

Manual

USB-Server Industry Isochron



Model
Release

53642
1.10, January 2013

© 01/2013 by Wiesemann und Theis GmbH
Microsoft, MS-DOS, Windows, Winsock and Visual Basic
are registered trademarks of Microsoft Corporation

Subject to errors and changes:

Since mistakes are always possible, all of the information in this manual should be applied with discretion. Please let us know of any errors or unclear instructions so that we can correct them as quickly as possible.

Perform work on and with W&T products only as described here and after you have read and understood the manual in full. Unauthorized actions may create hazardous conditions. We are not liable for the consequences of unauthorized actions. When in doubt, please consult with us or your dealer.

This device contains software components which are subject to one or more Open Source licenses. The Appendix to this document contains copies of these licenses.

The associated source text can be downloaded at no charge from:

<http://www.wut.de/e.5www-60-inus-000.php>

You may also obtain the source code from us in the form of a data medium for a period of three years after the last product shipment for a nominal charge. To avail yourself of this offer, please contact us at *info@wut.de*.

This offer is valid for every recipient of this notification.

Inhalt

1 Quickstart	7
Step 1: Installation	8
Step 2: Power and network connection	9
Step 3: Connecting the USB devices	10
Step 4: Setting the network parameters	11
Step 5: Installing the W&T USB Port Redirector	12
Step 6: Connecting to a USB device	13
2 Assigning/Changing IP Parameters	15
2.1 Managing the network parameters in the USB-Server	16
2.2 DHCP mode (factory default setting)	17
2.3 Static mode	22
3 Hardware - Interfaces and Indicators	27
3.1 Supply voltage	28
3.1.1 PoE supply	28
3.1.2 External supply	28
3.2 Ethernet - Anschluss	29
3.2.1 Link-Status	29
3.3 USB ports	31
3.4 Multicolor LED	32
4 System Overview and Function	33
4.1 Introduction to the W&T USB-Server	34
4.1.1 Supported USB modes	34
4.1.2 Maximum number of USB devices	34
4.1.3 System overview	35
4.1.4 Port numbers	35
5 The W&T USB Port Redirector	37
5.1 Overview and system requirements	38
5.2 Download & installation	39
5.3 The inventory list	41
5.4 Using USB devices - Plug/Unplug	44

W&T

- 6 Web-Based-Management 53**
 - 6.1 Starting and navigating the WBM 54
 - 6.2 WBM - configuration sessions 56
 - 6.3 WBM - Assigning passwords 58
 - 6.4 WBM - Network basic parameters 59
 - 6.5 WBM - Netzwerk services 61
 - 6.6 WBM - Device information and WBM adjustments 64

- 7 Appendix 65**
 - 7.1 Up-/Downloading the configuration data 66
 - 7.2 Firmware update 68
 - 7.3 Resetting the USB-Server 70
 - 7.4 Reset to factory defaults 71
 - 7.5 Used ports and network security 73
 - 7.6 Technical data 76
 - 7.7 Licenses 77

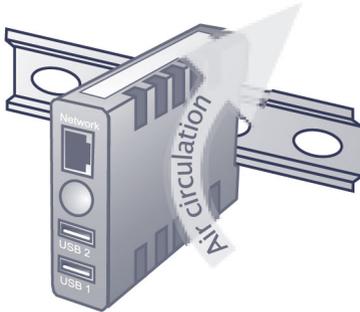
- Index 84**

1 Quickstart

Those who are already familiar with use of the W&T USB-Server will find on the following pages a quick start procedure with the basic steps from hardware installation to IP assignment and starting the Windows driver. Additional information is contained in the respective detail sections.

Step 1: Installation

The housing of the *W&T USB-Server* and the arrangement of the ventilation slot is designed for installation on a standard DIN rail per DIN EN 50022-35.

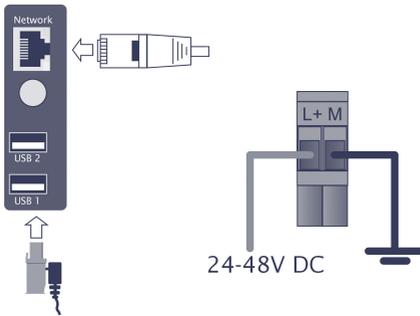


Especially in local conditions at elevated temperatures any alternate method of mounting must still ensure adequate air circulation.

Step 2: Power and network connection

Power supply

When PoE is used (IEEE802.3af) power for the *W&T USB-Server* is provided by the network infrastructure, so that simply connecting the network cable is all that is required. Alternately power can be brought in externally to the screw terminal located on the underneath of the device. The wide-range input of the USB-Server allows use of DC voltage from +24 - +48V. The input is reverse polarity protected,



Network connection

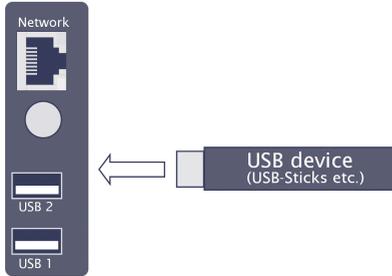
Connection to the 10/100BaseT network is accomplished using a 1:1 wired, standard RJ45 patch cable. If a link can be established with the switch, this is indicated by illumination of the green *Status* LED. Addressed data traffic is indicated by blue flashing.



Detailed information about the supply voltage and the network connection of the W&T USB-Server can be found in the Hardware section.

Step 3: Connecting the USB devices

The *W&T USB-Server* provides two USB 2.0 ports for connecting USB devices. The ports are capable of providing max. 500mA each for supplying the connected devices.



Detailed information about the USB connections of the W&T USB-Server can be found in the Hardware section.

Step 4: Setting the network parameters

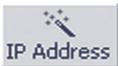
The default address of the *W&T USB-Server* is:

190.107.233.110

In addition, DHCP protocol is the factory default. If the network in question has a DHCP server, the network basic parameters are automatically assigned after powering up the *W&T USB-Server* and after it is connected to the network.

Alternately the *WuTility* inventory and management tool can be used to switch to static network parameters. Install this tool on a Windows PC from the included product CD; the PC must be located in the same subnet as the *W&T USB-Server*.

After starting, *WuTility* automatically searches the network for accessible W&T network devices. Select from the list of found devices the desired *W&T USB-Server* and then click on the *IP Address* button.



The following dialog allows you to switch to *Static* mode for manually assigning the IP address, subnet mask and gateway. Activating *Static* mode automatically deactivates DHCP protocol.



Detailed information about the various methods of assigning the IP address is found in the Assigning the IP address section.

Step 5: Installing the W&T USB Port Redirector

The *W&T USB Port Redirector* implemented as a Windows core driver makes a virtual USB host controller available. Install it on a Windows XP or higher machine using the W&T product CD included in the scope of delivery. Login as Administrator or with administrator rights is required for installation.

In addition to the actual core driver the associated configuration- and management tool is installed in the new program group *W&T USB Port Redirector*.



To make it possible to publish updates to the W&T USB Redirector as soon as possible, the driver is not WHQL certified. To successfully finish the installation the corresponding message from the Windows logo test must be acknowledged with Continue installation.



Detailed information about installing is found in the W&T USB Port Redirector section.

Step 6: Connecting to a USB device

The configuration tool is started from the new program group *W&T USB Port Redirector*. The local subnet is automatically searched for by *W&T USB Servers* and connected USB devices.

 *If the Windows computer and the W&T USB-Server are not located in the same subnet, no automatic inventorying can take place. The W&T USB-Server must first be manually added using Device – Add.*



Quick connecting the USB device

Highlight the desired USB device in the inventory list of the USB Port Redirector and click on the *Add* button in the icon list. Similar to the local connection the USB device is now added into the Plug&Play system of Windows. The device-specific driver installation takes place automatically and the USB device can then be used just as if it were connected to a local USB port on the computer.

Now added devices are enabled for other users when closing the configuration tool or by clicking on the *Release* button.

