Manual
RFID Server

Release 1.00, July 2007

Typ 95001
Device-Firmware 4.10

W&T

Subject to errors and changes:

Since we can make mistakes, none of our statements should be used without checking. Please let us know of any mistakes or misunderstandings you are aware of, so that we can recognize and eliminate them quickly.

Perform work on and with W&T products only as described here and only if you have read and understood the manual fully. Unauthorized use can result in hazards. We are not liable for the consequences of unauthorized use. When in doubt, check with us or consult your dealer!

Introduction

The W&T RFID Server is a complete system with integrated antenna and integrated network connection for processing ISO15693 conformal RFID transponders up to a range of 35 cm. An intelligent W&T Tag Control mode relieves the user from having to become familiar with the ISO standard and enables event-triggered communication of the tag data. In parallel with this communication the Reader can use configured filters to autonomously carry out actions depending on the respective tag, the point in time and the state of the digital inputs.

In addition to configuration of these standard functions, this Manual describes the complete network protocol of the RFID Server and thus enables custom incorporation into your own application.

Inhalt

1 System Overview and Quickstart 7
1.1 Quickstart 8
1.2 System overview 10
1.3 Factory default settings 12

2 Assigning the IP Address 13
2. Configuring the network parameters using WuTility 14
2.2 Assigning the IP using the ARP command 17
2.3 IP assignment via DHCP protocol 19
2.3.1 Activating/deactivating DHCP 19
2.3.2 System Name 20
2.3.3 Lease-Time 20
2.3.4 Reserved IP addresses 21
2.3.5 Dynamic IP addresses 21
2.4 IP assignment via BOOTP protocol 22
2.4.1 Address reservation 22
2.5 IP assignment using an RARP server 24

3 Installation and Antenna Tuning 25
3.1 Installing the RFID Server 26
3.2 Antenna tuning 28

4 Connections and Indicators 29
4.1 Supply voltage 30
4.2 Network connection 31
4.3 Digital in-/outputs 33
4.3.1 Digital inputs 34
4.3.2 Digital outputs 35
4.3.3 Relay output 36
4.4 LED indicators 37
4.4.1 Power and network status 37
4.4.2 RFID status 38

5 Web-Based-Management - Basics 41
5.1 Starting Web Based Management 42
5.2 Web Based Management - Login and navigation 43
5.2.2 Navigation 43
5.2.3 Saving and activating the settings 45

6 WBM - General Configuration 47
6.1 Session Control 48
6.1.1 Session Control >> Reset ... 48
6.1.2 Session Control >> New Password ... 48
6.2 Device 50
6.2.1 Device >> Network 50
6.2.2 Device >> Time and Date 53
6.2.3 Device >> Mode 54
6.3 Up-/Download - Configuration profiles 55
6.4 Diagnostics and calibration 56

7 W&T Tag-Control - Configuration 57
7.1 Structure of the W&T Tag Control 58
7.2 Filter TAG- Listen 61
7.3 Filter Time Condition 62
7.4 Filter Input Condition 64
7.5 Actions 65
7.6 Master (Filterset) 67

8 W&T Tag-Control - Network Protocol 70
8.1 Basics of communication 71
8.2 Opening a connection 72
8.3 Definition of the protocol structures 73
8.3.1 Filtermatch (0300) 75
8.3.2 Buffered Match (0301) 76
8.3.3 Clear Buffer (0302) 77
8.3.4 Buffer out of memory (030F) 77
8.3.5 Readflash (0320) 78
8.3.6 Writeflash (0321) 79
8.3.7 Get IO (0322) 81
8.3.8 Set Output (0323) 83
8.4 Error handling 85
8.4.1 Syntax errors(FF00) 85
8.4.2 Functional errors (FF02) 85

9 Communication via OPC **87**

10 Database integration via ODBC **89**
10.1 Basics of ODBC 90

11 Protocol Mode **91**
11.1 Function description 92

Appendix **93**
Firmware-Update 94
Resetting the RFID server over the network 96
Ports used and network security 97
Hardware reset to default settings 100
Number systems/Programing basics 101
Technical Data 104
Declaration of Conformity 105

Index 106

1 System Overview and Quickstart

The following pages provide an overview of the communication concept and operating modes of the RFID Server. In addition, already experienced users will find the basic steps for startup in abbreviated form. Detailed information can be found in the following sections.

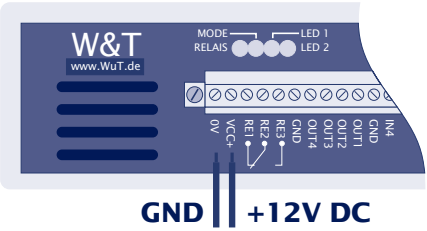
1.1 Quickstart

Location

The RFID Server can be operated in any position or orientation. To attain the optimal capture range, the housing side marked with the antenna symbol should be directed towards the read direction. The air vents on the narrow sides of the housing should not be blocked.

Supply voltage

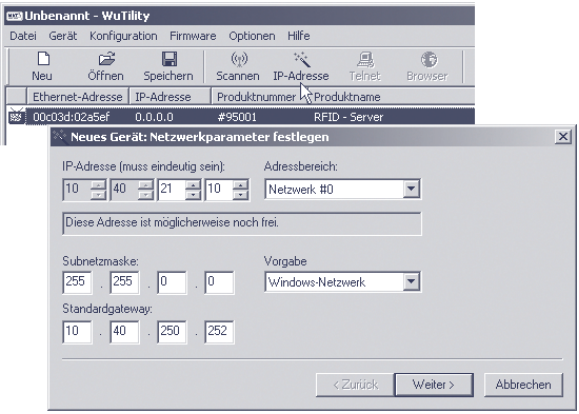
The RFID Server is powered by a regulated DC voltage of 12V/ +/-5%. Connect the power supply (observe polarity) to the plug-in screw terminal.



Network installation

The network connection to the hub or switch is made using a 1:1 RJ45 cable. The default setting is for the DHCP client of the RFID Server to be activated, so that the IP address, subnet mask and gateway are automatically handled in a corresponding network environment.

In network environments without DHCP, first install the Windows tool *WuTility* from the included product CD and start it on a PC which is in the same subnet as the RFID Server. Highlight the RFID Server in the list displayed, then click on the *IP-Address* button and follow the instructions in the dialog box.



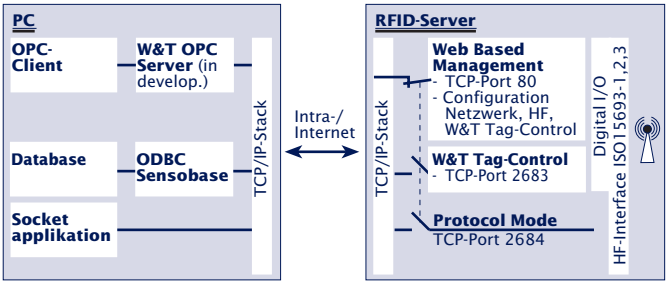
After assigning the IP address, the RFID Server starts W&T Tag-Control mode and operates using the set filter rules. In the default setting capture and loss of every tag is acknowledged with a short audible tone. If a TCP clent is connected to the W&T Tag-Control server port, the latter receives a data packet of type 0x300 (Direct Filtermatch).

The entire remainder of the RFID Server configuration including automatic antenna tuning is done using Web Based Management and a standard Internet browser.

To attain the maximum antenna range, you must after startup or a reset calibrate the HF interface to the default settings at the installed location using Web Based Management.

1.2 System overview

The RFID Server is a midrange, complete system for processing ISO15693 conformal transponders operating at 13.56 MHz. The central communications interface of the RFID Server is the network connection, which provides TCP server services for capturing and processing ISO15693 conformal transponders and for configuring the system from an Internet browser.



Web Based Management mode (Default-Port TCP 80)
The entire configuration of network and HF parameters as well as of the individual modes is done using a standard Internet browser. During an active configuration session the RFID Server is not able to process transponders. The TCP servers for *W&T Tag-Control* as well as *Protocol Mode* are deactivated.

W&T Tag-Control mode (Default-Port TCP 2683)
W&T Tag-Control is the standard operating mode for capturing and processing RFID tags. Including collision detection and handling, the RFID Server independently handles the complete processing of the HF protocol for the ISO15693 standard. Capture and loss of transponders represent events which pass through pre-configured filter chains. A result of this pre-filtering can be for example the sending of a time-stamped TAG-ID to a network application. In addition, regardless of any existing network connection, you can also directly switch the digital outputs, thereby enabling fully autonomous offline operation of the RFID Server.

Der Modus W&T Tag-Control wird von allen W&T RFID-Tools genutzt.

Protocol Mode (Default-Port TP 2684)
As an alternative to use of the W&T Tag-Control mode, protocol mode offers the possibility of transparent access to the commands from the ISO15693-3 standard. The network-side application must initiate the start of the inventory cycles as well as take over collision handling for multiple tags captured at the same time.

Detailed information about the individual operating nodes can be found in the corresponding sections of this Manual.

1.3 Factory default settings

The list contains an overview of the main factory default settings. Detailed information about the individual parameters and their configuration can be found in the corresponding sections of this Manual:

Network parameters

Hardware connection:	Auto-Negotiating
IP-Address:	0.0.0.0
Gateway address:	0.0.0.0
Subnet mask:	255.0.0.0
DHCP protocol:	active

To prevent unintended address assignments or address changes, we recommend deactivating DHCP and BOOTP protocols unless these are expressly used in the respective network environment.

Passwords

System and user password are empty.

HF interface

Mode:	W&T Tag-Control
Filterset 1:	Active (audible signal when a tag is lost)
Filtersets 2-8:	Deactivated

TCP-Ports

Web Based Management:	80
W&T Tag-Control:	2683
Protocol-Mode:	2684

To attain the maximum antenna range, you must after startup or a reset calibrate the HF interface to the default settings at the installed location using Web Based Management..

2 Assigning the IP Address

The RFID Server is factory set to IP address 0.0.0.0. Before assigning an address, you must obtain an appropriate IP address from your system administrator. In smaller, non-routed networks you use the IP address of your PC and simply change the last place. Always note however that IP addresses must be unique within the network.

- Assigning the IP address, subnet mask and gateway address using the *WuTility* management tool
- IP assignment using the ARP command
- Setting the IP address, subnet mask and gateway address using DHCP-/ BOOTP protocol
- IP assignment via RARP protocol

2. *Configuring the network parameters using WuTility*

The Windows tool *WuTility* version 3.0 or higher allows inventorying of all W&T network devices as well as convenient assignment/changing of the following network-side basic parameters for the RFID Server:

- IP address
- Subnet mask
- Gateway address
- Activating/deactivating BOOTP/DHCP

Assignment requires that the PC and RFID server be located in the same network. Any set system password must be known.

Download and installation of *WuTility*
WuTility is contained on the product CD and can be installed directly from there. The most current version is also published on our Web pages at the following address:

http://www.wut.de

From there the simplest way to navigate is using the menu tree on the left side:

Accessories: Downloads → RFID-Server

After extracting the program from the ZIP file, install by double-clicking on the file *setup_de.exe*. To start *WuTility* go to

Start → Programs → W&T Software Toolkit → WuTility

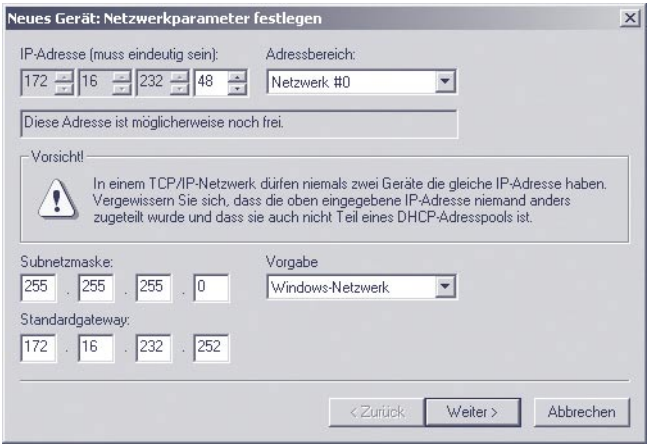
Starting the assignment dialog
Be sure that both the RFID Server and the computer you are using are connected to the network and are located in the same subnet. At the start *WuTility* automatically searches the local network for connected W&T network devices and generates an

inventory list. This search procedure can be repeated manually as often as desired by clicking on the *Scan* button:

Within the inventory list you can identify the desired RFID Server based on its MAC address. At initial installation this IP address is always 0.0.0.0.

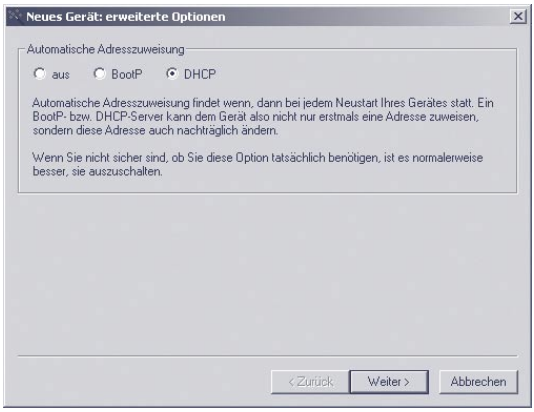
Select the RFID Server and then click on the *IP address* button:

In the fields in the following window enter the desired values for the IP address, subnet mask and gateway address and click on *Next*.



