W&T

www.WuT.de

Manual

Installation, Startup and Application

USB-Server

valid for

#53663	USB-Server Gigabit 2.0 (from firmware 2.00)

Release 2.00 11/2022

Subject to error and alteration:

Since it is posssible that we make mistakes, you mustn't use any of our statements without verification. Please inform us of any error or misunderstanding you come about, so we can identify and eliminate it as soon as possible.

Carry out your work on or with W&T products only to the extent that they are described here and after you have completely read and understood the manual or guide. We are not liable for unauthorized repairs or tampering. When in doubt, check first with us or with your local distributor.

Inhalt

1. Legal notices

Warning notice system

This manual contains notices that must be observed for your personal safety as well as to prevent damage to equipment. The notices are emphasized using a warning sign. Depending on the hazard level the warning notices are shown in decreasing severity as follows.

⚠ DANGER

Indicates a hazard which results in death or severe injury if no appropriate preventive actions are taken.

⚠ WARNING

Indicates a hazard which can result in death or severe injury if no appropriate preventive actions are taken.

⚠ CAUTION

Indicates a hazard that can result in slight injury if no appropriate preventive actions are taken.

⚠ NOTE

Indicates a hazard which can result in equipment damage if no appropriate preventive actions are taken.

If more than one hazard level pertains, the highest level of warning is always used. If the warning sign is used in a warning notice to warn of personal injury, the same warning notice may have an additional warning of equipment damage appended.

Some additional information is also highlighted in this manual:

i **General Information**
General information concerning the following paragraphs.

Reference
A reference to a source for more detailed information.

Product
The following paragraphs are tailored to a specific product.

Audience
The following paragraphs are primarily intended for a specific audience.

Qualified personnel

The product described in this manual may be installed and placed in operation only by personnel who are qualified for the respective task.

The documentation associated with the respective task must be followed, especially the safety and warning notices contained therein.

Qualified personnel are defined as those who are qualified by their training and experience to recognize risks when handling the described products and to avoid possible hazards.

Intended Use

The USB-Servers produced by Wiesemann & Theis provide a universal hardware platform to connect USB devices to the network.

Every other usage or modifications of the hardware are not considered intended use.

Disposal

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

Symbols on the product

Symbol	Explanation
CE	CE-Mark The product conforms to the requirements of the relevant EU Directives.
	WEEE-Mark The product may not be disposed of with normal waste, but rather in accordance with local disposal regulations for electrical scrap.

Electrical safety

The USB-Server Gigabit 2.0 may only be used in enclosed and dry areas. The device should not be exposed to high ambient temperatures and not be operated near heat sources. Please note the restrictions regarding the maximum ambient temperature.

The power supply unit used to power the respective USB-Server Gigabit 2.0 must guarantee a safe separation of the low voltage side from the grid in accordance with EN62368-1 and have „LPS“ characteristics.

Input voltage and output currents must not exceed the rated values in the specification.

Ventilation openings must be clear of any obstacles. A distance of 10-15 cm between the USB-Server Gigabit 2.0 and nearby heat sources must be maintained.

When installing, be sure that no stray wires stick through the ventilation slits of the USB-Server Gigabit 2.0 into the housing.

EMC

Only shielded network cables may be used for connecting the USB-Server Gigabit 2.0 to the network.

Only shielded cables may be used for connecting the USB-Server Gigabit 2.0 to USB

devices.

In this case the USB-Server Gigabit 2.0 meets the noise immunity limits for industrial applications and the stricter emissions limits for households and small businesses. Therefore there are no EMC-related limitations with respect to the usability of the devices in such environments.

Declarations of conformity
The complete Declarations of Conformity for the devices described in the manual can be found on the corresponding Internet page at the W&T homepage: http://www.wut.de.

1. Quickstart

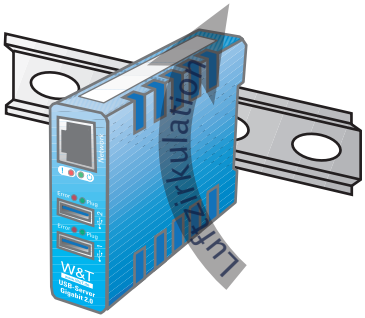
For customers already familiar with the W&T USB-Server the following pages feature a quick start guide with the basic steps neccessary from hardware installation to a working setup of the USB Server and the USB redirector software.