 *The type of connection opened to the USB device using the Add button is configurable in the menu Options → Standard Claim. The factory default is ... until configuration tool exits.*



Expanded incorporation of the USB device

This dialog provides expanded functions for incorporating and enabling the USB device. For example when there is a permanent connection, the USB device is enabled even before user login in Windows.

Other options include time-limited incorporation, links to certain programs or print jobs and rules for competing access to USB devices.

Claim Device for Local Use

Identification

USB Server: 10.40.21.41 TCP port: 32032 USB port: 2

OK Cancel

Use for how long?

don't use

basic

until configuration tool exits

until Windows is restarted

permanently

advanced

ends after 5 minutes

automatic, for this application: [] [] []

automatic, while printing

as alternate device for []

When someone else wants to use this device...

let go, based on priority. Mine is: 0

hold on just the same Advise me of denied requests

let go, unless I object within 30 seconds



Detailed information on the function of the W&T USB Port Redirector is found in the W&T USB Port Redirector section.

2 Assigning/Changing IP Parameters

After the hardware installation of the USB-Server, the IP address and any subnet mask and gateway for operation in a TCP/IP network must be assigned. Please check with your systems administrator for the correct values of these parameters. The USB-Server factory default IP address is 190.107.233.110.

- Setting the IP address, subnet mask and gateway address using the management tool *WuTility*
- Setting the IP address, subnet mask and gateway address using DHCP protocol
- Changing the IP parameters using Web-Based-Management

2.1 Managing the network parameters in the USB-Server

The W&T USB-Server distinguishes between two modes with respect to its network-side basic parameters..

Static

IP address, subnet mask and gateway are stored in the non-volatile setup of the USB-Server, and DHCP protocol is disabled. The parameters set using this method remain stored even after power interruptions and resets until they are changed using *WuTility* or Web-Based-Management.

DHCP (factory default setting)

DHCP protocol is enabled and the USB-Server attempts to obtain its IP parameters from a DHCP server located in the network. If no DHCP server can be accessed or the attempt to obtain an IP address is rejected, the USB server operates using the factory default IP address 190.107.233.110. When switching from *Static* to *DHCP* mode using *WuTility* or Web-Based-Management, the USB-Server reverts to this default IP address until valid new parameters are assigned.

2.2 DHCP mode (factory default setting)

Many networks use DHCP (Dynamic Host Configuration Protocol) for centralized and dynamic assigning of the network parameters. As shipped and after a reset to the factory default settings, *DHCP* mode is enabled, so that in network environments with dynamic IP assigning all you need to do is connect the device to the network. The following parameters can be assigned using DHCP:

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



After an unintended address assignment or address change to an unknown address using DHCP protocol, the management tool WuTility can be used to find the USB server and uniquely identify it based on its MAC address. Changing the wrong IP address or switching to Static mode while disabling DHCP protocol can also be done using WuTility.



An explanation of the basic terms and fundamentals of addressing in the Internet as well as DHCP and BOOTP can be found in our manual „TCP/IP-Ethernet and Web-IO“.

2.2.1 Activating DHCP mode

DHCP protocol is activated by switching from *Static* mode to *DHCP* mode using WuTility or Web-Based Management of the USB-Server. The previous static IP address is then deleted and DHCP protocol is enabled. The USB-Server returns to its default address 190.107.233.110 until new network parameters are assigned using a DHCP server.

- **Activating using the management tool WuTility**
In the device list select the desired USB-Server and click on the *IP Address* button. In the following dialog

window check the radio button *DHCP* and then click on the *Continue* button.

- **Activating using Web Based Management**

In the menu *Config* → *Device* → *Basic Settings* → *Network* select the option *Static*. After entering the new IP address and the valid subnet mask and gateway address, click on the *Apply* button. To save the new setting in the USB-Server, select *Logout* and *Save*. The device can now be reached under the new IP address.



Switching from Static to DHCP mode causes the device to revert from the static set IP address to the factory default setting 190.107.233.110. If the IP assignment using DHCP fails, for example because no DHCP server is available, the USB-Server may no longer be reachable, especially in routed network environments. Reactivating Static mode using WuTility can only be done using a computer in the same physical network.

2.2.2 Deactivating DHCP mode

DHCP mode is deactivated by switching from *DHCP* mode to *Static* mode using WuTility or Web-Based-Management on the USB-Server. In both cases the new values for IP address, subnet mask and gateway address must be manually specified.



Each IP address must be unique within the network.

- **Deactivating using the WuTility management tool**

From the device list select the desired USB-Server and click on the *IP Address* button. In the resulting dialog window activate the *Static* radio button. After entering the new IP address and the valid subnet mask and gateway address click on the *Continue* button..

- **Activating using Web Based Management**

In the menu *Config* → *Device* → *Basic Settings* → *Network* activate the *Static* option. After entering the new IP address as well as the valid subnet mask and gateway address click on the *Apply* button. Clicking on *Logout* and *Save* saves the new setting in the USB-Server and the device can again be accessed under the new IP address.

2.2.3 System Name

To support a possible later automated updating of the DNS system using the DHCP server, the USB-Server identifies itself within the DHCP protocol by its system name. The factory default name is *USB-Server-* followed by the last three places of the Ethernet address. For example the factory set system name of a USB-Server having Ethernet address 00:c0:3d:01:02:03 is *USB-Server-010203*. The system name of the USB-Server can be changed using Web Based Management.

2.2.4 Lease-Time

The lease time determined and sent by the DHCP server specifies the time limit of the assigned IP address. After half the lease time has expired the USB-Server attempts to extend the time and update the address. If this is not possible by the time the lease time expires, for example because the DHCP server can no longer be reached, the USB-Server deletes the IP address and reverts to the factory default address 190.107.233.110. At the same time the cyclical search for alternate DHCP servers for assigning a new IP address is started.

Because the clock is absent the lease time for the current IP address is no longer available after a reset. After the restart there is then a corresponding update request with

the original DHCP server. If the latter cannot be reached at this point in time, the USB-Server deletes the IP address and reverts to the factory default address 190.107.233.110. At the same time the cyclical search for alternate DHCP servers for assigning a new IP address is started.

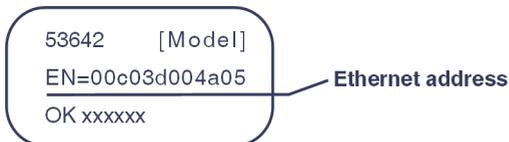
In *DHCP* mode the remaining lease time in seconds together with the current IP address is displayed on the Web page *Doc* → *Properties*.



If after the assigned lease time has expired the DHCP server cannot be reached, the USB-Server deletes the IP address and reverts to the factory default address 190.107.233.110 and starts the cyclical search for alternate DHCP servers. All existing connections to W&T USB Port Redirectors are closed. To prevent problems of this kind we recommend configuring the lease time in the DHCP server to infinite whenever possible.

2.2.5 Reserved IP addresses

The USB-Server is designed as a TCP server and therefore provides services which can be used as needed by computer-side USB Port Redirectors. In order to open a connection these need of course the current IP address of the USB-Server, so that it makes sense to reserve a particular IP address for the USB-Server on the DHCP server. This is generally done by linking the IP address to be assigned to the unique Ethernet address of the USB-Server, which can be found on the sticker on the housing.



2.2.6 Dynamic IP addresses

Fully dynamic address assignment, where the USB-Server gets another IP address after each restart or after expiration of the lease time, only makes sense in network environments with automatic cross-connection between the DHCP and DNS services. This means when a new IP address is assigned to the UBS-Server, the DHCP server then also automatically updates the DNS system.

2.3 *Static mode*

In *Static mode* the USB-Server uses static network parameters and DHCP protocol is disabled. There are two ways of assigning the static values for IP address, subnet mask and gateway.

2.3.1 Assigning static IP parameters using WuTility

The Windows tool WuTility in version 3.70 and higher supports inventorying and management of the network basic parameters of W&T USB-Servers:

- IP address
- Subnet mask
- Gateway address
- Umschaltung Static/DHCP

To assign these parameters the PC and USB-Server must be located in the same physical network, whereby the function is independent of the current address settings of the USB-Server. This means even if the current parameters of the USB-Server do not match the settings of the PC, you can still always use *WuTility* to make a change. Any system password set in the USB-Server must however be known.