Each IP address must be unique within the network.

In the following dialog box you can activate and deactivate the DHCP- and BOOTP/RARP client of the RFID Server.



To prevent unintended address assignments or address changes, we recommend deactivating DHCP and BOOTP protocols unless these are expressly used in the respective network environment. RFID Servers with an incorrectly assigned IP address can be conveniently found later and reconfigured using the scan function of the WuTility *managemen tool.*

Click on the *Next* button assigns the network parameters to the RFID Server. All the columns in the device list in WuTility are filled with information.

This concludes network-side startup of the RFID Server. The entire rest of the configuration is doine using a standard Internet browser. From WuTility you do this by clicking on the *Browser* button:

Changing the network parameters is protected by a system password. To prevent unauthorized access, we recommend assigning a system password for any RFID Servers in use.

Additional information can be found in the section *General Configuration.*

2.2 Assigning the IP using the ARP command

This method can only be used if the RFID Server does not yet have an IP address, i.e. the entry is 0.0.0.0. To change an IP address use one of the other methods described in this section, or use the Web Based Management for the device.

An additional prerequisite is a computer which is located in the same network segment as the RFID Server and on which TCP/IP protocol is installed. Read off the Ethernet address of the RFID Server from the sticker on the front of the housing:

Now use the following command line from the ARP table of the computer to insert a static entry:

```
arp -s [IP address]  [MAC-Address]
```

Example under Windows:

```
arp -s 172.16.231.10 00-C0-3D-00-12-FF
```

Example under SCO UNIX:

```
arp -s 172.16.231.10 00:C0:3D:00:12:FF
```

Finally, use the following command line under *Start → Run* to ping the RFID server with the desired IP address:

```
ping [IP address] [Return]
```

In Windows environments the IP addresses may only be entered without leading zeroes. Otherwise the system incorrectly interprets the entry and the RFID Server is assigned an incorrect IP address.

The RFID Server takes the IP address from the first network packet sent to it as its own and saves it in non-volatile memory. Then the pings are replied to.

Each IP address must be unique within the network.

Older Windows systems accept a static entry only if a dynamic entry is already present. FIrst ping another network station.

The entire rest of the configuration is done from a standard Internet borwser. From WuTility you can do this by clicking on the *Browser* button.

2.3 IP assignment via DHCP protocol

Many networks use DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) or its predecessor (described in the following section) BOOTP for centralized and dynamic assigning of network parameters. The default setting here is for DHCP protocol enabled, so that in network environments with dynamic IP asignments you only need to connect the RFID Server to the network. The following parameters can be assigned using DHCP:

- IP address
- Subnet mask
- Gateway address
- Lease time

To prevent unintended address assignments or address changes, we recommend deactivating DHCP, BOOTP and RARP protocols unless these are expressly used in the respective network environment. RFID Servers with an incorrectly assigned IP address can be conveniently found later and reconfigured using the scan function of the WuTility *management tool.*

2.3.1 Activating/deactivating DHCP

DHCP protocol is activated by default. To deactivate it or later reactivate it, the following options are available.

- **Management-Tool WuTility**
  In the device list select the desired RFID Server and click on the *IP address* button. In the first dialog box enter the new network parameters for assignment and then click on *Next*. In the following dialog box deactivate the options *BOOTP* and *DHCP*. Clicking on *Next* sends the new configuration data to the RFID Server.

- **Web Based Management**

In the menu path *Home → Config → Device → Network* you can activate and deactivate the protocols individually.

2.3.2 System Name

To support possible automated updating of the DNS system by the DHCP server, the RFID Server identifies itself with its system name within the DHCP protocol. In the default setting this is *RFID-Server* followed by the last three places of the Ethernet address. For example, the default system name of an RFID Server with Ethernet address 00:c0:3d:01:02:03 is *RFID-SERVER-010203*. The system name of the RFID server can be changed from menu path *Home → Config → Device → Network*.

2.3.3 Lease-Time

The lease time determined and sent by the DHCP server specifies the validity time of the assigned IP address. After half the lease time has expired the RFID Server attempts to extend the validity with the assigning DHCP server and to update the address. If this is not possible by when the lease time expires, for example because the DHCP server can no longer be reached, the RFID Server deletes the IP address and starts a cyclical search for alternate DHCP servers for the purpose of assigning a new IP address.

After the restart there is an update prompt to the original DHCP server. If it is not reachable at this time, the RFID server deletes the IP address and starts a cyclical search for alternate DHCP servers.

If DHCP is enabled, the remaining lease time together with the current IP address is displaced in the submenu *Home → Config → Device → Network* of the Web configuration.

If after the assigned lease time has expired the DHCP server cannot be reached, the RFID Server deletes its IP

address. All existing TCP connections between the RFID Server and other network stations are aborted by this. To prevent disturbances of this kind, we recommend configuring the lease time in the DHCP server to infinite.

2.3.4 Reserved IP addresses

As a TCP server, the RFID Server provides services which other clients in the network can make use of as needed. To open connections, they of course need the current IP address of the RFID Server, so that in such cases it makes sense to reserve a particular IP address for the RFID Server on the DHCP server. In general this is done by linking to IP address to the worldwide unique Ethernet address of the RFID Server, which can be found on the sticker on the front of the housing.

2.3.5 Dynamic IP addresses

Fully dynamic address assignment, in which the RFID Server gets a different IP address after every restarwt or after the lease time expires, only makes sense in network environments with automated cross-linking between the DHCP and DNS services. THis means when an IP address is newly assigned to the RFID Server, the DHCP server automatically updates the DNS system as well. The new IP address is thereby associated with the respective domain name. For detailed information in this regard pertaining to your network environment, check with your system administrator if in doubt.

2.4 IP assignment via BOOTP protocol

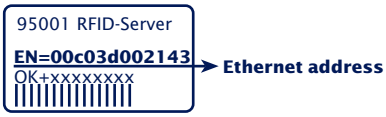
Many networks use for centralized and dynamic assignment of IP addresses BOOTP, the predecessor of DHCP protocol. The default setting for the RFID Server is for BOOTP disabled. It can be activated as part of the IP assignment using *WuTility* and the configuration tool *RFID-Explorer*. The following parameters can be transmitted:

- IP address
- Subnet mask
- Gateway address

To prevent unintended address assignments or address changes, we recommend deactivating DHCP, BOOTP and RARP protocols unless these are expressly used in the respective network environment. RFID Servers with an incorrectly assigned IP address can be conveniently found later and reconfigured using the scan function of the WuTility *management tool.*

2.4.1 Address reservation

BOOTP protocol is based on fixed reservations of fixed IP addresses for particular Ethernet addresses. This means an RFID Server connected to the network oinly gets an IP address if the address was previously stored in the BOOTP server. To create the reservation, contact your responsible system administrator. The required Ethernet address can be found on the sticker on the front of the housing.



After the administrator has made the necessary entries, the RFID Server obtains the desired IP address after every reset. To ensure that the RFID Server is accessible even if the BOOTP server goes down, the previous IP address is retained should there be no response.

2.5 IP assignment using an RARP server

UNIX environments especially often use RARP protocol for centralized assignment of IP addresses. TCP/IP devices that want to obtain an IP address send RARP requests with their Ethernet address over the network as a broadcast.

Activate the RARP server on the UNIX system and in the file */etc/ethers* enter the Ethernet address of the RFID Server and enter the IP address in the file */etc/hosts*.

The RFID Servger must be located in the same subnet as the RARP server.

Example
Your RFID Server has MAC address EN= 00C03D0012FF (sticker on the unit). You want it to get IP address 172.16.231.10 and the alias WT_1:

- Entry in the file */etc/hosts*:
  `172.16.231.10WT_1`
- Entry in the file */etc/ethers*:
  `00:C0:3D:00:12:FF WT_1`

RARP broadcasts are generated by default after every reset of the RFID Server. The reply from an RARP server overwrites the current IP address of the RFID Server. We therefore recommend deactivating the DHCP and BOOTP/RARP protocols unless they are specifically needed. To do this, use the function *IP address* in *WuTility*. You can also deactivate BOOTP/RARP using the Web configuration in the submenu *Home → Config → Device → Network*.

3 Installation and Antenna Tuning

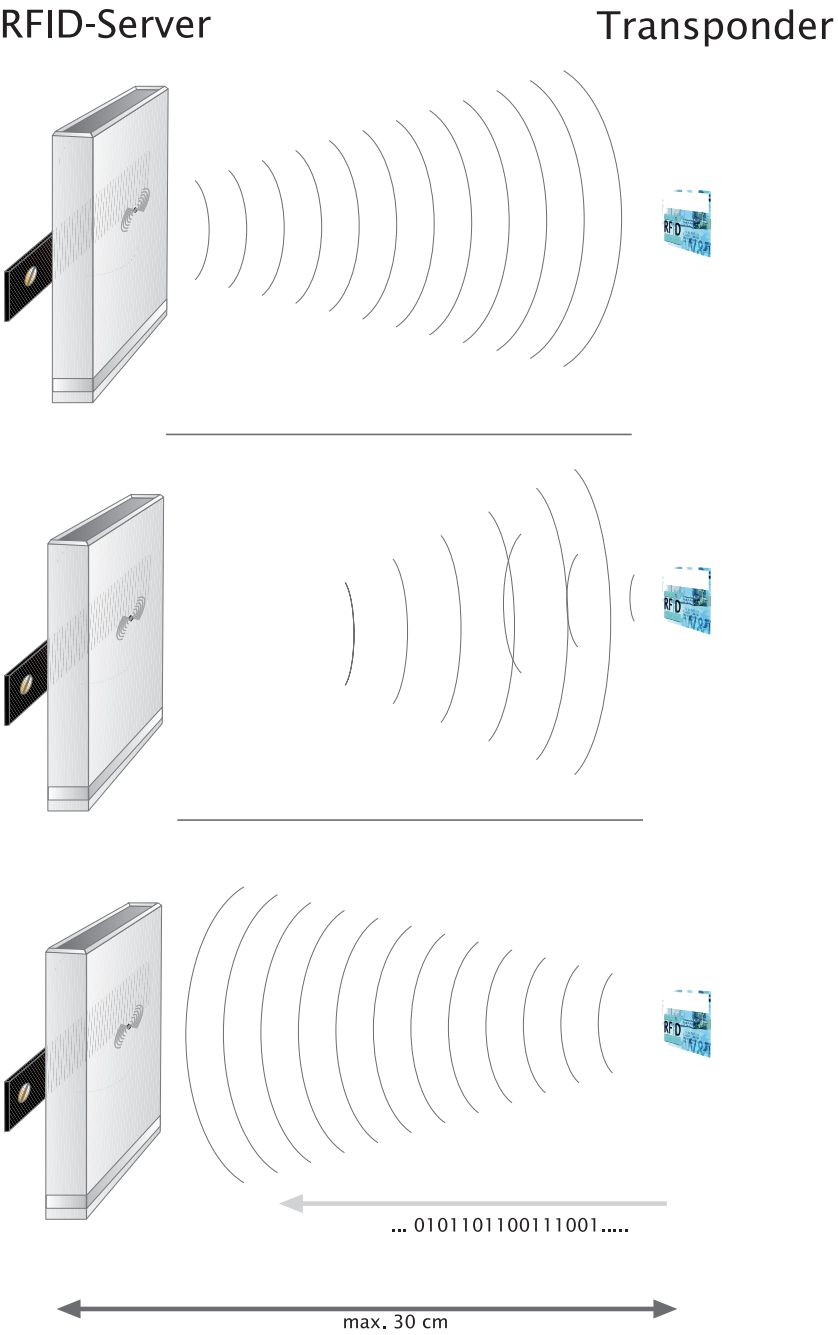
- Installation and operating environment
- Antenna orientation
- Antenna tuning

3.1 Installing the RFID Server

The RFID Server is suitable for use either as a tabletop device or, using the optional installation kit (95201) for wall mount. The integrated antenna of the RFID Server is located below the correspondingly marked housing sidse. To achieve the greatest possible capture range the antenna side should be oriented in the read direction.

When selecting a location, simply avoid direct proximity (<15cm) to *closed* metal surfaces. Non-closed metallic structures such as in steel reinforced concrete or drywall are compensated by calibrating the RFID Server.

To ensure trouble-free air circulation, the ventilation slits on the front sides of the housing should not be covered.


RFID-Server
Transponder
RFID
RFID
RFID
... 0101101100111001.....
max. 30 cm

3.2 Antenna tuning

Optimum adaptation to the local magnetic environment requires tuning of the integrated antenna. After initial startup in the respective environment, this initial tuning is done using the RFID Server Web configuration. Detailed information can be found in section *WBM - General Functions*.