Additional Information
A more detailed explanation of the individual steps is available in the respective sections.

Step 1: Hardware installation

Mounting

The housing of the W&T USB-Server is designed for on a standard DIN rail.



⚠ NOTE

A lack of appropriate air circulation may cause damage to the USB Server

- Ensure the air flow depicted above is not blocked during operation of the device, especially when operating in conditions at elevated temperatures.

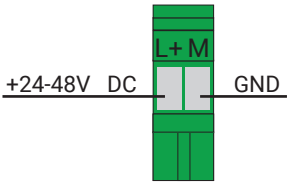
- Alternate mounting methods must still ensure the depicted air circulation

Power supply

Power may be supplied either via

- a PoE capable network environment or
- using a separate power supply of 24-48 VDC (+- 10%).

Please take note of the correct polarity when connecting the external power supply:



Network connection and USB devices
Use a standard patch cable to connect the USB-Server to the network and plug your desired USB devices into the USB ports of the USB-Server, just as with a local USB port.

After the hardware setup has been completed the USB-Server should start booting. Once the booting process has finished the link and activity LEDs of the network connector should indicate a working link and the system LED of the USB-Server should turn on.

Step 2: Setting up the network parameters

The USB-Server comes pre-configured with an activated DHCP client. Should your local network use DHCP for IP-address management you may continue with step 3 without any further action required.

Network settings with WuTility
The pre-configured default IP-Address of the W&T USB-Server is

```
190.107.233.110
```

Install the management-tool WuTility available from the product CD included with the USB-Server on a Windows-PC. The PC has to be connected to the same subnet as the USB-Server.

The WuTility-Tool will automatically scan the network for connected W&T devices on startup. Select your USB-Server form the list of found devices and click on the *IP Address* button in the tool bar of the WuTility application.

The newly opened dialog gives you the option to set the USB-Server into static IP mode for manually assigning IP-address, subnet mask and gateway. Enter the values in accordance to your local network setup and confirm using the *OK* button.

The USB-Server will accept the new settings and automatically perform a reboot. After approximately 30 seconds the USB-Server should be available with the new IP parameters and can be found e.g. by performing a new scan with WuTility.

IP assignment
A more detailed description of the available methods for assigning the network parameters can be found in the section *Assigning/Changing IP Parameters*.

Step 3: Installating the W&T USB-Redirector

Install the W&T USB Redirector on the desired Windows-PC (Windows 7 or higher). You can download the installer from the USB-Servers web interface or from the online datasheet at *http://www.wut.de/53663*

The installation requires adminstrator privileges on the Windows-PC.

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

i **WHQL Certification**
To allow publishing of updates of 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*. If you need a WHQL certified version, please contact your local distributor or W&T directly.

Installation
More details concerning the installation of the W&T USB Redirector can be found in the section *The W&T USB-Redirector*.

Step 4: Connecting to a USB-Device

The configuration tool can be started from the program group W&T USB Redirector. The local subnet will automatically be scanned for W&T USB Servers and attached USB devices on startup.

i **Inventory**

Should the Windows-PC and the USB-Server not be connected to the same subnet, the USB-Server has to be manually added to the inventory via the menu bar option *Devices → Insert New*

Quick connecting to a USB device

Select the desired USB device in the inventory and use the Claim button in the tool bar. Similar to a local connection the USB device is now inserted 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.

In the default configuration USB devices claimed using the quick connect will be released when closing the configuration tool or by using the Release button in the tool bar. After releasing a USB device it may be claimed again by other users.