Installing WuTility

The quickest way to install WuTility is using the *Install* button on the start screen of the product CD included with the product.

Then start *WuTility* using

Start → *Programs* → *W&T Software Toolkit* → *WuTility*

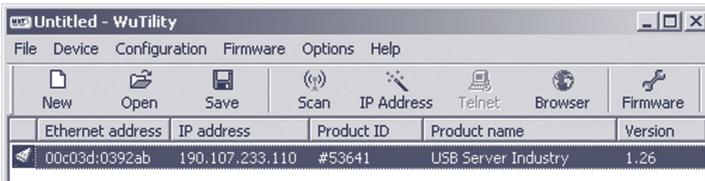
Starting the assignment dialog

Be sure that both the USB-Server and the computer are connected to the same physical network. After starting, *WuTility* automatically searches the local network for connected W&T network devices and creates an inventory

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



Within the inventory list you can identify the desired USB-Server by its MAC address. For initial installations this IP address is 190.107.233.110.



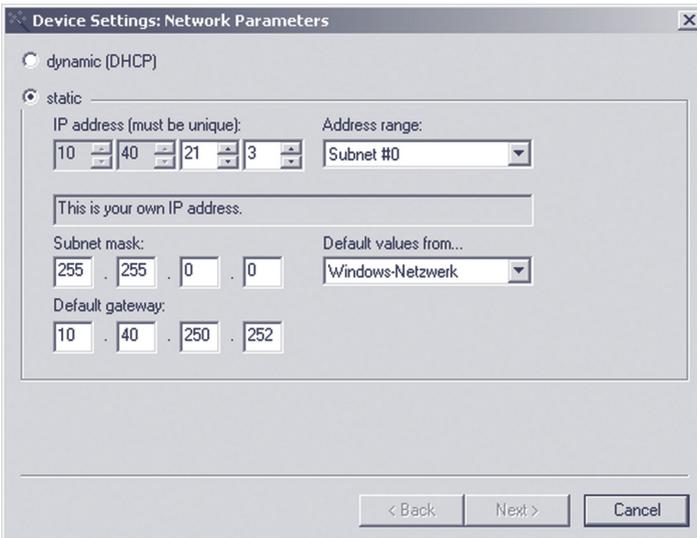
Select the desired USB-Server and then click on the *IP address* button:



In the resulting dialog window activate the radio button *Static* and enter the desired values for the IP address, the subnet mask and the gateway address.



Each IP address must be unique within the network.



After clicking on the *Continue* button you are also prompted for the system password. Then the network parameters are stored in the USB-Server in non-volatile memory.

All further settings are made using Web-Based-Management of the USB-Server and an Internet browser. Select the desired USB-Server from the WuTility inventory list and click on the *Browser* button.



Additional information about management of the USB-Server can be found in the section *Web-Based-Management*.



Changing the network parameters is protected by the system password. To prevent unauthorized use, we recommend assigning a system password for operating USB-Servers.

2.3.2 Assigning static IP parameters using WBM

As shipped and after a reset to the factory default settings the USB-Server is in *DHCP* mode. As long as no address is assigned using a DHCP server, the USB-Server can also be reached in parallel through its default IP address 190.107.233.110. Switching to *Static* mode and assigning the new IP parameters can also be done using Web-Based-Management and a browser.



In contrast to address assigning using WuTility, initial startup of multiple USB-Servers using the methods described in the following can be done only in sequence. Only after a USB-Server has received its new IP address can the next USB-Server be connected to the network. Clarify any changes to the network settings in advance with the responsible network supervisor.

On the computer side one of the two following conditions must be met:

- The IP address of the computer used is in the subnet range 190.107.0.0 or is temporarily changed to an appropriate value. You need administrator rights to change the IP address of a computer. Notify your responsible network administrator before making changes to the network settings of a computer.
- A fixed route which directs the IP address 190.107.233.110 to the local network is set up on the computer. Administrator rights are required in order to set up such a route. The command line syntax for creating a fixed route under Windows XP is:

```
route ADD 190.107.233.110 MASK 255.255.255.255 [IP address of the PC]
```

Finally, start the Internet browser and enter the destination *http:// 190.107.233.110* in the address line and change the network settings to the new values on the Web pages of the USB-Server.

3 Hardware - Interfaces and Indicators

- **Supply voltage via PoE and external**
- **Ethernet port**
- **USB ports**
- **LED indicators**

3.1 Supply voltage

Power for the W&T USB-Server can be provided either via PoE or from an external power supply.

3.1.1 PoE supply

The model 53642 USB-Server is suitable for use in PoE environments according to IEEE802.3af. Here the supply voltage is brought in by the network infrastructure through the RJ45 terminal. The USB-Server supports both phantom power using data pairs 1/2 and 3/6 as well as power through the unused wire pairs 4/5 and 7/8.

In order to enable power management for the supplying components, the USB-Server identifies itself as a Power Class 3 device (power consumption from 6.49W to 12.95W).

3.1.2 External supply

As an alternative to PoE, the USB-Server can also be powered through the plug-in screw terminal located on the underneath of the housing. The DC voltage used must lie in the following range:

- DC voltage: 24V (-10%) - 48V (+10%)

The W&T USB Server input is reverse polarity protected. Proper function does however require the following polarity setting:



The current draw can be found in the technical appendix.

3.2 Ethernet connector

The USB-Server Industry has an IEEE 802.3 and IEEE 802.3af (PoE) compatible RJ45 network terminal.

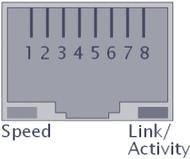
3.2.1 Link-Status

Link Status is indicated by the two LEDs built into the RJ45 receptacle.

- **Link/Activity (green)**
ON indicates a valid link to a hub/switch port. The LED flashes during data communication.
- **Speed (yellow)**
ON indicates a 100MBit/s-Link (100BaseT). OFF corresponds to a link at 10MBit/s (10BaseT)

3.2.2 10/100BaseT

A shielded RJ45 connector serves as the network connection. The configuration shown in the drawing below refers to an MDI interface, so that the connection to the switch/hub is made using a max 100m long, 1:1 shielded patch cable.



Pin	Direction	Device w/o PoE	Device with PoE
1	Out	Tx+	Tx+
2	Out	Tx-	Tx-
3	In	Rx+	Rx+
4	In	nc	Vcc positive
5	IN	nc	Vcc positive
6	In	Rx-	Rx-
7	In	nc	Vcc negative
8	In	nc	Vcc negative

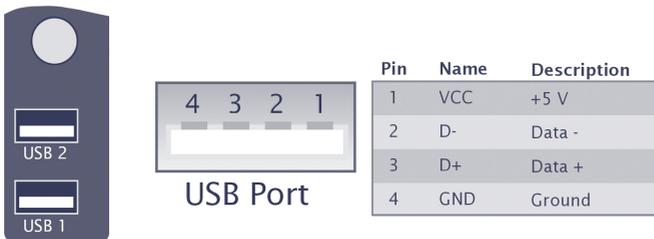
The network connection is galvanically isolated from the supply voltage and the USB ports to at least $500V_{rms}$.

Auto Negotiation: 10/100BaseT, Full/Half Duplex

In its factory default setting the W&T USB-Server uses *Auto-Negotiation* mode. To prevent communication problems caused for example by a duplex mismatch, we recommend also operating the used port on the switch or hub in *Auto-Negotiation* mode. Here both the transmission speed and the duplex procedure are automatically negotiated and correspondingly set in the devices.

3.3 USB ports

The USB standard specifies both the wiring of the port and the names of the signal lines. The configuration shown below corresponds to a USB standard port. Both USB ports are able to provide devices with 5V and a maximum of 500mA each, independently of each other. To prevent hardware damage the respective USB port is automatically disconnected when overload is present, with this disconnected state indicated by a red multi-color LED.