During tuning no tags are allowed in the capture range of the RFID Server. You may have to repeat the tuning after removing the tag(s).

For alter productive continuous operation in W&T Tag-Control mode, it is also possible to enable a cyclical, automatic tuning procedure. This prevents changes in the magnetic surroundings or significant fluctuations in the ambient temperature to have a negative effect on the capture range.

If operation in a non-tuned state continuous exceeding of the permissible ambient temperature of 50°C results in overheating of the HF final stage, the RFID Server will turn the latter off. In W&T Tag-Control mode this is indicated by flashing of the *MODE* LED. Applications associated with the network side receive a corresponding error packet. After cool-down the RFID Server performs an automatic retuning and attempts to restart the set W&T Tag-Control or protocol mode.

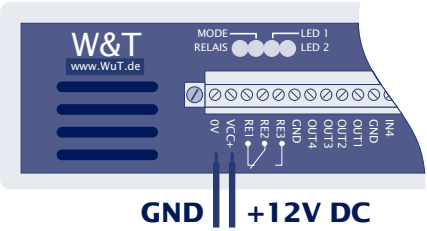
During an automatically or manually initiated antenna tuning the RFID Server will be unable to capture tags for approx. 2s.

4 Connections and Indicators

- Supply voltage
- The network connection
- Digital in-/outputs
- LED indicators

4.1 Supply voltage

The supply voltage for the RFID Server comes in at the 16-position screw terminal on the front side of the housing with the following polarity:

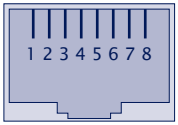


The supply voltage must be 12V DC +/-5%.

To maintain the EMC Directives a ferrite ring must be installed in the incoming line of the supply voltage for the RFID Server (included in the scope of delivery). The supply voltage cable must be wrapped through the ferrite ring at least 4 turns. The ferrite ring as well as the plug-in screw terminal are already pre-assembled with the optional W&T model 11083 AC adapter.

4.2 Network connection

The RFID Server has an IEEE 802.3 compatible network connection on a shielded RJ45 connector. The pin configuration corresponds to an MDI interface, so that the connection to the hub is made using a 1:1 shielded patch cable.



Pin	Direction	Function
1	Out	Tx+
2	Out	Tx-
3	In	Rx+
4	--	nc
5	--	nc
6	In	Rx-
7	--	nc
8	--	nc

Auto Negotiation

The RFID Server uses *Auto-Negotiation* on the network side. Baid rate and duplex procedures are automatically negotiated with the connected switch/hub and set accordingly. In modern infrastructures the result is generally 100BaseT/Full-Duplex.

If in managable environments the RS45 port of the respective needs to be fixed for a ceratin mode, half-duplex must be configured.

Galvanic isolation

The network connection is galvanically isolated with respect to the power supply to at least $500V_{rms}$.

Link-Status

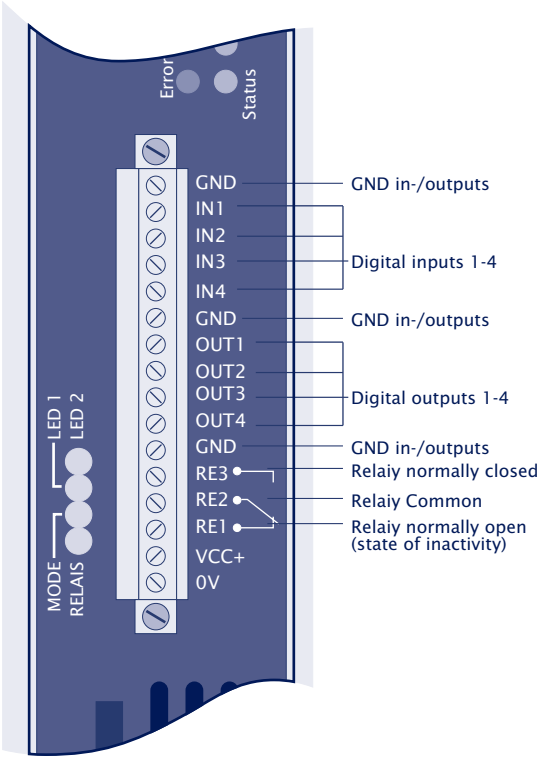
The *Error*-LED on the front of the device indicates the current link status. If it flashes at 1-2 second intervals, there is no connection to the hub or the connection is faulted.

Manageable switches often have speciual protocols (Spanning Tree Protocol, Port-Trunking, ...), as they are required for example for uplinks to other switches or for broadband connection of servers. These protocols are generally not required for connecting normal terminal devices like the RFID Server, and may only significantly delay the opening of communication after a restart. We recommend disabling these protocols and functions on the port used for the RFID Server. Please get in touch with your responsible network administrator.

4.3 Digital in-/outputs

The RFID Server has four digital in- and outputs each with a common reference potential. Galvanic isolation with respect to supply ground is provided by optocouplers. Furthermore a potential-free relay switchover contact is available. All signals are brought to the plug-in screw terminal located on the front of the housing.

In *W&T Tag-Control* mode the in- and outputs are accessed either autonomously by the device-specific filter rules or by the external network side application. Detailed information about this can be found in the section *W&T Tag Control Configuration* and *W&T Tag-Control - Network Protocol.*

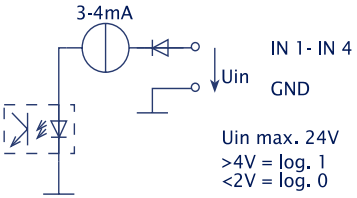


4.3.1 Digital inputs

The RFID Server has four digital inputs with the following characteristics:

- Input voltage: 0-24VDC
- Input current: 3-4mA (sourcing)
- Switching threshold: 3V +/-1V
  (OFF: < 2V / ON: > 4V)

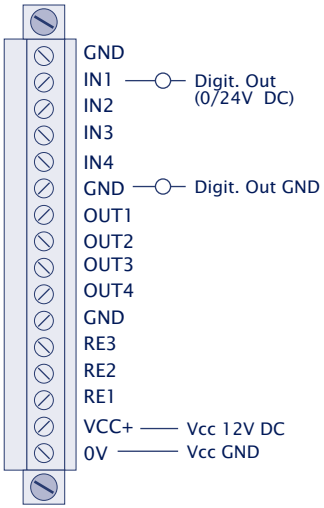
Basic schematic



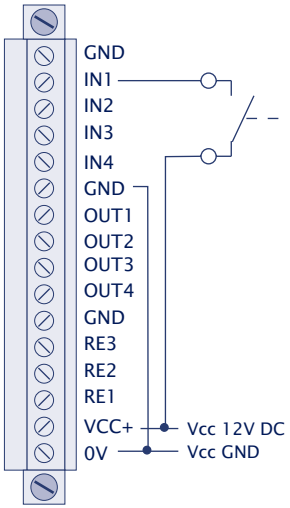
At an input voltage of >4V the input is set to ON on the network side. A voltage of < 2V corresponds to the OFF state.

Wiring example

Connection example for voltage outputs



Connection example for potential-free contacts

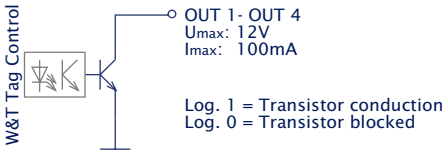


4.3.2 Digital outputs

The RFID Server provides four digital outputs (open-collector) for driving external relays, indicators, etc. Their characteristics are as follows:

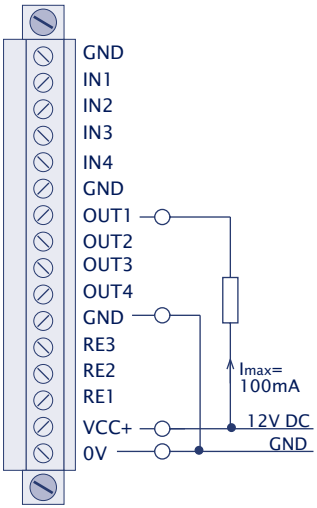
- Voltage range: 0-12VDC
- max. switching current: 100mA
- Internal resistance: < 17Ω

Basic schematic

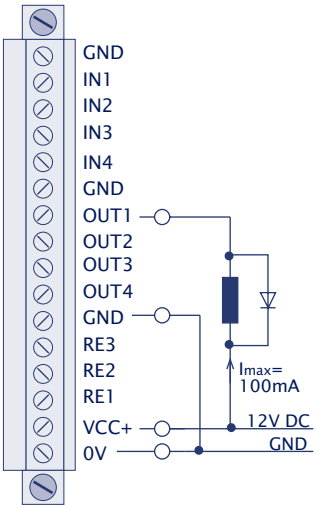


Wiring example

Connection example with resistive load (z.B. semiconductoir relay)



Connection example with inductive load (z.B. relay coil)

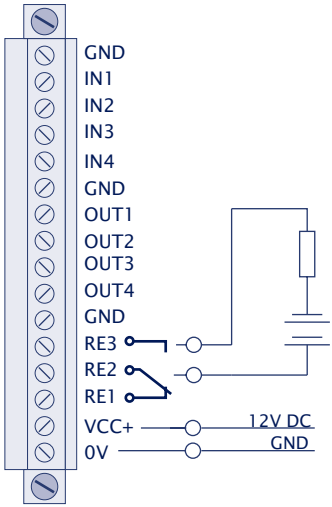


4.3.3 Relay output

For potential-free switching of external consumers the RFID Server has, in addition to the open-collector outputs, a relay with a changeover contact.

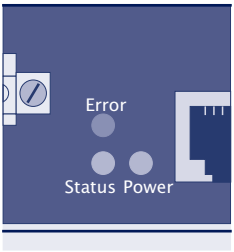
- max. permissible switching voltage: 48V DC
- max. switching current: 2A
- max. switching frequency: 1800/hour (1s=ON 1s=OFF)

Wiring example
Connection example Relaycontact



4.4 LED indicators

4.4.1 Power and network status



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

- **Status**
  This flashes whenever there is network activity with the RFID Server. Periodic flashing indicates that there is a coinnection to a client in the network.

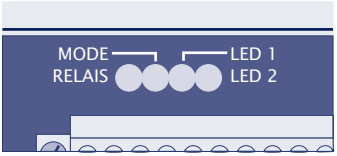
- **Error**
  The Error-LED indicates the link status of the Ethernet connection. If the RFID Server has properly connected to a hub or switch, the Error LED is constantly off. If the RFID Server does not receive valid link signals, this is indicated by periodic flashing. Possible causes of this are...

  ... Incorrectly wired patch cable or RJ45 sockets
  ... Missing connection of the RJ45 socket on the switch
  ... Cable break
  ... Switch or hub turned off

  Constant illumination of the Error-LED indicates an incorrectly finished self-test of the TCP/IP stack. The RFID Server is no longer operable in this state. If the error occurs due to a prematurely aborted firmware update, restart the update using the old IP address. If the problem cannot be

resolved or should it occur in connection with a preceding firmware update, please return the unit to us for inspection.

4.4.2 RFID status



- **MODE**
  The Mode-LED indicates the current mode of the RFID Server as well as the status of the HF module responsible for capturing tags.

  MODE-LED = ON
  The RFID Server is in *W&T Tag-Control* mode and is ready to capture tags using any filter rules stored in the Setup.

  MODE-LED = Flashing
  The RFID Server is in *W&T Tag-Control* mode, but the HF module was automatically turned off due to excessive temperature. In this state no tags can be captured. The possible causes for this are...

  ... Longer operation without previously tuning the internal antenna
  ... Longer operation at too high an ambient temperature (> 50°C)
  ... SIgnificant change in the electromagnetic surroundings after tuning the internal antenna

  MODE-LED = OFF
  An Internet browser has logged on to the WBM configuration. No tags can be processed. The TCP services *W&T Tag-Control* as well as *Protocol-Mode* are stopped.

- **RELAY**
  The Relay LED indicates the current status of the internal relay. If the LED is not on, the relay is in the rest state. If the LED is continuously on, the relay is energized. The assignments for which contact is closed in the respective state can be found o the housing label.

- **LED1 and LED2**
  The functions of LED1 and LED2 can be configured using *Actions* of the filter rules in W&T Tag-Control mode. By default the LEDs have no function.