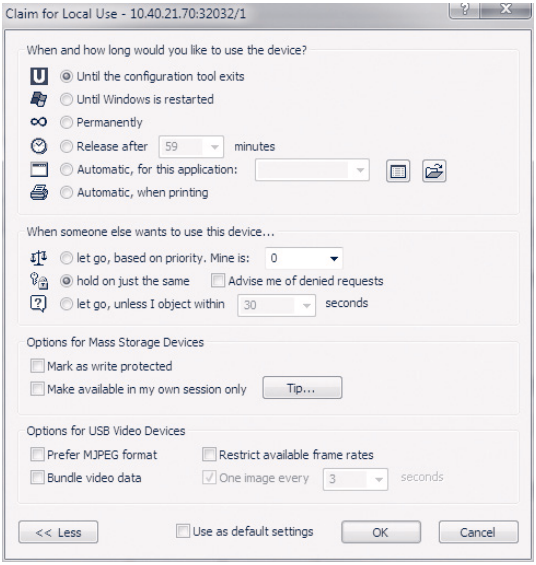
i **Claim settings**

The type of connection can be configured more thoroughly using the *Advanced* button in the tool bar. The pre-configured default setting is „until the configuration tool exits“

Advanced incorporating settings

This dialog provides advanced options for incorporating and enabling the USB device. For example, the device can be claimed even before a user login in WIndows by using a permanent connection.

Other options include time-limited incorporation, automatic incorporation when running certain programs or print jobs, rules for competing access to USB devices and camera specific modes.



USB Redirector

More details concerning the different options of the W&T USB Redirector can be found in the section *The W&T USB-Redirector*.

2. Assigning/Changing IP Parameters

After the hardware installation of the USB-Server, the IP address and other network settings, such as the subnet mask and gateway, have to be set according to the local network environment. Please ask the local responsible system administrator for valid settings for your application.

The pre-configured IP-Address of the USB-Server 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 the DHCP protocol
- Changing the IP parameters using Web-Based-Management

2.1 Managing the USB-Server network parameters

The USB-Server can be operated in two different modes with respect to its network parameters.

Static
IP address, subnet mask and gateway are stored in the non-volatile setup of the USB-Server, and the 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 settings)
The 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 is available or the attempt to obtain an IP address is rejected, the USB server operates using the factory default fallback 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 Operation with DHCP

Many networks are setup for centralised and dynamic assignment of network settings via DHCP (Dynamic Host Configuration Protocol). In its delivery state and after a reset to factory default settings the USB-Server acts as an DHCP client. This way, it is often sufficient to connect the USB-Server to the local network and the IP parameters are dynamically assigned. The following parameters can be configured using DHCP:

- IP address
- Subnet mask
- Gateway

i **Discovery of devices**
Should the USB-Server have inadvertently accepted IP parameters from a DHCP server it is always possible to find the current settings using the management tool WuTility. The same tool can also be used to set the USB-Server into static mode of operation, allowing the user to set the IP parameters to a valid state.

2.2.1 Activating DHCP mode

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

- **Activating using the management tool WuTility**
  Select the desired USB-Server in the device list and click on the IP Address button. In the following dialog window check the radio button DHCP and then confirm with the Continue button.
- **Activating using Web Based Management**
  In the menu Home → Config → USB-Server → LAN select the option *Enable DHCP* and click on the Send button. To save the new setting in the USB-Server, select Logout and Save.

i **DHCP**
Switching from Static to DHCP mode causes the device to revert from the static 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 subnet.

2.2.2 Deactivating DHCP mode

DHCP mode is deactivated by switching from DHCP mode to Static mode using the WuTility Tool or the 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.

- **Deactivating using the WuTility management tool**
  Select the desired USB-Server from the device list 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.
- **Deactivating using Web Based Management**
  In the menu Home → Config → USB-Server → LAN deactivate the Enable DHCP option. After entering the new IP address as well as the valid subnet mask and gateway address click on the Send button. Clicking on Logout and Save saves the new settings in the USB-Server and the device can be accessed using the new IP address.

2.2.3 System name

To support automated updating of the DNS system using the DHCP server, the USB-Server identifies itself with its system name within the DHCP protocol. The factory default name is *USB-Server-* followed by the last three bytes of the Ethernet address. For example the factory default 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 duration for which the assigned IP address is valid. 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 a cyclical search for alternate DHCP servers is started.

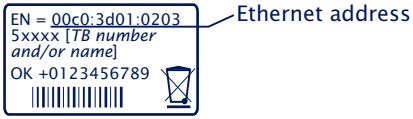
Because the USB-Server has no realtime clock installed, the lease time for the current IP address is lost on reset. After the restart a corresponding update request is sent to the original DHCP server. If the server cannot be reached at this point in time, the USB-Server deletes the IP address and reverts to the factory default address 190.107.233.110. At the same time a cyclical search for alternate DHCP servers is started.