Both ports of the *W&T USB-Server* conform with USB 1.0, 1.1 and 2.0 with transmission speeds of 1.5 Mbit/s (Low), 12 Mbit/s (Full) and 480 Mbit/s (High). This means most USB devices using the transfer modes *Control*, *Interrupt*, *Bulk* and *Isochronous* are supported.



In accordance with the USB standard, connecting and unplugging USB devices is always possible and permissible from a purely electrical point of view (hot-plugging). To prevent data loss - for example when using memory sticks - we recommend disconnecting devices only when there is no connection between a network computer and the USB device.

3.4 Multicolor LED

In addition to the LEDs built into the RJ45 connector for the network connection (see Ethernet Connection section), the USB Server has a multicolor LED combined with a Reset button. The following colors are used:

- **green**
The USB Server firmware is ready to use. Underlying cyclical flashing indicates the system load. The higher the flashing frequency the greater the load.
- **blue**
The USB Server performs a system reset. During normal operation blue flashing indicates data traffic to and from the USB Server.
- **white pulsing**
The USB Server is receiving new firmware. During this process ensure that neither the supply voltage nor the network connection is interrupted.
- **red flashing**
The USB Server does not detect a network link.
- **red**
Serious system error - the system cannot be properly started.

4 System Overview and Function

The W&T USB-Server together with the W&T USB Port Redirector provides a transparent network tunnel for sending USB datagrams.

- Data connection concept
- Virtual USB-Host-Controller

4.1 Introduction to the W&T USB-Server

The *W&T USB-Server* in conjunction with the computer-side in *W&T USB Port Redirector* enables the addition of remote USB devices located in the network. With respect to the device-specific drivers and applications these behave as if they were connected to a local USB port on the computer.

4.1.1 Supported USB modes

The *W&T USB-Server* conforms with USB 1.0, 1.1 and 2.0 with transmission speeds of 1.5 Mbit/s (Low), 12 Mbit/s (Full) and 480 Mbit/s (High). This means most USB devices using the transfer modes *Control*, *Interrupt*, *Bulk* and *Isochronous* are supported.

4.1.2 Maximum number of USB devices

Although the *W&T USB-Server* is designed for direct connection of two USB devices, connection of an external USB hub per USB port is also supported. This allows max. 6 USB devices to be connected and incorporated through the *W&T USB Port Redirector* into Windows systems. It should be noted however that multi-function devices do often already have internal hubs.



With respect to data throughput - especially when connecting High-Speed USB devices - it must be remembered that only a theoretical bandwidth of maximum 100Mbit/s is available on the network side.

4.1.3 System overview

On the hardware side the *W&T USB-Server* adapts the USB devices. Processing of the time-critical USB protocol takes place locally and is mirrored - time-decoupled - on the network side to a TCP server service.

On the software side the *W&T USB Port Redirector* acts as a virtual USB host controller. When the user connects to one of the USB devices, the latter is available to the respective system after opening the network connection as if it were locally connected. Connections to USB devices are always exclusive, i.e. a simultaneous attempt from a competing USB Port Redirector is rejected and can only take place after closing the first connection.

In order to keep the configuration effort of the firewall in protected environments to a minimum, the entire network communication takes place on a single, configurable TCP port. In parallel with this there are management services for configuration, firmware updates etc. available which, however, are not required for the connection between USB-Server and USB Port Redirector.

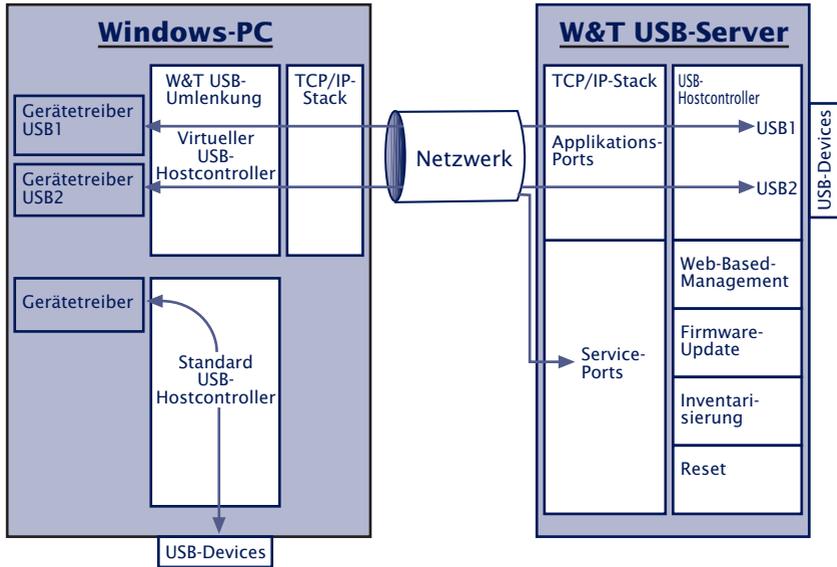
A list of all ports used by the USB-Server can be found in the Appendix.

4.1.4 Port numbers

To communicate with USB devices the USB Redirector uses by default TCP Port 32032. This port number can be changed from the USB Server web pages in the menu branch *Home → Config → USB-Server 2 → Network-Services*.

Any installed security components (software or hardware firewall, security suites etc.) *must* allow communication over this port number without delay. This is now however absolutely necessary for the UDP port 8513 used for

automatic inventorying. Inserting the USB-Servers can be done in this case manually (for additional information see section *The inventory list*).



5 The W&T USB Port Redirector

The W&T USB Port Redirector consists on one hand of the virtual host controller designed as a Windows core driver. In addition to controlling the network connection to the USB-Server, it takes care of system-side processing of the USB handling. The associated configuration tool inventories the available USB-Servers and allows the connected USB devices to be logged on and off with a mouse click.

- **System requirements**
- **Installation/Deinstallation**
- **Using the configuration tool**
- **Configuring the W&T USB Port Redirector**

5.1 Overview and system requirements

Configuration of the USB Port Redirector, implemented as a core driver, is registry-based using the *USB Port Redirector configuration tool*, configured in the Windows start menu. In addition, the configuration tool automatically searches the local subnet for W&T USB-Servers and enters them in a list with any connected USB devices.



Additional and possibly more recent information about the individual configuration options can be found in the online help for the W&T USB Port Redirector.

5.1.1 System requirements

On the system side the following requirements must be met:

- Operating system Windows XP/Vista/7/8 incl. 64-bit and server editions
- Login as Administrator or with Administrator rights

5.1.2 Verwendete Portnummern

To communicate with USB devices the USB Redirector uses by default TCP Port 32032. This port number can be changed from the USB Server web pages in the menu branch *Home → Config → USB-Server 2 → Network Services*.

Any installed security components (software or hardware firewall, security suites etc.) *must* allow communication over this port number without delay. This is now however absolutely necessary for the UDP port 8513 used for automatic inventorying. Inserting the USB-Servers can be done in this case manually (for additional information see section *The inventory list*).

5.2 Download & installation

The MSI installation package for the USB Redirector contains 32- and 64-bit versions of the core driver as well as the German and English language options. The package is found on the included product CD. The most current version is always available on our web site under *http://www.wut.de*

5.2.1 Download the *W&T USB redirector*

A direct link to the MSI installation package can be found on the Start page of the W&T product CD, which is configured as a web site. From the homepage *http://www.wut.de* the simplest method is to enter article number 53642 in the *Search* function. Set the drop-down box to *Drivers* and then click on the *Go* button.



The following page contains a direct link to the current version.

5.2.2 Installing the *W&T USB redirector*

The MSI installation package can be run directly. In addition to the actual core driver the associated configuration and management tool is also installed to the new *W&T USB Redirector* program group.



In order to be able to publish W&T USB Port Redirector updates in as timely a fashion as possible, the driver is not WHQL certified. To successfully finish the installation the corresponding message for the Windows logo test must be acknowledged with Continue installation.



Usually installation of the W&T USB Port Redirector is done as an update to any already present older versions. All the settings and connection parameters made remain intact and are then available unchanged.