5 Web-Based-Management - Basics

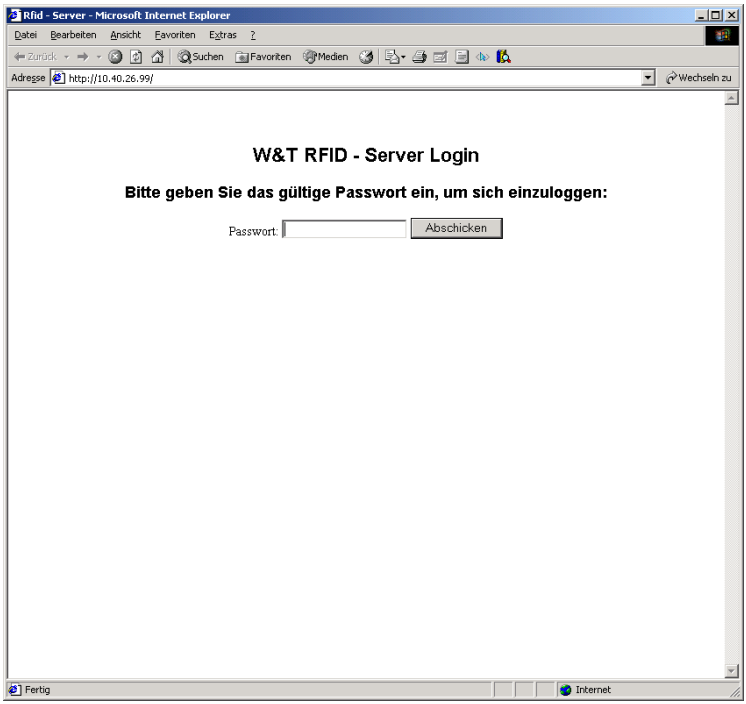
After connecting the hardware and assigning the IP address, the entire rest of the RFID Server configuration is done over the network using the device-internal Web server and a standard Internet browser.

- Navigation on the Web pages
- Structure of the Web pages
- Receiving the applying the settings

5.1 Starting Web Based Management

The entire configuration of the RFID Server is done using the integrated Web server of the RFID Server. This **W**eb-**B**ased-**M**anagement allows all the settings to be made using a standard Internet browser - regardless of the operating system of the respective computer.

Entering the IP address or URL of the RFID Server in the address bar of the browser takes you to the WBM start page. Alternately you can also click on the *Browser* button in WuTility.



After a successful login to the WBM of the RFID Server all further Web pages are divided in two. The left side always contains the navigation frame which you could compare with the table of contents of a book. At right is the display and configuration frame.

5.2 Web Based Management - Login and navigation

WBM access is session-based and protected by the system password which must be entered on the start page. The default is for no system password, and the corresponding field can be left empty. If a system password was set as part of the configuration, it must be entered on the start page before clicking on the *Send* button.

D The start of a WBM session results in TCP connections to applications which process the tags being closed. A new connection to the W&T Tag-Control and protocol mode services cannot be opened until the WBM session has been quit.

Simultaneous access to the WBM of the RFID Server by multiple computers is not *possible. If a WBM session is active, the attempt to open a connection is rejected by a second computer.*

Login Timeout
If no entry is made for longer than 40 seconds, the RFID Server independently quits the current WBM session and you must log in again. All entries and changes on the current configuration page are cancelled.

5.2.2 Navigation

The navigation frame contains a directory tree in which all available menu points for the RFID Server are listed by categories. Clicking on the individual elements displays additional menu points for a category and/or creates a new content in the configuration frame.

Avoid using the Forward *and* Back *buttons of your browser. For navigation use only the navigation tree and the buttons and links from the WBM. Otherwise parameters buffer-saved in the background may be lost when skipping forward or back.*

The icons in the menu tree have the following meanings:


Main or sub-category with branches to additional contents. Clicking on this icon expands the menu tree.


Main or sub-category with branches to additional contents. Clicking on this icon expands the menu tree and displays a new content in the configuration frame.


Indicates that additional sub-categories or contents are available. Clicking on this icon expands the menu tree but does not change the content of the configuration frame.


Clicking on this icon closes the expanded directory tree.


Indicates a configuration page which is displayed by clicking in the configuration frame.

5.2.3 Saving and activating the settings

All entries and changes on a Web page are first simply buffer stored by the browser.

To save the settings in the RFID Server, cancelling changes or to quit a WBM session, the configuration pages provide three buttons.

Speichern

The settings made on the respective page are sent to the RFID Server and saved there in non-volatile memory. When changes are made to the network-side basic parameters, the RFID Server then automatically restarts, and a new WBM session must be opened to make additional settings.

Rücksetzen

All changes made since opening the respective Web page are cancelled and returned to their original values. No parameters are sent to the RFID Server.

Logout

Ends the WBM session with the RFID Server. Any settings made on the respective Web page must *first* be saved using the *Save* button. Ending the WBM session automatically starts the set communication mode *W&T Tag-Control* or *Protocol Mode*, so that tag-processing client applicat4ions can connect to the RFID Server.

6 WBM - General Configuration

This section describes configuration of the basic parameters as well as diagnostics options.

- Session Control
  - Setting passwords
  - Device reset / factory defaults
- Device
  - Setting network parameters
  - Setting the system clock
  - Setting the operating mode
- Saving / restoring the overall configuration
- Diagnostics

6.1 Session Control

In additional to the possibility of resetting the RFID Server, the menu branch *Session Control* also contains the configuration page for passwords.

6.1.1 Session Control >> Reset ...

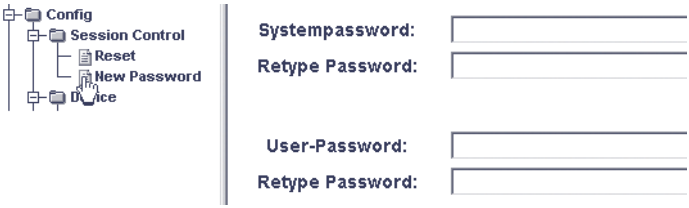
... Hardware Reset

Clicking on the *Hardware Reset* button has the same function as turning the RFID Server on and off. After the reset the RFID Server starts the configured mode *W&T Tag-Control* or *Protocol-Mode*.

... Restore Factory Defaults

The entire configuration of the RFID Server including the IP address is reset by clicking on the *Restore Factory Defaults* button. The IP address is then 0.0.0.0 and must be reassigned (see section *Assigning the IP Address*).

6.1.2 Session Control >> New Password ...



Accesses to the Web Based Management as well as to the data services for tag communication can be protected using two separate passwords. The passwords are not permitted to be identical and must differ from each other by at least one character.

The factory setting is for no system password and no user password. The entry field when starting the WBM may remain empty. After optning the TCP connection for *W&T Tag-Control* you do not need to send a user password.

After assigning the new passwords and clicking on the *Save* button, the RFID Server automatically performs a reset.

... System password

The system password protects the configuration and control accesses to the RFID Server indicated below. It is limited to a length o no more than 31 characters.

- WBM-Port (configurable, default = 80)
- Reset-Port (not configurable, 8888)

When accessing the WBM of the RFID Server you must enter the system password on the Web page. When using the reset port you must send the system password null-terminated ([password] + 0x00) no later than 2s after opening the TCP connection to the RFID Server (see *Resetting the RFID server over the network*).

... User Password

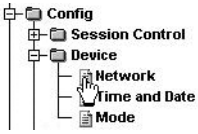
The user password protects network communication with *W&T Tag-Control* and *Protocol-Port* mode from unauthorized access. The password is limited to 31 characters.

Once you have made all your entries, click on the *Save* button. This sends the parameters to the RFID Server, which in turn automatically performs a restart.

6.2 Device

The menu branch *Device* contains the configuration pages for setting the network-side basic parameters, the integrated system clock as well as the mode for capturing tags.

6.2.1 Device >> Network



Config >> Device >> Network

IP-Address : 10.10.1.20

Subnetmask : 255.255.0.0

Gateway : 10.10.10.1

BOOTP bzw. DHCP kann nur verwendet werden, wenn ein entsprechender Eintrag im DHCP-Server eine reservierte IP-Adresse zuweist.
Wichtig:
Im Zweifelsfall 'BOOTP enable' und 'DHCP enable' abschalten!

BOOTP Client : ☐ BOOTP enable

DHCP Client: ☐ DHCP enable

Leasetime: 0 Minuten

HTTP-Config-Port: 80

W&T Tag Control Port: 2683

Protokoll-Port: 2684

Systemname: RFID - Server

MAC Adresse anhängen

Speichern Rücksetzen Logout

Once all the entries have been made, click on the *Save* button. The parameters are sent to the RFID server and a reset is automatically carried out.

IP Address

The IP address can be changed at this point. If the new IP address is nont located in the same subnet as that of the computer used for the configuration, the RFID Server may not be accessible after saving.

Each IP address must be unique within the network.

When incorrect entries are made - regardless of the current address of the RFID Server - you can always use WuTility *to change the IP address (see section* Assigning the IP Address*)*

Subnet Mask / Gateway

In routed network environments the appropriate subnet mask and the gateway IP address must be entered. Both parameters can be obtained from your system administrator.

BOOTP-/DHCP Client

To prevent unintended address assignment or address changes, we recommend deactivating BOOTP and DHCP protocols unless they are explicitly used in the respective network environment .

If the RFID receives its network parameters from a DHCP server, the remaining lease time is displayed (see section *IP assignment using DHCP protocol*).

WBM-Port

The port number for Web Based Management can be changed here. The default is HTTP standard port 80. If you set a different port number here, it must be specified in the address line of the browser when opening WBM (e.g. http://10.10.10.20:8080)

W&T Tag-Control Port

A client can access *W&T Tag Control* mode using the TCP port configured here. The default setting is port 2683 voreingestellt.

Protocol Port

A client can access *Protocol Mode* mode using the TCP port configured here. The default setting is port 2684 voreingestellt.

WBM-Port, W&T Tag-Control-Port and Protocol-Port must be different from each other. You may not use the same port numbers for different services.

System name

When multiple RFID Servers are in the same network, the system name allows the devices to be distinguished within the display of the inventorying tool *WuTility*. In addition, the system name is also used for identification with respect to a DHCP server.

To create a unique system name you can use the *Attach MAC address* button to add a special keyword (<wut1>). The RFID Server replaces this with the last six places (3 bytes) of the worldwide unique Ethernet address when using DHCP protocol.

6.2.2 Device >> Time and Date

The RFID Server has a realtime clock with date function. Time of day and date are factory set and can be changed on this configuration page. The clock is backed up by an internal battery, so that the set time remains intact even when the power supply is turned off.

Time
Enter the time of day in *hh:mm*.

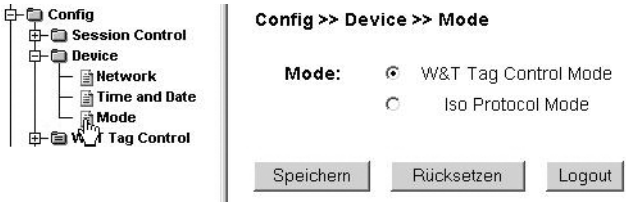
Offset
Offset of local time from UTC time. For German winter time the offset is +1 (= UTC+1). For summer time it is +2 (= UTC+2).

Day
Day in the date display, formatted *dd*.

Month
Month of the date display, formatted *mm*.

Year
Year, formatted *yy*.

6.2.3 Device >> Mode



FFor productive use and processing of tags the RFID Server provides two operating modes. After the unit is started up and after ending a WBM session the mode set here is automatically activated.

W&T Tag-Control Mode

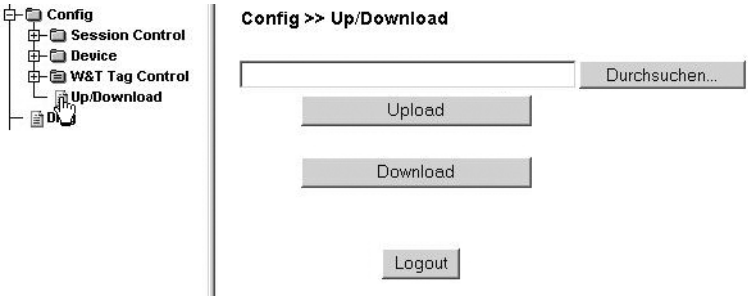
The cumbersome running of HF communication according to ISO15693 is fully taken over by the RFID Server. Capturing and loss of tags represent events which pass through filter rules set by the user. If a filter rule has been made use of, the result is that an action takes place. This can be for example switching an output or network-side sending of the event to a client (see section *W&T Tag Control - Configuration*).

Protocol Mode

In this mode the RFID Server operates more or less like a gateway between the network and the HF interface. All ISO15693-3 commands can be sent to the RFID Server over the network, and the Server then executes them on the HF interface. The network application must handle all tasks such as tage inventorying, collision handling, etc. (see section *Protocol Mode*).

By starting a WBM session the set operating mode is interrupted. No more tags are captured and any existing TCP connections to network clients are aborted. The set operating mode is started again as soon as the WBM session is quit.

6.3 Up-/Download - Configuration profiles



The RFID Server makes it possible for the user to download all the settings made in Web Based Management as a binary file or to upload saved settings.

Download

The entire configuration of the RFID Server is opened as a binary file. Thus the user can set the basic configuration on a unit for projects with multiple equally configured RFID Servers, read the configuration out and later upload it to the other devices.