In DHCP mode the remaining lease time as well as the current IP address is displayed on the Web page Home → Properties.

i **Reserved DHCP addresses**
A reset to the factory-side IP address 190.107.233.110 causes all open connections to W&T USB Redirectors to be closed. To prevent faults of this kind we recommend using reserved IP addresses in the DHCP server.

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 W&T USB Redirectors. Since the IP address of the USB-Server is needed to open such a connection, it is often useful to reserve a known IP address for the USB-Server in the DHCP server settings. 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 slim side of 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 of operation

In static mode the USB-Server uses static network parameters and the 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 scanning for and managing USB-Servers, e.g. by altering the following network settings:

- IP address
- Subnet mask
- Gateway address
- Switching between static and DHCP

To assign these parameters the PC and USB-Server must be located in the same physical subnet, i.e. the USB-Server and PC may not be separated by a router. Even if the current parameters of the USB-Server do not match the subnet settings of the PC, WuTility is able to reach the USB-Server as long as no routing needs to take place. Any system password set in the USB-Server must, however, be known.

Installation of WuTility

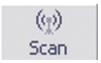
The current version of WuTility is available for download at https://www.wut.de/wutility

After the installation, WuTility can be started from the start menu at

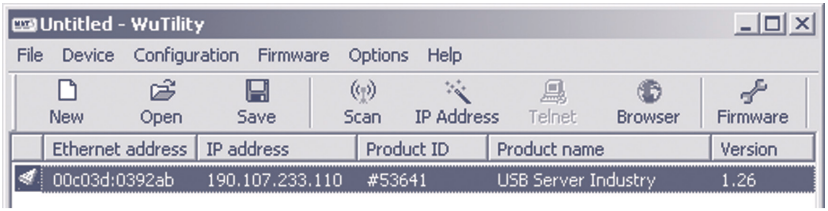
Start → Programs → Wutility Version 4 → WuTility

Starting the assignment dialog

Make sure that both the USB-Server and the computer are connected to the same physical subnet. 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:

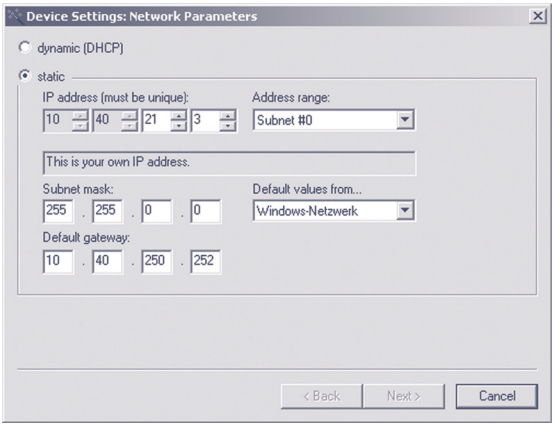


Within the inventory the desired USB-Server can be identified by its MAC address. For initial installations the IP address is 190.107. 233.110.



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, subnet mask and gateway address.



Should the USB-Server have a passwort set, you may at this stage be prompted to enter the system password. Then the network parameters are stored in the USB-Servers non-volatile memory.

All further settings are made using Web-Based-Management of the USB-Server and your browser of choice. To open the USB-Servers web interface select it in the inventory and click on the Browser button in the tool bar:

i **Web-Based-Management**

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

i **System password**

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

In its delivery state and after a reset to the factory default settings the USB-Server operates in DHCP mode. As long as no address is assigned by a DHCP server, the USB-Server can also be reached by 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 only be done one after the other. Only after a USB-Server has received its new IP address can the next USB-Server be connected to the network. Please check with the responsible network administrator to check the new network settings against your local network setup.

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

Finally, start your browser of choice and enter the URL http://190.107.233.110 in the address line. You can now change the network settings to the desired values using the USB-Servers web interface.

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. Connecting an external supply voltage and a PoE infrastructure at the same time is not permitted.

The current draw can be found in the technical appendix.