5.2.3 Uninstalling

For uninstalling, the program group *W&T USB Port Redirector* has its own *Uninstall* entry. Alternatively you can uninstall using the Windows software management function in the Control Panel.

5.3 The inventory list

The inventory lists in the configuration tool represent the required and available W&T USB-Servers with the connected USB devices along with additional information in a tree structure.

	Identification	Port	Description	Requested	Client	Status
	10.40.26.26	32032	USB Server - 049F99			
	0474-FF00	1	Sanyo Electric Co. Ltd. Sanyo...			
	0D7A-0001	2	Marx USB crypToken		10.40.26.5	

-  **Icon for USB-Server**
-  **Icon for a USB device.** This is connected to the first USB-Server shown above.
- **Identification**
For USB-Servers you enter here the IP address. For USB devices the vendor and product ID are shown.
- **Port**
For USB-Servers the TCP port used for USB data exchange is shown (factory setting = 32032). For USB devices which of the two physical USB ports on the USB-Server the device is connected to is shown.
- **Description**
For USB-Servers the system name is indicated here. This is configurable using Web Based Management and is factory set to *USB-Server-* followed by the last three places of the MAC address (e.g.. *USB-Server-040506*). For USB devices the description read out via USB is shown..
- **Requested**
Indication whether and, if appropriate, how long USB devices are connected on the respective computer.
- **Client**
IP address of the computer on which the USB device is connected. To open a connection to this USB device this column must be blank.
- **Status**
Error and status messages for the respective USB device..

5.3.1 Automatic inventory list creation

Here the local subnet automatically searches for *W&T USB-Servers* and USB devices connected to them. The inventoring is done in two phases, whereby first the *W&T USB-Servers* are found using a UDP broadcast (port 8513). Then any connected USB devices are queried using a TCP connection to the *UsbServerPort* (factory setting 32032). If the *UsbServerPort* is reconfigured via Web Based Management in the USB-Server, the specification *TCP-Port* must be changed accordingly in the Properties dialog box.

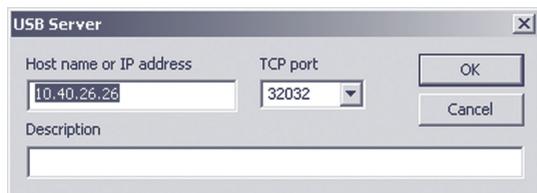
The search is carried out automatically each time the configuration tool is started and when creating a new list using the *File* → *New* function. A manual search can be performed at any time by clicking the *Scan*  button.



Automatic inventoring is done using UDP port 8513 and the TCP UsbServerPort configured in the USB-Server (factory setting = 32032). Any firewall or security software installed in the respective computer must permit this communication.

5.3.2 Manual entries in the configuration list

Remote USB-Servers connected through routers or gateways cannot be detected by the automatic scan function of the configuration tool. The entry in the inventory list must in such cases be made manually. The menu path *Devices* → *Add* opens the following dialog:



USB Server

Host name or IP address: 10.40.26.26

TCP port: 32032

OK

Cancel

Description:

Enter here the IP address or the host name of the desired USB-Server. The local TCP port on the USB-Server used for further communication is factory set to 32032. If the *UsbServerPort* is reconfigured via Web Based Management in the USB-Server, the specification *TCP-Port* must be changed accordingly in the Properties dialog box.

Clicking on *OK* adds the USB-Server to the inventory list and the configuration tool attempts to use the specified TCP port to locate the connected USB devices.

5.3.3 Saving and opening inventory lists

Especially in routed environments with manually added USB-Servers you should save created inventory lists.

The configuration tool always opens automatically at startup and checks the availability of the USB-Servers and USB devices. In addition, the local network is always searched for new devices.

Saved but no longer accessible devices remain in the list but are shown as grayed out.

5.4 Using USB devices - Plug/Unplug

To enable a USB device connected on the USB-Server in the Windows plug and play system, it must be included using the configuration tool. Compared with a local computer, this corresponds to plugging the device into a USB port. Windows then installs any existing standard drivers (e.g. many memory sticks), keyboards, etc.) or starts the search for device-specific drivers.

5.4.1 System response / conflict protection

A USB device can be used by only one PC at any given time. Only after the latter has closed the connection can the device be used by a different computer. The information as to whether a USB device is already in use can be found in the *Users* column in the inventory list.

The procedure described below for including a USB device is irrespective of any conflict. If the desired USB device is in use, the USB Port Redirector cyclically attempts to open a connection.



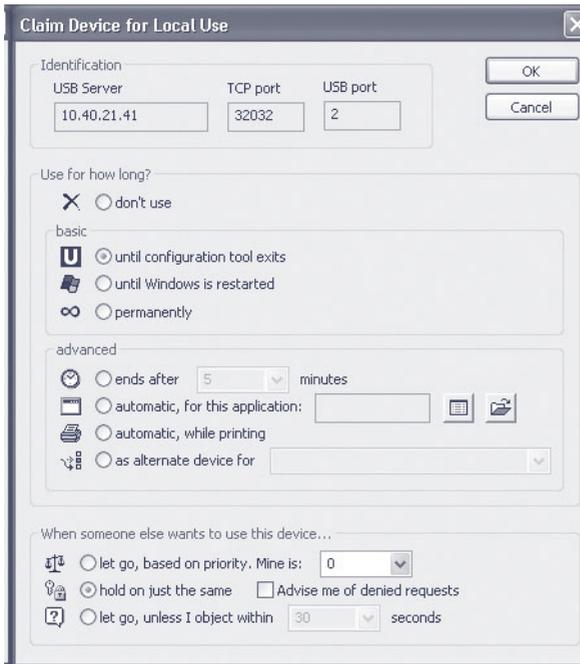
Conflict protection refers to the respective USB port to which the device is connected. This means a simultaneous access from two PCs to different USB ports is of course not a problem.

5.4.2 Adding a USB device - Plug

Select the desired USB device in the inventory list of the configuration tool and right-click on it. You can also double-click on the desired device.



The *Properties* menu opens the following dialog box:



In addition to the duration of an incorporation, events can be configured here which automatically trigger opening of a connection. In addition, you can specify the response when there are competing accesses from other computers to the added USB device. Clicking on the *OK* button after selecting the desired option opens the connection to the USB device and triggers the plug event in the Windows system.

Einbindung - einfach -

- 
 until configuration tool exits
 The USB device remains added until the connection is manually closed or the configuration tool is closed.
- 
 until Windows is restarted
 The device remains linked in the system until Windows is closed. The Start/Stop configuration tool can be closed without affecting the connection to the device.
- 
 permanently
 The USB device is linked permanently. When the computer is restarted an attempt is automatically made to link the device again. Due to the implementation as a core driver, no Windows user login is necessary.

Incorporation - expanded -

- 
 ends after minutes
 The USB device is added for the specified time. After this time expires the connection is automatically closed, so that the USB device is available for other stations.
- 
 automatic, for this application:  
 Incorporation of the USB device is linked to the start of another application. When the specified program is started the connection is opened. Ending the program re-enables the USB device.
- 
 automatic, while printing
 Incorporation of the USB device is linked to the Windows print system. The connection is established as soon as there is a print job in the Windows printer spooler. Once the print job is finished, the USB device is re-enabled.

-  as alternate device for

Incorporation as a backup device is mainly conceived for working with a dongle pool and is only available if another connection to a different USB device was already established. If the first USB device cannot be reached (e.g. is in use by another PC), an attempt is made to open the connection to the backup device.

Competing accesses

Connections to USB devices are always exclusive. This means that a competing access from a different PC is rejected by the presetting. The following options permit a controlled take-over of the USB device by a different USB Port Redirector.

-  let go, based on priority. Mine is:

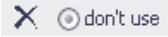
The decision whether take-over of the USB device is possible is made based on a freely selectable priority value assigned by the administrator. If the competing access has higher priority, the first connection is closed and the USB device is connected to the second PC.
-  hold on just the same

With this option no take-over of a USB device by a competing USP Port Redirector is possible. Only when the connection is closed is the USB device available to other applications.
-  let go, unless I object within seconds

The user having the connection is informed of the connection request from the competing PC in the form of a balloon notification. Within the configured time this competing access is rejected by means of the configuration tool or it is directly allowed. Use the right mouse key to select the corresponding USB device from the inventory list and select deny device take-over or approve device take-over. After the configured time has expired with no response the device take-over is automatically approved.