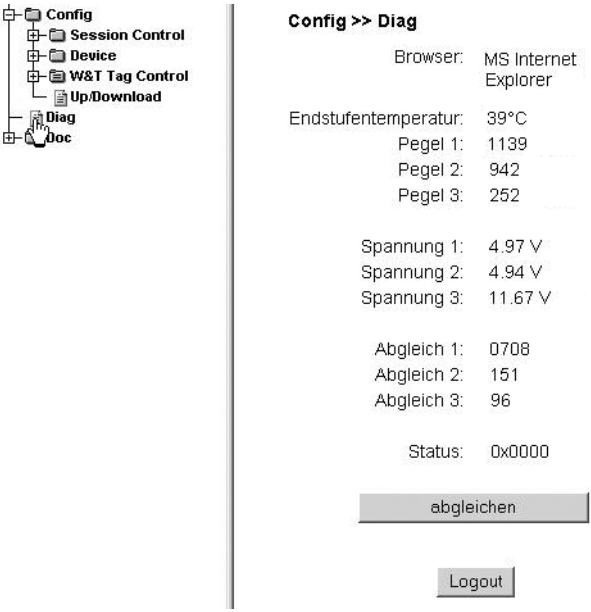
To open the configuration file, click on the *Download* button and save the file under the desired name.

Upload

To load a saved configuration into the RFID Server, use the *Search* dialog to select the desired file. Clicking on the *Upload* button starts transmission and the device then automatically restarts itself.

When sending binary files to an RFID Server, all *the settings contained in it* except *for the IP address are applied.*

6.4 Diagnostics and calibration



The diagnostics page of WBM allows you to manually tune the integrated antenna of the RFID Server. Tuning is necessary for example when the locat4ion of the RFID Server or its magnetic surroundings change.

For *W&T Tag-Control* mode, in addition to the manual antenna tuning described here you can also have an automatic tuning performed cyclically.

The output measurement values are internal circuit parameters which normally have no meaning for the user.

While tuning is taking palce no tags are allowed in the capture range of the RFID Server. It may be necessary to retune after removing the tag(s)..

7 W&T Tag-Control - Configuration

In this section the functionality and configuration of W&T Tag-Control mode is described.

- Structure
- Filters
- Tag-Listen
- Time Condition
- Input Condition
- Action
- Master (Filter set)

7.1 Structure of the W&T Tag Control

In *W&T Tag-Control* mode the RFID Server continuously scans its capture range. New recognition of a tag or loss of a tag both represent events which together with the individual tag IDare fed to the user-configurable *Filtersets*.

When the *Action* of a Filterset is set, the conditions - those which are set - are checked in sequence as follows, whereby the result is either *True* or *False*.

- Tag-Listen
  Is the detected tag included in the tag list?

- Time Condition
  Is the current time within the configured time window?

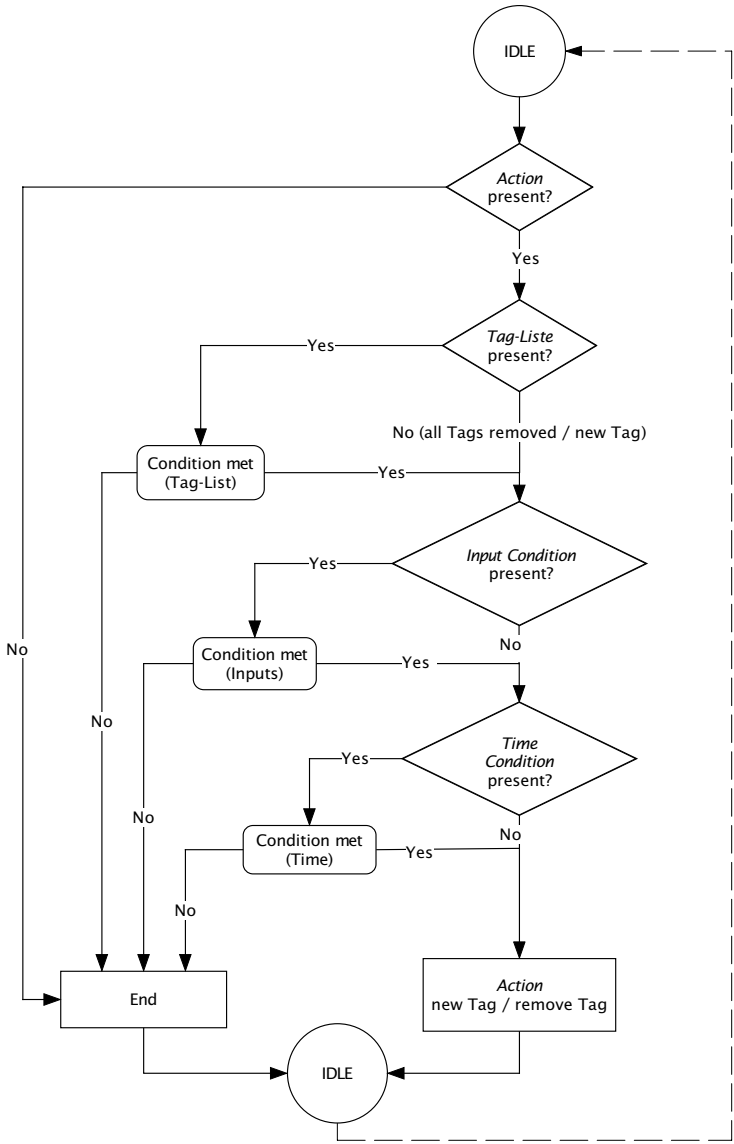
- Input Condition
  Does the current status of the digital inputs match the configured status?

If the result of one of these checks is *False*, the FIlterset is exited with no further action.

If all checks within a Filterset yield *True*, the Action configured by the user is executed. The following possibilities are available:

- Switch digital outputs
- Switch the relay
- Geneate acoustic signal from the integrated buzzer
- Save the events
- Send the tag ID with time stamp to a connected TCP client application.

The detailed decison process as run for every tag event can be seen in the following flow diagram.



Example

With the default setting *Filterset 1* is configured so that the capture and loss of *every* tag is acknowledged with a long and short audible signal. The following settings are provided on the configuration page of the Filterset:

Config >> W&T Tag Control >>MASTER >>Filterset 1

		beachten	ignorieren
TAG-List:	Liste 1 ☐	○	○
	Liste 2 ☐	○	○
	Liste 3 ☐	○	○
	Liste 4 ☐	○	○
	Liste 5 ☐	○	○
	Liste 6 ☐	○	○
	Liste 7 ☐	○	○
	Liste 8 ☐	○	○

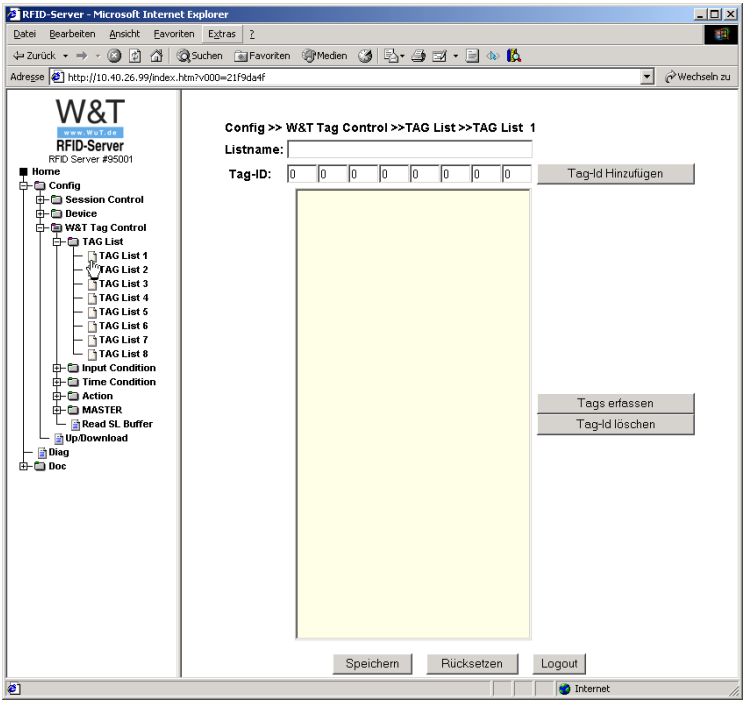
Input Condition:	-	
Time Condition:	-	
Action:	action 1	TAG kommt
	action 2	TAG geht

The conditions *Tag-List*, *Input Condition* and *Time Condition* are empty. Under Action *Action 1* (long tone) is configured for new capture of a tag and *Action 2* (short tone) for loss of a tag.

Details on the definition of the Filtersets and their conditions and actions are found in the following section.

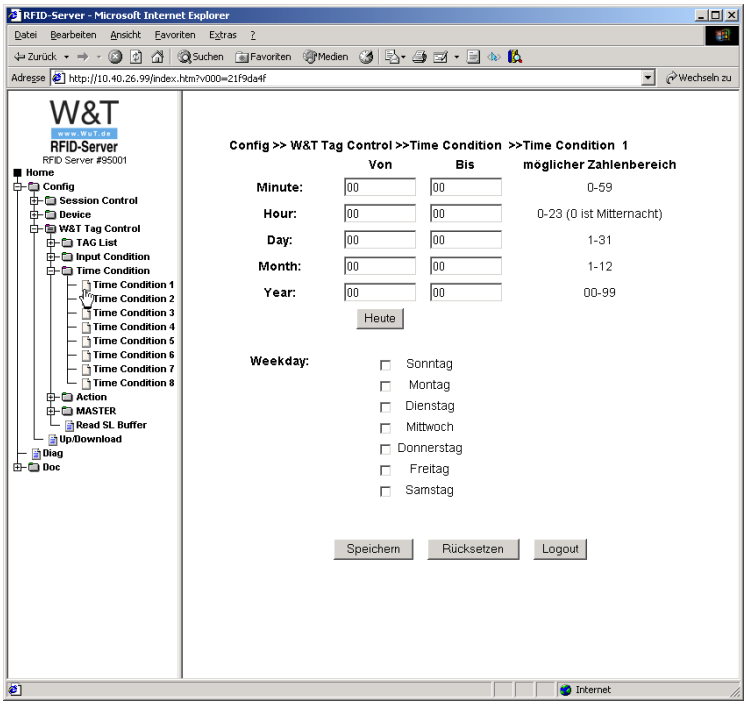
7.2 Filter TAG- Listen

Each tag has an individual ID consisting of 8 bytes which uniquely identifies the tag. This ID can be stored in a list to group the existing tags (e.g. Administators group). The lists can be described by a 20-character name to give each group an individual name.



7.3 Filter Time Condition

THe time limit allows for very flexible settings, ranging from a clearly limited rawnge (e.g. 12/12/2005 at 7:00 a.m. to 12/13/2005 at 5:00 p.m.) up to a cyclically repeating period (e.g. all day every Wednesday).



The filter has the following structure:

Start and Stop

- Year
- Month
- Day
- Hour
- Minute

optional weekday

Weekday

The entries Start and stop sepcify the start and end respectively of a time period. Optionally weekdays can also be specified for this period.

If in one of the elements year, month or day of the time period is not defined, it is always active starting with or from this time point! Thus if the start month is given as 05 and nothing is specified for the stop month, the period runs from 05 (May) until the end of the year (December).

Example:

Die Regel ist jedes Jahr zwischen dem 05.07. 08.00 Uhr und dem 06.07. 18.00 Uhr erfüllt.

	Year	Month	Day	Hour	Minute
Start	Leer	07	05	08	00
Stop	Leer	07	06	18	00
Weekday					empty

The rule is met each Saturday and Sunday between 8:00 a.m. and 6:00 p.m.

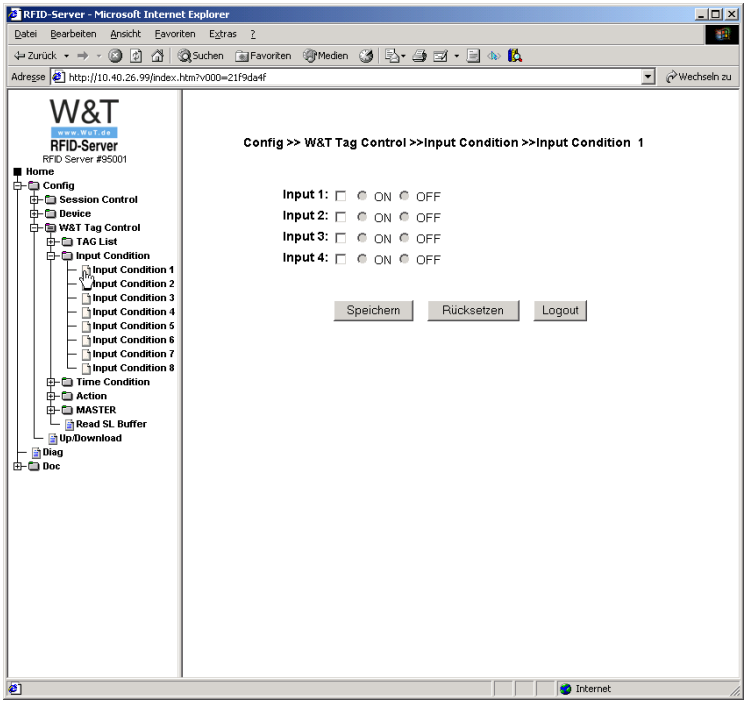
	Year	Month	Day	Hour	Minute
Start	Leer	Leer	Leer	08	00
Stop	Leer	Leer	Leer	18	00
Weekday				Saturday	Sunday

The rule is met every year starting with July on every Saturday and Sunday between 8:00 a.m. and 6:00 p.m.