3.1.1 PoE-Supply

The model 53663 USB-Server is suitable for use in PoE environments according to IEEE802.3af. Here the supply voltage is supplied 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.

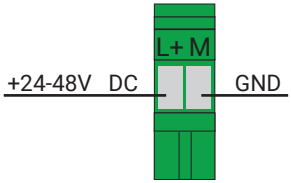
The USB-Server identifies itself as a Power Class 3 device (power consumption from 6.49W to 12.95W).

3.1.2 External Supply

As an alternative to PoE, the USB-Server can also be powered via the plug-in screw terminal located on the bottom side of the housing. The DC voltage used must be 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:



⚠ NOTE

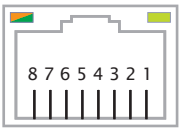
Only potential-free power supplies may be used for powering the model 53663 USB-Server. Their reference ground for the output voltage must not have a direct connection to the PE conductor.

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 state

The link state is indicated by the two LEDs built into the RJ45 receptacle.



Pin	Richtung	Funktion
1	Out	Tx+
2	Out	Tx-
3	In	Rx+
4	In	Vcc positive
5	In	Vcc positive
6	In	Rx-
7	In	Vcc negative
8	In	Vcc negative

- **Speed/Activity**
  Green <=> 1.000Mbit/s link
  Green, blinking <=> 1.000Mbit/s link with activity

  Orange = 100Mbit/s link
  Orange, blinking <=> 100Mbit/s link with activity

- **FD/HD**
  ON <=> Full-Duplex link
  OFF <=> Half-Duplex link

3.2.2 100/1000BaseT

The network connection is made using the shielded RJ45 socket and a max. 100m long shielded patch cable. The autocrossing function allows both 1:1 and crossed patch cables to be used.

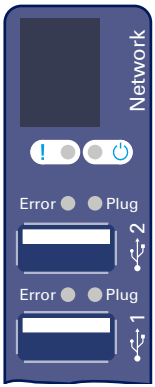
The network connection is galvanically isolated from the supply voltage and the USB ports to at least 500V_{RMS}.

Auto Negotiation: 10/100/1000BaseT, Full/Half Duplex

In its factory default setting the USB-Server uses Auto-Negotiation mode. To prevent communication problems caused by e.g. a duplex mismatch, we recommend also setting Auto-Negotiation mode the switch or hub the USB-Server is connected to. This way, 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. The overload state is indicated by the red State LED of the respective port.



USB Port

Pin	Name	Description
1	VCC	+5 V
2	D-	Data -
3	D+	Data +
4	GND	Ground

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.

i **USB Hot-Plugging**

In accordance with the USB standard, connecting and unplugging USB devices is possible at all times and permissible from a purely electrical point of view (hot-plugging). To prevent data loss, e.g. when using flash drives, we recommend disconnecting devices only when there is no active connection between a network computer and the USB device.

3.4 LED indicators

In addition to the LEDs integrated in the RJ45 connector for the network connection (see section on Ethernet connection), the USB Server has a System LED as well as two Status LEDs for each of the USB ports.

- **System-LED (green/red)**
  Green <=> Power supply and System OK
  Green, blinking<=> System start, Firmware-Update or Factory Default settings
  Red <=> System error

- **State-LEDs (green/red)**
  Green <=> The USB port is currently in use by a network connection
  Red, blinking <=> The USB-Server detected a higher than allowed current consumption, but the USB supply can still be maintained
  Red <=> The USB-Server has disabled the USB supply, due to either an overload condition or to reset the connected usb device, e.g. because the device was unplugged by the USB Redirector

4. The W&T USB Redirector

The W&T USB Redirector consists of both a virtual host controller designed as a Windows core driver as well as a corresponding configuration tool. The core driver-takes care of system-side processing of the USB handling. The associated configuration tool scans the network for available USB-Servers and allows the connected USB devices to be plugged and unplugged with just a click of the mouse.