5.4.3 Closing a connection - Unplug

Select the desired USB device from the inventory list of the configuration tool and right-click. Alternately you can double-click on the desired device.

- 
 Clicking on the **OK** button after selecting closes the connection to the USB device and triggers the Unplug event in the Windows system.

5.4.4 Script-/batch controlled incorporation

As an alternative to the graphical configuration tool, the core driver of the USB Port Redirector can also be controlled by the command line tool *usbcontrol.exe*. This makes it possible – for example when working with dongles – to implement incorporating and deleting USB devices using batch jobs or scripts.

The tool is located in the directory for the program group *W&T USB Port Redirector*.

Entering *usbcontrol -?* provides an overview of the available commands and brief examples.

Command line commands

```
usbcontrol /ADD [/P] [/POOL <n>] <server> <port>
```

/ADD r Add a USB device

/P → Optional parameter for permanent adding of a device, even after a restart of the computer. Without this option the adding of the USB device ends when Windows is restarted.

/POOL <n> → Optional parameter for adding as a backup device for the pool named <n>.

server → IP address or hostname of the USB server

port → Port 1 or 2 of the USB server

```
usbcontrol /DEL [/POOL <n>] <server> <port>
```

/DEL → Close the connection to a USB device. By deleting the master device in a pool, all other backup devices are automatically removed as well.

/POOL <n> → Optional parameter when the corresponding addition as a backup device was accomplished for the pool named <n>.

server → IP address or hostname of the USB server.

port → Port 1 or 2 of the USB server

usbcontrol /LIST

/LIST → Provides the list of the added USB devices

usbcontrol /SLEEP <ms>

/SLEEP → Postpones further running of the batch job by the time in ms specified by <ms>.



An inventory of the USB servers and USB devices available in the network is not possible using usbcontrol. Here you need to use the graphical configuration tool of the USB Port Redirector.

Examples

The following examples for a batch job and a VBScript first add a dongle as master device when a particular application is started. If this device is already busy or for some other reason not available, two backup devices are also defined. After a 2s delay the application (*notepad.exe* in the example) is then started. After it is quit the connection to the master including all backup devices is deleted.

Batchjob

```
@REM Add USB dongle (master device + backup device) then start the
@REM licensed application. The dongle is released again at the end of the program.
Set Application=C:\Windows\notepad.exe
Set MasterDevice=10.40.41.18 2
Set AuxDevice1=10.40.21.41 1
Set AuxDevice2=10.40.21.41 2
Set UsbControl="C:\Programme\W&T USB Redirector\UsbControl.exe"

@REM Geräte einbinden
%UsbControl% /ADD %MasterDevice%
%UsbControl% /ADD /POOL 0 %AuxDevice1%
%UsbControl% /ADD /POOL 0 %AuxDevice2%

@REM Kurze Pause (in ms), dann die Anwendung starten
%UsbControl% /SLEEP 2000
%Application%

@REM Geräte wieder freigeben
%UsbControl% /DEL %MasterDevice%
```

VBScript

' Add USB dongle (master device + backup device) then start the
' licensed application. The dongle is released again at the end of the program.

```
Application = "C:\Windows\notepad.exe"  
MasterDevice = "10.40.41.18 2"  
Dim AuxDevices( 1 )  
AuxDevices( 0 ) = "10.40.26.32 2"  
AuxDevices( 1 ) = "10.40.26.33 2"  
  
UsbControl = ""C:\Programme\W&T USB Redirector\UsbControl.exe""  
  
Set WShell = CreateObject( "WScript.Shell" )  
  
' Geräte einbinden  
WShell.Run UsbControl & " /ADD " & MasterDevice, 0, True  
For Each Dev in AuxDevices  
    WShell.Run UsbControl & " /ADD /POOL 0 " & Dev, 0, True  
Next  
  
' Kurze Pause (in ms), dann die Anwendung starten  
WScript.Sleep 2000  
WShell.Run Application, 1, True  
  
' Geräte wieder freigeben  
WShell.Run UsbControl & " /DEL " & MasterDevice, 0, True
```


6 Web-Based-Management

The W&T USB-Server configuration is Web-based and can be opened using any Web browser. WBM (Web-Based Management) is session-oriented. This means all changes made are first temporarily buffer stored and not saved in the non-volatile Setup of the USB-Server until a final save function has been performed.

- Navigation within the WBM
- List of connected USB-Devices
- Network basic parameters
- Diagnostic functions

6.1 Starting and navigating the WBM

To access the WBM of the USB-Server, start your Internet browser and enter the IP address of the USB-Server and a port number if appropriate.

http://[IP-Adresse]:[port number]

The factory default setting is for HTTP standard Port 80. In this case you do not need to enter the port number in the address line.

6.1.1 Navigation concept of the USB-Server

The WBM of the USB-Server is session-oriented using a password-protected login. Without a login the start page simply shows basic information but does not permit any changes to the settings.

After logging in you can make any number of settings during a configuration session. Clicking on the *Apply* button on the respective pages causes them to be temporarily stored by the USB-Server. Once all the settings have been made, exit the configuration session and use *Logout* and click on *Save*. Only now are all changes sent to the non-volatile memory of the USB-Server and activated..

You can exit a configuration session at any time without saving your changes by clicking on the *Cancel* button.

6.1.2 The Start page of the USB-Server

The basic structure of the Web pages in the USB-Server is divided into the navigation tree on the left side and the main frame with the contents of the respective menu branch on the right side.



Home

USB-Sever-06305d

 Refresh					
USB Device	Manufacturer Name	USB Speed	Connected PC	Duration (H:M:SEC)	Port
No USB-Devices in list					
0 USB-Devices					

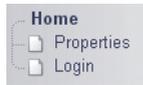
Without logging in you can view a list of the connected USB devices with their associated information. In addition, the menu branch *Doc* provides access to the quick user's guide, the data sheet and the Properties page with device-specific information.

6.2 WBM - configuration sessions

Setting on the W&T USB-Server are made within password-protected configuration sessions. These are exclusive, i.e. only one session can be active at a time.

6.2.1 Login

The *Config* link in the navigation tree takes you to the login page of the USB-Server.



In its factory default setting the USB-Server does not require a password. In this case the *Password* entry field remains blank, and clicking on the *Login* button starts a configuration session. If a password as assigned by the user, it must of course be entered.

Login

A screenshot of the login page. It features a 'Password' label next to a text input field. Below the input field is a 'Send' button.

After successful login an expanded configuration tree appears.



6.2.2 Logout

Quit a configuration session by using the *Logout* page of the USB-Server.



All functions except for Cancel cause any connections from PCs to connected USB devices to be closed. To prevent data loss, we recommend any users listed on the homepage of the USB-Server to be previously notified.

Save

... closes the session and saves all changes made to the non-volatile memory of the USB-Server. If the changes require restarting the device, this is automatically performed.

Logout

... closes the session and cancels all changes.

Factory defaults

... closes the session and reverts to the settings of the USB-Server. All settings which are different from the default values including the network parameters are lost.



In environments with static network parameters (no DHCP) assigning the new IP address can be done only from a workstation which is located in the same subnet as the USB-Server.

Restart

...closes the session without saving any changes and restarts the USB-Server.

6.3 WBM - Assigning passwords

The password may be up to 32 characters and protects the following configuration accesses to the W&T USB-Server.

- Web Based Management
- Uploading configurations
- Firmware update
- Reset Port
- Setting using WuTility

 *Deleting an unknown or forgotten password to the can only be done by a hardware reset of the USB-Server to its default settings.*

Configuration → *USB-Server 2* → *password* in the navigation tree takes you to the Web page for assigning or changing the password.