	Year	Month	Day	Hour	Minute
Start	Leer	07	05	08	00
Stop	Leer	Leer	Leer	18	00
Weekday				Saturday	Sunday

7.4 Filter Input Condition

The logical state on an input can be used as a filter

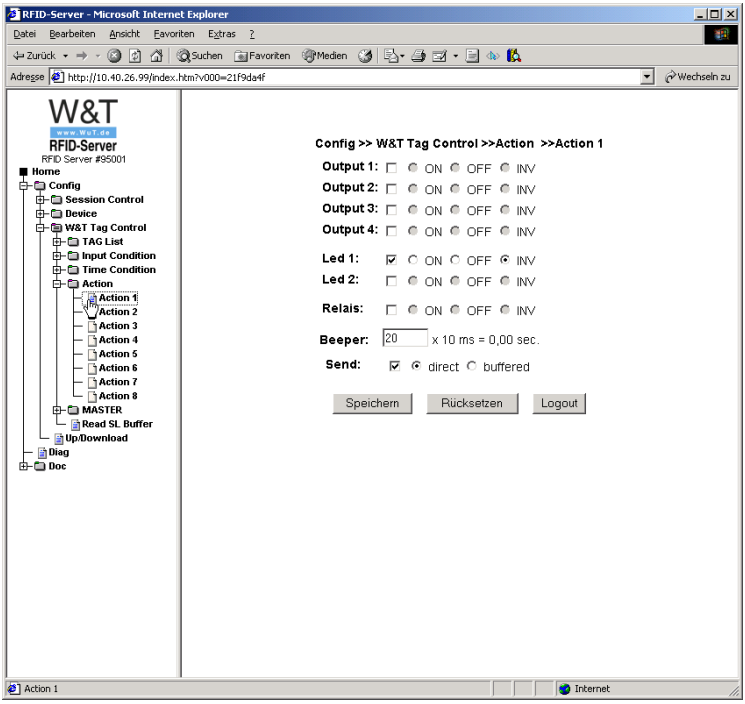


Each of the inputs can be used as a filter with the state „On“ or „Off“ if the input is wired

7.5 Actions

After a tag has passed through the filter and if it was not filtered out, various actions may be performed:

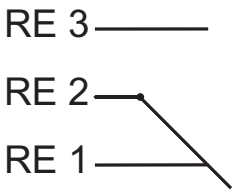
- Setting the digital outputs
- Setting LEDs 1 and 2
- Switching the relay
- Acoustic signal (buzzer)
- Report to client application



The actions can be executed when recognizing and/or leaving a new tag respectively in the capture range of the RFID Server (see *4.4 Filterset*). 8 freely configurable action lists can be defined.

If an action is performed out with the help of a tag, the digital outpouts and LEDs may be on, off or switched inverted respectively.

As an additional action the relay can be opened or closed



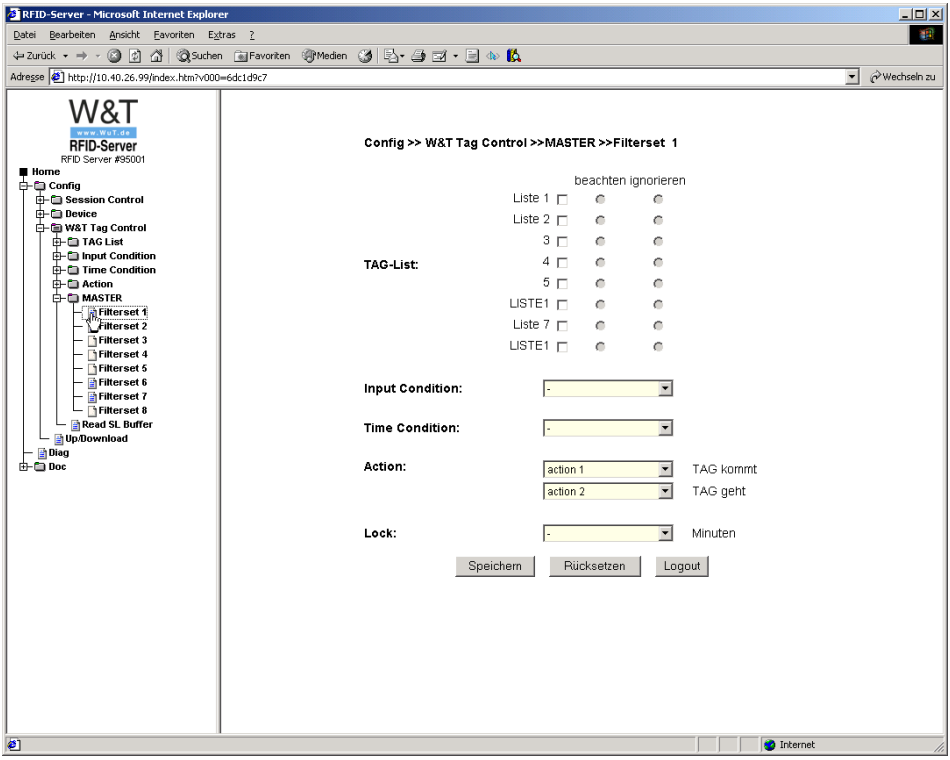
In addition, an acoustic signal using the buzzer can be generated for from 0.01 sec. to 2.55 sec.

The Send TAG Data option sends the current Tag-ID including the status and a time stamp as well as the Filterset number triggered by the tag.

The tag data can be sent directly, i.e. they are sent to the client immediately after triggering of the action. If at this time there is no network connection available, the message is lost. A more secure option is to buffer store the tag data in the unit. The data are then written to a ring buffer and must be explicitly (via command) read out of the buffer. An acknowledgement which must be sent by the client application is then used to delete the message from the ring buffer. If there is no message, the option „Send no data“ must be activated. This option generates no logging of the coming and going tags.

7.6 Master (Filterset)

FIlters and actions are specified in a Filterset. The filters are used for sorting the tags entering and exiting the capture area. Actions are only executed if the tag was not sorted out by the filters. Filtersets link the invidual filter elements of the W&T Tag Control to a function unit. A Filterset msut bontain **at least one action**, either for a coming or going tag.



A Filter set consists of 6 elements which can be combined as desired. It is comprised of four filters and one action for capturing a tag and an additional action for leaving the capture area of a tag.

- TAG-Listen filter
- Time limit filter

- State of the digital inputs
- Re-recogniztion filter

The „TAG-Listen“ filter is divided into two areas. Here the Tag-IDs combined into groups (see section 2.3) for processing in the W&T Tag Control can be allowed or ignored. The groups can be allowed or ignored in any combination. If the permitted list contains no group, all tag ID‘s are allowed**!**

If the tag list is given no entry, all RFID tags (any Tag-ID) are used for further processing!

Example:

List 1: Administrators

List 2: Customers

List 3: Employees

In the *Time Condition* filter time periods are specified during which the Filterset is active. If no time period is entered, this Filterset is always active.

As an additional filter condition the logical states of the four digital inputs can be used. These can be combined as desired.

The recapture time of a tag is set to zero in the basic setting. This means when a tag exits the capture area and immediately reappears, the tag is processed again. If a time greater than zero is set, this Tag-ID is blocked for the set time. Block times of from 9 to 255 min. can be set.

Actions can be executed when a tag enters or leaves the capture area of the RFID server. Each filter element consists of one of the 8 lists which was previously configured.

8 W&T Tag-Control - Network Protocol

In W&T Tag-Control mode the RFID Server provides a TCP server service which can be used with a simple binary protocol to read tag events. In addition, you can directly access the digital in- and outputs of the RFID Server. The following section describes the structure and individual commands of this protocol for implementation in your own applications.

- Data structures
- Capturing/losing tags
- Reading/writing user data on tags
- Reading/writing the digital in-/outputs
- Error handling

8.1 Basics of communication

In order to access the RFID Server from applications and get to the data, access via TCP sockets is possible. As already mentioned, the RFID Server provides a way to password-protect access.

The RFID Server offers a server socket on the TCP/IP data port (TCP-Port 2683), through which a client can connect. Communication takes place with only **one** active client per port. If an active connection is faulted, the RFID Server quits the connection and waits for a new connection opening.

Communication between the RFID Server and the client (PC) takes place through a TCP/IP socket.

The communication protocol is comprised of a transmission layer and an application layer. The transmissdion layer defines the form of data exchange between both communication partners and the application layer defines the command structure.

8.2 Opening a connection

To establish a TCP socket connection to the RFID Server the IP address, the corresponding TCP port on the device and any assigned user password are required.

If a password has been assigned, it must be sent within 3 seconds of opening the conneciton, otherwise the connection is immediately closed again. This password must be nul-terminated, i.e. it must be finnished with a zero byte (00). The IP address and the data port are configured in the network settings in Web Based Management.

The RFID Server returns „PASSWD?“ if the data password is incorrect, and immediately closes the connection.

Data exchange between the PC and RFID Server takes place using simple commands which are described in detail on the following pages.

8.3 Definition of the protocol structures

In order to be able to uniquely identify and process the contents of a packet, all the data must be sent to the RFID Server in the form of protocol structures.

All structures begin with the same header, which consists of two words (*send_sequence* and *req_sequence*). The two values are always 0 (00 00). This is followed by the command („*Command*“) which the RFID Server is supposed to execute and the *entire length* („*length*“) of the structure including the first 4 bytes. The header of a structure thus always consists of 4 words. The function parameters for a command are appended to the length specification („*length*“). They have a variable length (see Commands section) and must be included in the calculation for the overall length.

The following data structure applies to sending of data:

			2		4		6		8						
Structure	send_seq.		rec_seq.		command		length		Parameter						
Contents	00	00	00	00	22	03	08	00	00	00	.....	00	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High	Low				High
Variable type	Word		Word		Word		Word		Variable				

BYTE:	Unsigned number with a length of 8 bits	00
WORD:	Unsigned number with a length of 16 bits	00 00
LONG:	Unsigned number with a length of 32 bits	00 00 00 00

When sending and receiving, the following applies for all structure variables: ***Low-Byte first***

Example:

Output string from the RFID-Server

```
00 00 00 00 00 03 00 19 00 E0 04 01 00 0F 1E 41 F9 07 05 08 02 0B 1C 20 01
```

Structure head:

		2		4		6		8
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	00	03	19	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

Structure parameters:

8	10								18							25	26	
Action	Tag-ID								Timestamp							Filterset	Structure
00	E9	3F	0F	1E	E9	1E	00	04	20	1C	0B	02	08	05	07	01	Contents
	Low							High									Byte sequnce
Byte	8 Byte								7 Byte							Byte	Variable type

Structure:

From this you get command 03 00 and an overall structure length of 00 19 Bytes.

User data:

A tag was detected (*Action* 00) having ID E00401000F1E41F9.

The time stamp is comprised of 7 bytes.

Byte	Description	Hex	Example
1	Year	07	2007
1	Month	05	May
1	Day	08	8
1	Weekday	02	Tuesday
1	Hour	0B	11 hrs.
1	Minute	1C	28 min.
1	Second	20	32 sec.

This results in a time (11:28:32), a day of the week (Tuesday) and a data (5/8/07). Valid values for the year are in a range of from 0x00 (2000) tpo 0x63)2099). The day of the week begins with 0x00 (Sunday) and ends with 0x06 (Saturday).

The trigger for the packet was Filterset 01.

8.3.1 Filtermatch (0300)

The RFID Server outputs this structure when a tag enters or leaves its capture range and the direct sending action is enabled in the device configuration.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	00	03	19	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

	8	10							18							25	26
Structure	Action	Tag-ID							Timestamp							Filterset	
Contents	XX	XX	XX	XX	XX	XX	XX	XX	HH	MM	SS	DDDD	DD	MM	YY	XX	
Byte sequnce		Low						High									
Variable type	Byte	8 Byte							7 Byte							Byte	

The structure consists of a general section, which in turn is comprised of an initialization, the command to be executed, and the overall length of the structure. Then the actual user data come. These consist of:

- *Action*: A tag has been detected in the capture range (*Action* 01) or has left it (*Action* 00).

- *Tag ID*: The 8-character Tag ID

- *Timestamp*: A date stamp, accurate to the second. It is comprised of:

Byte	Description
1	Year
1	Month
1	Day
1	Weekday
1	Hour
1	Minute
1	Second

- *Filterset*: The number of the FIlterset triggered by the tag event.

