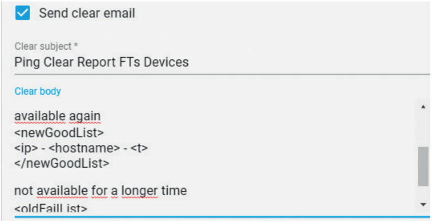
Test mail delivery

The button *SEND TEST-MAIL* can be used to trigger the sending of a test mail.

The entries in the lists do not correspond to the real IP inventory or status in the test mail. Instead, the lists are filled arbitrarily with predefined information.

Mail - Reachability message

If configured accordingly, the IP Watcher can also send a mail when a clear event occurs, the IP watcher can also send a mail.



☑ Send clear email

Clear subject *
Ping Clear Report FTs Devices

Clear body

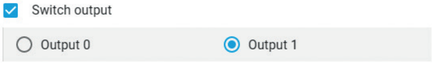
```
available again
<newGoodList>
<ip> - <hostname> - <t>
</newGoodList>

not available for a longer time
<oldFaill ist>
```

The same rules apply here as for the alarm mails.

Signaling via the outputs

In addition or as an alternative to the mail alarm, an output can be switched in the event of an alarm event.



☑ Switch output

○ Output 0 ● Output 1

Logically, the output is always switched to the ON state when an alarm event occurs. Which actual switching state this corresponds to or whether only a short pulse is to be output can be configured in the IO ports menu branch.

Different to the mail messages, which are triggered by occurring events, the switching of the outputs is also oriented to the alarm status.

This means: Switching on is triggered by every occurring alarm event. Switching off is only done when the alarm status is finished - i.e. when NewFailList and old-FailList are empty.

Alternatively, a set output can be switched off manually by the user in the browser via the menu branch IO ports or on the home page by operating the corresponding button.

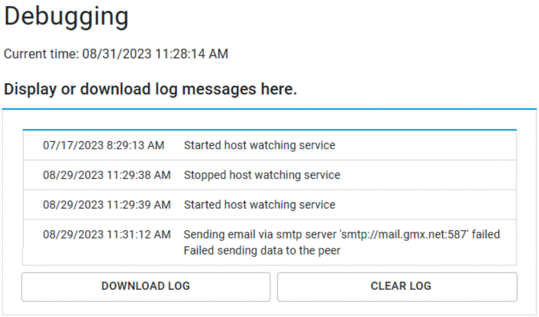
12. Maintenance

Under the menu branch *Maintenance* you have the options:

- restart the IP-Watcher
- reset to factory settings
- update the firmware to the latest version
- save the current configuration
- restore a saved configuration in IP-Watcher
- switch on the LEDs in the front panel for a short time to identify the IP-Watcher in the control cabinet

13. Debugging

This menu item displays log messages with time stamps for the operating states or errors that have occurred.



Debugging

Current time: 08/31/2023 11:28:14 AM

Display or download log messages here.

```
07/17/2023 8:29:13 AM     Started host watching service
08/29/2023 11:29:38 AM    Stopped host watching service
08/29/2023 11:29:39 AM    Started host watching service
08/29/2023 11:31:12 AM    Sending email via smtp server 'smtp://mail.gmx.net:587' failed
                          Failed sending data to the peer
```

In addition, the displayed messages can be downloaded as a log file in CSV format.

If required, the log messages can be deleted.

14. Technical data

Connections and displays

Network:	1 x 100/1000BaseT Autosensing/Auto-MDIX, RJ45
Digital inputs:	2 x Digital In, max. input voltage 30V DC Switching threshold: 8V DC (+/-1V DC)
Digital outputs:	2 x Digital Out, 6 ... 30V DC, 500mA short circuit proof
Supply voltage:	Power over Ethernet (PoE) or 24 ... 48V DC (+/- 10%) per screw terminal
Power consumption:	PoE Class 2 (3.84 ... 6.49W) typ. 140mA at 24V DC external supply
Indicators:	LEDs for system, error and network status

Housing and other data

Housing:	Plastic housing with integrated top-hat rail mounting 105 x 22 x 77mm (L x W x H)
Storage temperature: -	40...+70°C
Operating temperature:	0...60°C
Permissible humidity:	0...95% relative humidity, non-condensing

Wiesemann & Theis GmbH
Porschestraße 12
D-42279 Wuppertal

Mail info@wut.de
Web www.wut.de

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