To create or change a password you must first activate the *Change password* option. The new password must then be entered twice in both input fields. *Send* applies the change temporarily. To permanently store the change in non-volatile memory, use the logoff page and click on *Save*.

Change password	<input type="checkbox"/> Check here for modifying the password
Password	<input type="text"/>
Re-enter	<input type="text"/>

6.4 WBM - Network basic parameters

Configuration → *USB-Server 2* → *LAN* in the navigation tree takes you to the Web page with the network-side basic parameters.



 ***Saving changes made here closes any connections from PCs to connected USB devices. To prevent data loss, we recommend any users listed on the homepage of the USB-Server to be previously notified.***

Enable DHCP	<input type="checkbox"/>	Activates automatic IP-settings via DHCP
IP-Address	<input type="text" value="10.10.10.1"/>	Scheme: xxx.xxx.xxx.xxx
Subnet Mask	<input type="text" value="255.255.0.0"/>	Scheme: xxx.xxx.xxx.xxx
Gateway	<input type="text" value="10.10.10.2"/>	Scheme: xxx.xxx.xxx.xxx

Enable DHCP

In *DHCP* mode the USB-Server obtains the network-side basic parameters IP address, subnet mask and gateway address from a DHCP server located in a network. In *Static* mode these parameters are determined statically using the following entry fields. Detailed information about both modes can be found in the sections *DHCP Mode* and *Static Mode*.

IP-Address

For entering the IP address when DHCP is disabled.

Subnet Mask

For entering the subnet mask for the respective network when DHCP is disabled.

Gateway

For entering the gateway for the respective network when DHCP is disabled.



Valid values for IP address, subnet mask and gateway can be obtained from your network administrator. If you assign the IP address yourself, be sure that there are no address conflicts with other devices.

6.5 WBM - Netzwerk services

From *Config* → *USB-Server 2* → *Network Services* you can configure and deactivate all TCP/UDP port numbers of the USB Server network services.



 **Changing and deactivating the services listed here can result in failure of application, configuration and help services. We therefore recommend using caution when making changes here and documenting those changes.**

6.5.1 Web access - Web-Based-Management

activate Web-Access	<input checked="" type="checkbox"/>	Higher security when using HTTPS
Protocol	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS	
HTTP-Port	<input type="text" value="80"/>	
HTTPS-Port	<input type="text" value="443"/>	
Personal HTTPS certificate	<input type="checkbox"/> (No certificate file existing)	
Private-key	<input type="text"/> <input type="button" value="Browse ..."/>	
HTTPS-certificate	<input type="text"/> <input type="button" value="Browse ..."/>	

Web access allows you to configure the USB Server with the help of a browser. By factory default the HTTP protocol is set to standard port 80. In security-critical applications you

may choose to use the encoded and certificate-based HTTPS protocol.



Deactivating web access or entering unknown values here may cause the USB Server to be no longer configurable. Resetting these parameters to their standard values is then possible only by means of a hardware reset to the factory settings.

6.5.2 USB-Server service

Enable USB-Server Service	<input checked="" type="checkbox"/>
USB-Server-Port	<input type="text" value="32032"/>

The USB Server service is used to enable the actual data exchange between the USB Redirector and the overlaid device drivers and USB terminal device. The port number used must be the same as used in the USB Redirector. Once a service is deactivated, a connection to connected USB devices is no longer possible.

6.5.3 Reset port

Enable Reset-Port	<input checked="" type="checkbox"/>	
Reset-Port	<input type="text" value="8888"/>	Reset über TCP-Port zulassen?

The Reset port configured here can be used to perform a reset of the USB Server. If no password is configured, the USB Server first accepts the connection but then immediately closes it again and carries out the reset. If a password is assigned, it must be sent to the USB Server with a null terminator within 2s after the TCP connection is established.

6.5.4 Firmware update permission

Allow Firmware-
Update

If this service (TCP port 2682) is enabled, the inventoring and management tool *WuTility* can be used to send new firmware to the USB Server. In addition, the *WuTility Management service* must be enabled to perform an update.

6.5.5 WuTility management

Activate WuTility-
Management

This service on UDP port 8513 allows *WuTility* as well as the USB Redirector to automatically detect USB Servers connected in the local network.

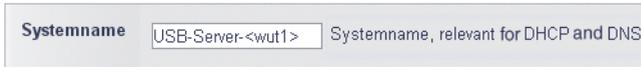
6.6 WBM - Device information and WBM adjustments

From *Config* → *USB-Server 2* → *Info/Language/Manufacturer* you can adapt informal texts and descriptions (location, service contact, installer etc.) for the USB Server.



Except for the system name these texts have no effect on the operation and function of the device.

6.6.1 System name



From *Config* → *USB-Server 2* → *Info* you can change the system name of the USB Server. This is invoked and used by the following applications and services:

- DHCP
- USB redirector
- WuTility

To generate a unique system name the placeholder tag `<wut1>` can be used. When invoking or outputting the system name the USB Server automatically replaces this tag with the last three places of the MAC address.

7 Appendix

- **Up-/downloading configuration data**
- **Firmware update**
- **Reset to factory default settings**
- **Used ports and network security**
- **Technical data**

7.1 Up-/Downloading the configuration data

WuTility allows you to read the configuration profiles from the USB Server and also send them back. This is a way to archive more complex setting profiles and/or load them into other devices as needed.

The USB Server provides the configuration data as an xml file in a compressed archive. This makes it possible to modify the data using a text editor before uploading to another device.



When uploading configuration profiles using WBM the USB-Server receives all the settings contained in the XML file including the basic parameters IP address, subnet mask and gateway address. If you want these settings to remain unchanged, the XML file must be modified accordingly before upload using a text editor.

7.1.2 Up-/Downloading the configuration using WuTility

After starting *WuTility* first highlight one or more USB servers in the inventory list.

Ethernet address	IP address	Product ID	Product name
00c03d:049568	10.40.21.22	#53641	USB Server Industry
00c03d:04ab42	10.40.26.95	#53641	USB Server Industry
00c03d:969696	10.40.41.18	#53641	USB Server Industry

Upload or download from the following menu paths:

Configuration	Firmware	Options	Help
Read and save as...			
Restore previously saved...			

The downloaded configuration profiles are named by default using the IP address of the devices.



To avoid address conflicts the USB Servers ignore the IP address contained in the configuration file. All other parameters are copied.

7.2 Firmware update

The operating software of the USB-Server is constantly being improved. The following section describes the procedure for uploading the firmware.

7.2.1 Where is the current firmware available?

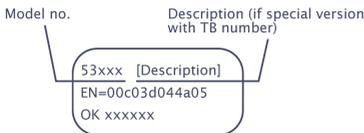
The latest firmware including the available update tools and a revision list is published on our Web site at the following address:

<http://www.wut.de>

The easiest way to navigate there is to use the Search function on the left side. First enter the model number of your device in the entry field. Select *Firmware* in the associated selection box and then click on the *Go* button.



If you do not know the model number, you can find it on the sticker on the narrow side of the housing. There the Ethernet address is also printed.



7.2.2 Firmware update under Windows

A firmware update requires that the services *Enable firmware update* and *WuTility-Management* be activated in the USB Server (see section *WBM - Network services*). No other preparation is needed for the USB Server.

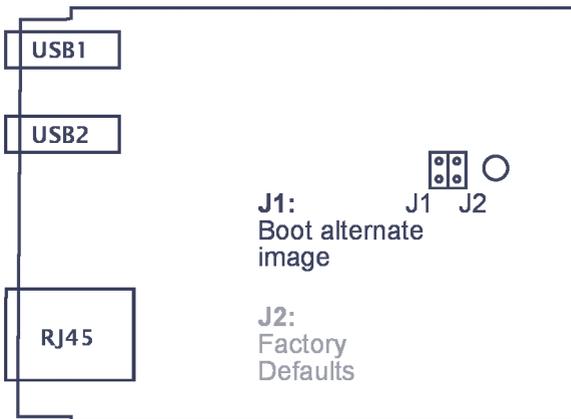
New firmware is sent to the USB-Server using the WuTility management tool. In the inventory list highlight the desired USB-Server and then click on the *Firmware* button.