8.3.2 Buffered Match (0301)

In order to initiate sending of all the events stored in the RFID Server, the following structure must be transmitted and set as an *Action* in the corresponding Filterset „buffered sending“.

			2		4		6		8
Structure	send_seq.		rec_seq.		command		length		
Contents	00	00	00	00	01	03	08	00	
Byte sequnce	Low	High	Low	High	Low	High	Low	High	
Variable type	Word		Word		Word		Word		

The RFID Server replies with the same structure as for a filter match. The RFID Server provides this structure for each tag event stored in the buffer:

			2		4		6		8
Structure	send_seq.		rec_seq.		command		length		
Contents	00	00	00	00	01	03	19	00	
Byte sequnce	Low	High	Low	High	Low	High	Low	High	
Variable type	Word		Word		Word		Word		

	8	10							18							25	26
Structure	Action	Tag-ID							Timestamp							Filterset	
Contents	XX	XX	XX	XX	XX	XX	XX	XX	HH	MM	SS	DDDD	DD	MM	YY	XX	
Byte sequnce		Low						High									
Variable type	Byte	8 Byte							7 Byte							Byte	

When the buffer contents is sent, the requested structure is send again as confirmation.

			2		4		6		8
Structure	send_seq.		rec_seq.		command		length		
Contents	00	00	00	00	01	03	08	00	
Byte sequnce	Low	High	Low	High	Low	High	Low	High	
Variable type	Word		Word		Word		Word		

The actual data consist of:

- *Action*: A tag has been detected within the capture range (*Action* 00).

- *Tag ID*: The 8-character Tag-ID

- *Timestamp*: : A date stamp, accurate to the second. It is comprised of:

Byte	Description
1	Year
1	Month
1	Day
1	Weekday
1	Hour
1	Minute
1	Second

- *Filterset*: The number of the FIlterset triggered by the tag event.

8.3.3 Clear Buffer (0302)

This structure is used for clearing the contents of the event buffer.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	02	03	08	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

The RFID Server confirms clearing with the same structure.

8.3.4 Buffer out of memory (030F)

The RFID Server sends the following structure only if its event buffer has overflowed ist (> 2990 events) and events have been lost.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	0F	03	08	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

8.3.5 Readflash (0320)

The following structure is used for reading the flash contents of a tag.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	20	03	14	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

8								18		20		22	
Tag-ID								Flash Addr.		Read Length			Structure
XX	XX	XX	XX	XX	XX	XX	XX	XX	00	XX	00		Contents
Low							High	Low	High	Low	High		Byte sequnce
8 Byte								Word		Word			Variable type

- *Tag ID*: The 8-chareacter Tag-ID

- *Flash Address*: The start address for reading.

- *Read Length:* The number of bytes to read.

The two tags supplied each have 128 bytes of memory, of which 112 bytes are available for user data and 16 bytes reserved for the Tag-ID.

The RFID Server replies with the same structure, which contains a status of the read request and the contents of the flash memory.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	20	03	XX	XX
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

8								18	19			∞	
Tag-ID								Status	Data				Structure
XX	XX	XX	XX	XX	XX	XX	XX	XX	00	....		00	Contents
Low							High		Low			High	Byte sequnce
8 Byte								Byte	n Byte				Variable type

- *Tag ID*: The 8-character Tag-ID

- *Status:* Result of the read operation:

Byte	Description
00	OK
01	no Answer
02	read Error
04	Busy

- *Data*: The actual data which were read.

To read, the complete ID of the tag in question is required, the start address (the address space is linear and begins at 0) and the number of bytes to read (max. 128 bytes).

*The **TAG data access** must be set in the configuration as required by the manufacturer!*

Example:

Send: 00 00 00 00 20 03 14 00 E9 3F 1E 0F 00 01 04 E0 00 00 09 00

This structure asks for the memory contents of the tag having ID E0 04 01 00 0F 1E 3F. Starting at address 0 (00 00) 9 bytes (00 09) should be read from the memory.

Rec.: 00 00 00 00 20 03 1A 00 E9 3F 1E 0F 00 01 04 E0 00 31 32 33 34 35 36 37 38 39

The RFID Server then sends this structure, which consists of the request from the command (03 20), the total length (00 1A) and the Tag ID (E0 04 01 00 0F 1E 3F E9). Next follows the status of the read operation (0) and the data which have been read (31 32 333 34 35 36 37 38 39).

8.3.6 Writeflash (0321)

The following structure is used for writing the tag flash contents.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	21	03	XX	XX
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

8							18	20		22				∞	
Tag-ID								Flash Addr.		Write Length		Data			Structure
XX	XX	XX	XX	XX	XX	XX	XX	XX	00	XX	00	00	....	00	Contents
Low							High	Low	High	Low	High	Low		High	Byte sequnce
8 Byte								Word		Word		n Byte			Variable type

- *Tag ID*: The 8-character Tag-ID

- *Flash Addresse*: The start address for writing.

- *Write Length:* The number of bytes to write.

- *Data*: The user data to write.

The two tags supplied each have 128 bytes of memory, of which 112 bytes are available for user data and 16 bytes reserved for the Tag-ID.

The RFID Server replies with the same structure, which contains a status of the write requeswt and the contents of the flash memory.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	21	03	XX	XX
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

8																									8
Tag-ID									Flash Addr.		Write Length		Data												Structure
XX	XX	XX	XX	XX	XX	XX	XX		XX	00	XX	00	00	....	00										Contents
Low							High		Low	High	Low	High	Low		High										Byte sequnce
8 Byte									Word		Word		n Byte												Variable type

- *Tag ID*: The 8-character Tag-ID

- *Status:* Result of the write operation:

Byte	Description
00	OK
01	no Answer
03	write Error
04	Busy

To write, the complete ID of the tag in question is required, the start address (the address space is linear and begins at 0) and the number of bytes to read (max. 128 bytes).

*The **TAG data access** must be set in the configuration as required by the manufacturer!*

Example:

8.3.7 Get IO (0322)

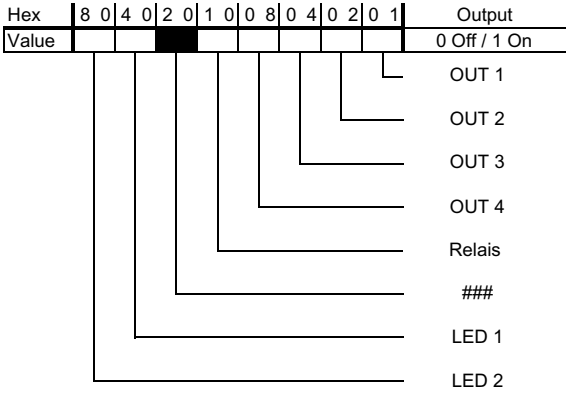
The following structure is used to get the status of the IOs.

	2		4		6		8	
Structure	send_seq.		rec_seq.		command		length	
Contents	00	00	00	00	22	03	08	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word	

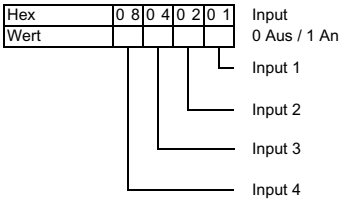
The RFID Server returns the status of the inputs and outputs in this structure.

	2		4		6		8		9	10
Structure	send_seq.		rec_seq.		command		length		Output	Input
Contents	00	00	00	00	22	03	0A	00	XX	XX
Byte sequnce	Low	High	Low	High	Low	High	Low	High		
Variable type	Word		Word		Word		Word		Byte	Byte

- Ouputs: All the digital outputs and the two LEDs are coded using this hex value. If the value is converted to binary, it can be translated using the following table.



- Inputs: All the digital inputs are coded using this hex value. If the value is converted to binary, it can be translated using the following table.



Example:

Outputs :	9	A
Binary conversion:	1001	1010
Switched:	LED 2, relay, Out 4, Out2	

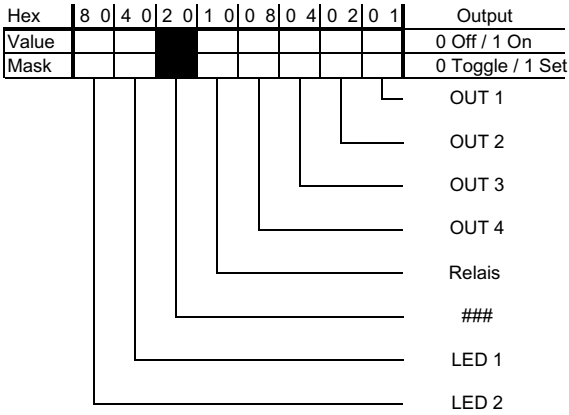
Inputs :	0	C
Binary conversion:	0000	1100
Switched:	Input 3, Input 4	

8.3.8 Set Output (0323)

The outputs on the RFID Server are set using this structure.

	2		4		6		8		9	10
Structure	send_seq.		rec_seq.		command		length		Output	Mask
Contents	00	00	00	00	23	03	0A	00	XX	XX
Byte sequnce	Low	High	Low	High	Low	High	Low	High		
Variable type	Word		Word		Word		Word		Byte	Byte

The value *Mask* is used to specify whether an output is set to a fixed value (Mask = 1) or the value is toggled (switched back and forth) (Mask = 0).



To set the outputs either the value which the output should assume is set (Mask = 1) or the output is set to toggle (Mask = 0).

Example:

Outputs :	9	A
Binary conversion:	1001	1010
Use:	LED 2, relay, Out 4, Out2	

Mask:	9	0
Binary conversion:	1001	0000
Switch on:	LED 2, relay	
Toggle:	Out 4, Out2	

8.4 Error handling

Errors occuring are indicated using two error functions.

8.4.1 Syntax errors(FF00)

Syntax errors in communication are represented using the function „*Syntax_Error (0xFF00)*“.

	2		4		6		8		9	
Structure	send_seq.		rec_seq.		command		length		Syntax_Err.	
Contents	00	00	00	00	FF	00	0A	00	XX	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word		Word	

The *Syntax_Error*-Code has the following meaning:

Syntax_Error	Description
00 00	Comand unknown
00 01	Parameter length
00 02	Parameter wrong
00 03	Comand forbidden

Cmd unknown means that the command which was sent is unknown. All commands usable in W&T Tag Control mode are described in Section 11.3.

If the structure length is not correct, error *Parameter length* is sent. The structure length must always be calculated over the entire structure.

Parameter wrong is always returned when an incorrect parameter for a command is sent to the RFID Server.

Commands which are not allowed at this time are sent with a *Cmd forbidden* error.

8.4.2 Functional errors (FF02)

Functional errors which occur internally are represented by the function RFID_Error (0xFF02).

	2		4		6		8		9	
Structure	send_seq.		rec_seq.		command		length		RFID_Err.	
Contents	00	00	00	00	F2	00	0A	00	XX	00
Byte sequnce	Low	High	Low	High	Low	High	Low	High	Low	High
Variable type	Word		Word		Word		Word		Word	

The *RFID_Error*-Code has the following meaning:

RFID_Error	Description
03 01	Out of Buffermemory
03 02	Temporary HW stop
03 03	Parameter wrong

Out of Buffermemory is sent by the RFID Server when buffered sending was activated in the W&T Tag Control Actions and more than 2990 events have arrived in the buffer. The ring buffer then overwrites the first events, so that only the most recent 2990 events are stored.

Temporarily stop of HW means sthat the hardware has reported a temporary failure. This may have been caused for example by an overheated final stage.

Parameter wrong. After the RFID Server has received the command, the associated parameters do not agree with the expected values. The indicated parameter was not understood by the device.

9 Communication via OPC

OPC makes it possible to use a standard software interface for processing capture and loss of tags. Applications which act as an OPC client can connect to the W&T OPC server, which handles communication with the RFID erver and then provides the events in corresponding OPC variables.

10 Database integration via ODBC

The W&T-Tool collects data from the W&T RFID Server and writes them to any desired database using the universal ODBC interface. The program also provides for export as an Excel spreadsheet, which in turn enables graphical representation.

10.1 Basics of ODBC

A central concept in the ODBC world is the „data source“. This is a named parameter set which references a database. The data source used by Sensobase is by default called „W&T Sensor Database“. All data sources installed on a computer can be managed using the WIndows service program „Data sources „ODBC)“. Sensobase will guide you through all the steps necessary for creating and configuring your data source.

The most important parameter of each data source is the ODBC driver used, which mainlyh determines the format for saving the data and which database operations are available. Additional parameters specify *where* the data are saved, as well as the options having to do with the special database format. Since the configuration dialog for entering these parameters is provided by the respective driver manufacturer, these options may be very different.

11 Protocol Mode

This mode is the transparent conversion of the ISO 15693-3 standard. After activating Protocol Mode, a network-side application can connect to the RFID Server using the set protocol port (default TCP port 2684).

11.1 Function description

(in Vorbereitung)

Appendix

- Firmware update
- Reset the RFID Server over the network (TCP-Port 8888)
- Port and socket numbers and network security
- Hardware reset to default settings
- Number systems / programming basics
- Technical Data

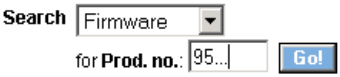
Firmware-Update

The RFID Server firmware is being continuously expanded. The following section describes how to perform a firmware update.

Where can I find the latest firmware?
The latest firmware including the available update tools and a revision list is published on our Web site at:

http://www.wut.de

From there it is easiest to use the search function on the left side. First enter the model number of your unit. In the associated selection box select *FIrmware* and click on the *Go* button.



This takes you directly to the page with the latest firmware for your RFID Server.

If you do not know the model number of your Server, you can find it on the sticker on the front panel along with the Ethernet address.

Especially if the sticker has a TB number as a designation, *it is possible that the RFID Server has special, custom firmware or configuration. This would be overwritten if you upload the standard firmware. In such cases please contact the appropriate administrator before updating.*

Firmware update over the network using Windows
Prerequisite is a PC running Windows 9x/NT/2000/XP/2003/Vista having a network connection and activated TCP/IP stack. For the update process you will need two files, which as already mentioned are available for downloading at *http://www.wut.de*.

- The executable update tool *WuTility* for sending the firmware to the RFID Server.
- The file with the new firmware for sending to the RFID Server.

No special preparation of the RFID Server is necessary for the firmware update.

The update tool is essentially self-explanatory. If you do have questions or anything is unclear, please use the associated documentation or online help.

Never intentionally interrupt the update process by pulling the power cord. After an incomplete update the RFID Server may become inoperable. If sending is interrupted due to a power failure, try restarting the update using the previous IP address of the device .

Resetting the RFID server over the network

For cases where the RFID Server needs to be reset over the network, TCP port 8888 has been set up. If a TCP connection is opened on this port. the RFID Server first accepts it, then immediate closes it and restarts its firmware.

Use of the system password

If a system password has been configured (see Section *Session Control*), it must be null-terminated (= [*passwort*] + 0x00) and sent to the RFID server within 2s of a successful connection opening.. If the RFID Server receives an incorrect or no password within this time, it sends the message *PASSWD?* followed by a null byte (0x00) to the client and closes the TCP connection.

If no system password is configured, the RFID server will, as described in the example, closes the TCP connection as soon as it has been opened and performs a reset.

This reset clears the buffer contents and any active connections. The reset can be generated from any desired station having knowledge of the system password.

Ports used and network security

In its default setting the RFID server uses the TCP and UDP port numbers listed in the following table.

Port number	Protocol	Application	Changeable	Can disable
69	TCP	Update via TFTP [2]	no	no
80	TCP	Listen port TCP/http	yes	no
2683	TCP	W&T Tag Control	yes	yes
2684	TCP	Protocol	yes	yes
8513	UDP	Inventorying [1]	no	no
8888	TCP	Reset [2]	no	no

[1] No write access to RFID-Server possible
[2] Password protected

Each port number in the RFID Server may be used for only one service. If different numbers are used for the changeable ports, be sure that no port number is duplicated.

The W&T RFID-Server and network security

Network security is rightfully gaining increasing attention. All experts agree that absolute security is impossible given the current state of technology. Each customer must therefore strive for a reasonable balance between security, functionality and cost given his specific requirements.

To give the customer the greatest possible flexibility based on changing security requirements from a pure testing and installation environment to critical production applications, the security measures have been made highly configurable by the customer. This section provides an overview of the security measures implemented on the W&T RFID Server and how they are used. It is assumed that the original W&T firmware (without custom modifications) is being used. Additional details can be found in the respective sections of this manual.

The authorization concept of the RFID Server

As already mentioned in the secion on Web Based Management, the RFID Server recognizes two levels of authorization:

- Administrator (System password)
- User (User password)

The control and configuration access to the RFID server is protected by the system password. The default setting is for *no* system password, so that after logging in, any user has full access to the corresponding settings and functions.

Access to the HF events such as capture and loss of tags as well as the digital I/Os is protected by the user password. The default here is for no password, so that anyone can connect to the corresponding TCP services of the RFID Server.

To prevent unauthorized access, we recommend using both a system password and a user password. Additional measures such as its composition and regular changing of the password can be determined by the customer.

The passwords are sesnt to the RFID server unencoded. You may therefore also want to ensure that password-protected access takes place only via an Intranet considered secure by the customer. For access over the public Internet, additional measures such as establishing a VPN tunnel (Virtual Private Network) may be considered. This is a general problem of network security, for which each customer must find his own solutions.

Ports with special functions

In addition to access via the Web interface, some functions can also be enabled using various TCP and UDP ports. These are shown in the table on the previous page. Some of the functions can be enabled and disabled from WBM. We basically recommend disabling all unneeded functions.

- **Port for inventorying using WuTility**
  Like all „intelligent“ components from W&T, the RFID Server can be accessed using the *WuTility* tool. The tool can use UDP port 8513 to read out information such as the hard- and software version, IP address, etc. This access cannot be turned off. Write access to the device is not however possible by this means.

- **Firmware-Update**

The firmware update is done also using the *WuTility* inventorying tool. After a special initialization of the update using TCP port 80 and using the system password, the actual firmware can then be sent via TFTP to the unit using UDP port 69.

- **Reset using Port 8888**
  A device reset can be performed by opening a connection (e.g. using telnet) to TCP port 8888. Immediately after opening a connection, the system password (if set) must be provided. This immediate sending of the password is not practical by manual means, and should be implemented using a program. The consequences of a reset are the same as for a momentary power interruption.

Restoring the factory default settings

By restoring the factory default settings using WBM, all the settings made by the customer can be cancelled. Among other things, this also cancels the system and user password.

Hardware reset to default settings

In addition to the possibility of restoring the RFID Server to its default settings using Web Based Management, you can also accomplish this by hardware. The device has jumpers on the circuit board which are normally open. To invoke factory default settings, proceed as follows:

- Turn power off to the RFID Server and open the housing by removing the two screws on the back of the enclosure.
- Close the jumpers and restore power.
- After approx. 3s the current configuration is cancelled and the factory default settings restored.
- Turn power off to the RFID Server, open the jumpers, and close up the housing.

Resetting the non-volatile memory results in the loss of all settings which deviate from the default values, including the IP address. The setting profile of the factory defaults can be replaced among other things by a custom profile. In this case the custom settings are activated after a reset.

Number systems/Programing basics

Binär				Hex
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	A
1	0	1	1	B
1	1	0	0	C
1	1	0	1	D
1	1	1	0	E
1	1	1	1	F

BYTE:	Unsigned number with a length of 8 bits	00
WORD:	Unsigned number with a length of 16 bits	00 00
LONG:	Unsigned number with a length of 32 bits	00 00 00 00

A brief refresher in number systems

In computer technology we work with bits and bytes, i.e. in dual, or binary number systems.

Dual numbers are unfortunately difficult to grasp for people. Who can recognize immediately that dual 110001110101 = decimal 3189?

Since you must see each input and output on the RFID Server as the place in a 12-digit binary number, there is no escaping having to review this material again.

Binary digit 110001110101

Bit 0	=	2^0	=	1	1	x	1	=	1
Bit 1	=	2^1	=	2	0	x	2	=	0
Bit 2	=	2^2	=	4	1	x	4	=	4
Bit 3	=	2^3	=	8	0	x	8	=	0
Bit 4	=	2^4	=	16	1	x	16	=	16
Bit 5	=	2^5	=	32	1	x	32	=	32
Bit 6	=	2^6	=	64	1	x	64	=	64
Bit 7	=	2^7	=	128	0	x	128	=	0
Bit 8	=	2^8	=	256	0	x	256	=	0
Bit 9	=	2^9	=	512	0	x	512	=	0
Bit 10	=	2^{10}	=	1024	1	x	1024	=	1024
Bit 11	=	2^{11}	=	2048	1	x	2048	=	2048
								Decimal digit	3819

Converting dual numbers to decimal numbers is not difficult. But there is no spontaneous relationship between sete outputs and the decimal value. Therefore, hexadecimal numbers are used where persons would have to be juggling bits and bytes.

In hexadecimal numbers the value of each place is can be represented by 15 various characters. Since our decimal number system only knows digits from 0...9, the hexadecimal system has been expanded to include the letters A...F.

A =10, B=11, C=12, D=13, E=14, F=15.

Again in somewhat clearer form.

Hexadecimal digit C75

Stelle 0	=	16^0	=	1	5	x	1	=	5
Stelle 1	=	16^1	=	16	7	x	16	=	112
Stelle 2	=	16^2	=	256	12	x	256	=	3072
								Decimal digit	3819

At first glance the use of the hexadecimal number system does not seem to simplify representation of the inputs and outputs.

But take a closer look. Each place in the hexadecimal number is a power of 16 multiplied by the digit. 16 in turn is the 4th power of 2, i.e. 2^4.

Each place in the hexadecimal number system can therefore be calculated by adding the powers of 2 2^0 to 2^3.

Hexadecimal digit 5 = Binary digit 0101

Bit	0	=	2^0	=	1	1 x	1 =	1
Bit	1	=	2^1	=	2	0 x	2 =	0
Bit	2	=	2^2	=	4	1 x	4 =	4
Bit	3	=	2^3	=	8	0 x	8 =	0
							Hexadecimal digit	5

If you break down a binary number into 4-bit ranges beginning with the lowest-value place, you can convert between binary numbers and hexadecimal numbers with little effort.

Hexadecimal digit C 7 5

Binary digit 1100 0111 0101

1 x	1 =	1	
0 x	2 =	0	
1 x	4 =	4	
0 x	8 =	0	
	Hexadecimal place	5	
1 x	1 =	1	
1 x	2 =	2	
1 x	4 =	4	
0 x	8 =	0	
	Hexadecimal place	7	
0 x	1 =	0	
0 x	2 =	0	
1 x	4 =	4	
1 x	8 =	8	
	Hexadecimal place	C	

With a little practice you can learn to do this easily in your head.

Technical Data

Supplay voltage ... ... DC	12V (+/-5%)
Current draw	typ. 700mA max. 950mA
Permissible ambient temperature ... ... Storage ... Operating	 -40 ... +70°C 0 ... +50°C
Permissible rel. humidity	0 - 95% (non-condensing)
Network	10/100BaseT, RJ45 for STP cabling
Galvanic isolation	Ethernet connetion: min. 500V
Dimensions	200 x 280 x 41mm
Weight	approx. 950g
Operationg frequency	13,56 MHz
HF transmitting power	approx. 1W
Supported transponders	ISO 15693-3 (others on request)
Read / write range	typ. 35cm
Digital inputs	4 x current sourcing 3-4mA 0-24V, switching threshold 4V +/-1V
Digital outputs ... ... Relay ... Open collector	 1 x changeover, max. 48V DC max. 5A, switching frequency 1800/h 4 x Open collector, 0-12V, max. 100mA, Ri approx. 17Ohms

Declaration of Conformity

W&T
www.WuT.de
W&T Interfaces für TCP/IP, Ethernet, RS-232, RS-485, USB, 20mA, Glas-und Kunststoff-LWL, http, SNMP, OPC, I/O digital, I/O analog, ISA, PCI, ...

Declaration of Conformity

We, Wiesemann & Theis GmbH, Porschestr. 12, 42279 Wuppertal, hereby declare that the product

RFID-Server, Type 95001

to which this declaration relates is in conformity with the essential provisions of the EC Council Directives

1. 89/336/EEC (2004/108) Electromagnetic Compatibility Directive (EMC)
2. 73/23/EEC, resp. 93/68/EEC Low Voltage Directive (LVD)
3. 99/5/EEC Radio Equipment and Telecommunications Terminal Equipment Directive (R&TTE)

in compliance with the following standards:

Emission according to ETS EN301489-3 (V.1.4.1):
1.1. EN 55022-B
1.2. EN 61000-3-2
1.3 EN 61000-3-3

Immunity according to ETS EN301489-3 (V.1.4.1):
1.4 EN 61000-4-2/2001
1.5 EN 61000-4-3/2002 +A1
1.6 EN 61000-4-4/2005
1.7 EN 61000-4-5/2001
1.8 EN 61000-4-6/2001
1.9 EN 61000-4-11/2005

2.1 EN 60950-1 (2003)

3.1 EN 50371 (2002)

3.2 EN 50364 (2001)

3.2 EN 300330-2 (V.1.3.1)

Wuppertal, 06/11/2007

Klaus Meyer, EMC-Representative

Dipl.-Ing. Rüdiger Theis, Managing Director

Wiesemann & Theis GmbH
Porschestr.12
42279 Wuppertal
GF: Dipl.-Ing. Rüdiger Theis

Tel.: 0202/2680-0
Fax: 0202/2680-265
info@WuT.de
www.WuT.de

Handelsregister:
Amtsgericht Wuppertal HR86377
UStID Nr.: DE121008340
Steuer Nr.: 131/5937/014

Bankverbindung:
Postbank Essen
Konto: 289397436
BLZ: 36010043