In the following dialog box you select only the firmware file you want to send (*.uhd) and then click on the *Continue* button. After successful sending the USB-Server automatically performs a restart and is then ready to use.

7.2.3 Interrupted updates, alternate image

If a firmware update is unsuccessfully finished, for example due to an interrupted network connection, the USB Server will then no longer be functional. In this case bridging jumper J1 at the next system start will reactivate the previous firmware. A subsequent and complete firmware update will restore the corrupted image.



7.3 Resetting the USB-Server

If the USB-Server needs to be reset without changing its settings, socket 8888 can be used. If a connection is opened to this port the USB-Server immediately closes it again and then performs a restart of the firmware.

Use of the system password

If a system password has been configured, this must be null terminated (= [*password*] + 0x00) and sent to the USB-Server within 2s after a successful connection opening. If the USB-Server receives an incorrect or no system 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 USB-Server, as described in the example, immediately closes the TCP connection after it is opened and performs a reset.

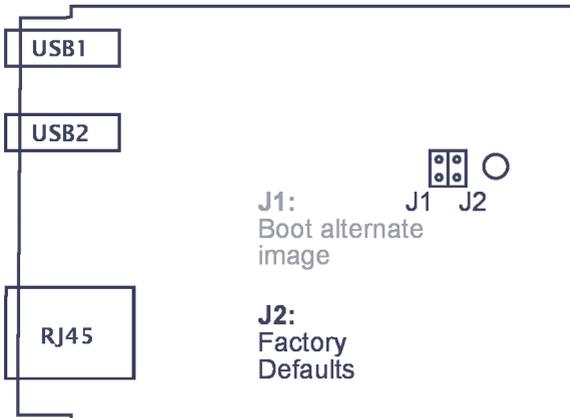
7.4 Reset to factory defaults

The USB-Server can be reset to its factory default settings using the following methods.

7.4.1 Hardware reset to factory default settings

The motherboard of the USB Server has two adjacent jumpers which are both open for standard operation. To reset to the factory default settings close only J2 and then connect the USB Server to power.

The multicolor LED will pulse blue until the reset is completed. If the multicolor LED is a continuous blue, open J2 again and perform a power-down reset. The USB Server will now be restored to its factory default settings.



Opening the housing

First disconnect all cables from the USB-Server. Open the DIN rail mount housing by gently pressing on the narrow sides of the housing. The housing cover can now be removed and the board removed from the housing body.

7.4.2 Software reset to factory default settings

In addition to the hardware method, the USB-Server can also be restored to its factory default settings using Web-Based-Management. After Login the *Factory Defaults* button is visible in the *Logout* menu branch.

7.5 Used ports and network security

In its standard factory setting the USB-Server uses the TCP and UDP port numbers shown in the table below.

Port-/Socket-number	Application	Password protection?	Configure/disable
32032 (TCP)	Data USB redirector	no	yes/yes
80 (TCP)	HTTP management	yes	yes/yes
443 (TCP)	HTTPS management (only if enabled)	yes	yes/yes
8888 (TCP)	Reset USB-Server	yes	yes/yes
2682 (TCP)	Initialize Firmware upate	yes	no/yes
8513 (UDP)	Inventory	no	no/yes
69 (UDP)	Firmware update (only after initialized through 2682)	(yes)	no



Different TCP port numbers must always be used for any reconfiguration of the factory default setting for USB data transmission services and the WBM.

The USB-Server and network security

Network security is being given increasing attention today, and rightly so. All experts agree that there is no such thing as absolute security given today's state of the art. Each customer must therefore seek an appropriate balance between security, functionality and cost for his specific needs and circumstances.

To give the customer the greatest possible flexibility based on changing security requirements, from a purely testing and installation environment to critical production applications, the security measures are highly configurable. The present document provides an overview of the security measures implemented in USB-Servers which can be used. It is assumed that the original firmware from W&T (without any customer-specific adaptations) is being used. Additional details can be found in the respective sections of this manual.

The authorization concept of the USB-Server

The control and configuration access to the USB-Server is password protected. The factory default setting is for *no* password, so that simply logging in provides full access to the corresponding settings and functions. To prevent unauthorized access, we therefore strongly recommend using a password. Additional related measures, such as the composition of the password and regularly changing it, should be organizationally ensured as needed by the customer.

Passwords are sent to the USB-Server unencrypted. It must therefore be ensured that password-protected access takes place only using an Intranet which the customer presumes to be secure. For access over the public Internet additional measures must be taken, for example constructing a VPN tunnel (Virtual Private Network). This is however a general problem of network security for which each customer must find an individual solution.

Ports with special functions

In addition to access using Web Based Management, other functions can be enabled using various TCP and UDP ports. These are shown in the previous table. Details can be found in the corresponding sections of this manual.

- **Inventorizing tool WuTility**

Like all intelligent components from W&T the USB-Server can be accessed using the *WuTility* tool. Here information is read from UDP port 8513. This port can be turned off. No write access is possible through this path.

- **Firmware-Update**

(see section *Firmware-Update*)

Initializing a firmware update is handled by the system password protected TCP port 2682. Nach erfolgreicher Initialisierung werden die eigentlichen Firmwaredateien dann per TFTP (UDP/69) an den USB-Server übertragen. For a firmware update only the operating system of the

USB-Server is updated. The configuration data (IP address, gateway etc.) remain intact.

- **Reading/writing the configuration data**

(see section *Up-/downloading the configuration data*)

The configuration profiles can be read from and written to USB-Servers using the WuTility tool. This is done using the TCP port reserved for Web-Based-Management.

- **USB-Server reset**

(see section *Resetting the USB-Server*)

TCP port 8888 permits a complete reset of the USB-Server. The port is configurable, can be disabled and is password protected.

7.6 Technical data

Supply voltage ... Power over Ethernet External supply	37 - 57V DC from PSE DC 24V - 48V (+/-10%)
Current draw ... Power over Ethernet Ext. supply without USB devices	PoE Class 3 (6,49-12,95W) typ. 90mA @24V DC
Network	10/100BaseT, autonegotiating RJ45 STP
Galvanic isolation	Network: min. 500V
USB ports	2 × Type A
USB speed	480 Mbit/s
Permissible ambient temperature storage ... operating, non-cascaded ... operating, cascaded	-40 ... +85° C 0 ... +70° C 0 ... +60° C
Permissible relative humidity	0 - 95% (non condensing)
Dimensions	ca. 200g
Weight	105 × 75 × 22mm

7.7 Licenses

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you

conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the

entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you

may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions

either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Index**A**

air circulation 8
Angefordert 41
authorization concept 74

B

Batchjob 50
Beschreibung 41
Bulk transfer 31

C

conflict protection 44
Control transfer 31

D

default IP address 11
DHCP 16, 17, 18, 59

E

Using USB devices 44
Ethernet connector 29

F

Factory defaults 71
Firmware Update 68
Full duplex 30
Full speed 31

G

Gateway 60

H

Half Duplex 30
High speed 31
Hot plugging 31

I

Identification 41
Interrupt transfer 31
Inventory list 41
IP address 15, 60

K

Configuration sessions 56

L

Lease-Time 19
Link-Status 29
Low speed 31

M

Installation 8

N

network parameter 11
Network security 73
Network connection 9

O

Opening the hosing 71

P

Password 58
Plug 44
Port 41
Portnumbers 38
Power management 28
Power supply 28

Q

Quickstart 7

R

Requested USB device 41
Reset 70

S

Skriptgesteuerte Einbindung 48

Spannungsversorgung 28

Static IP 17, 22, 59

Subnet mask 60

System Name 19

Systemübersicht 33

T

Technische Daten 76

U

Unplug 48

USB interface 31

USB modes 34

USB port 34

USB Port Redirector 12

USB-Schnittstelle 31

usbcontrol 48

V

VBScript 51

W

WB - Logout 56

WBM 54

WBM - Login 56

WuTility 11, 22