- **System requirements**
- **Installation and uninstallation**
- **Using the configuration tool**
- **Configuring the W&T USB Redirector**

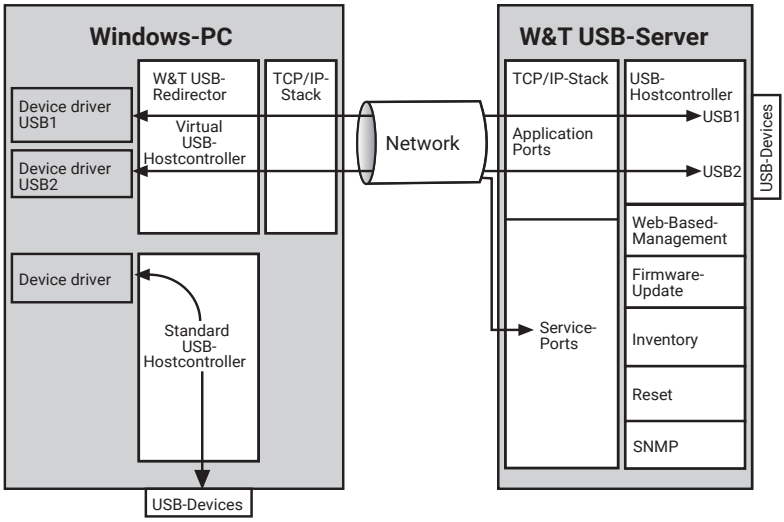
4.1 System overview

While the USB Server assumes the hardware-side adaptation, the USB Redirector is the software-side counterpart. It is implemented as a Windows core driver and, as a virtual USB host controller, represents the link between the USB Server, the Windows Plug & Play system and the device-specific drivers.

Configuration of the USB Redirector is registry-based using the USB Redirector tool in the Windows Start menu. In addition to this, it is also possible to control the USB Redirector from the commandline for script based configuration using the provided commandline tool *usbcontrol.exe*.

Script based configuration
More information regarding the script based configuration can be found in the section *Script-controlled integration of USB devices*

After successfully plugging a USB device via the USB Redirector, it will be made available to the system just as if it were locally connected. Connections to USB devices are exclusive, i.e. a simultaneous connection attempt by a competing USB Redirector will be rejected and can be established only after the prior connection has been closed.



4.1.1 System requirements

On the system side, the following requirements must be met:

- Operating system Windows 7/8/8.1/10/11 and their 64-bit and server editions
- Login as Administrator or with Administrator privileges

4.1.2 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.

4.1.3 Maximum number of USB devices

Although the 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 a maximum of 8 USB devices to be connected and incorporated through the USB Port Redirector into Windows systems. It should be noted however that some multi-function devices already present themselves as a hub to the system.

4.1.4 Port Numbers

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 (factory default = 32032). This port number can be changed from the USB Server web pages in the menu branch Home → Config → USB-Server → Network-Service

Any installed security components (software or hardware firewall, security suites etc.) must allow communication over this port number without delay. This is, however, not strictly necessary for the UDP port 8513 used for automatic inventorying. Inserting the USB-Servers can be done manually in this case.

4.2 Download & Installation

The 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 latest version is always available on our web site at http://www.wut.de

4.2.1 Downloading the W&T USB redirector

To download the latest version from our homepage, please navigate to *http://www.wut.de/53663* and follow the *Tools link*.

4.2.2 Installing the W&T USB redirector

The installation package can be run by a simple double click. In addition to the actual core driver the associated configuration and management tool is also installed and inserted into the new W&T USB Redirector program group.

i **WHQL Certification**

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*. If you need a WHQL certified version, please contact your local distributor or W&T directly.

i **Installation over an existing USB Redirector installation**

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

i **Version dependencies between USB-Server and USB-Redirector**

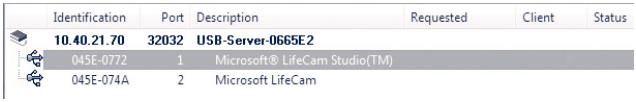
When downloading the USB Redirector, be aware of any instructions pertaining to the firmware versions of the USB Server which may be required. If necessary you may also need to also update the USB Server firmware when updating the USB Redirector.

4.2.3 Uninstalling

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

4.3 The Inventory

The inventory in the configuration tool lists the available USB-Servers with the connected USB devices along with additional information in a tree structure.



- 
  Icon for USB-Server
- 
  Icon for a USB device. This is connected to the first USB-Server shown above.

Identification
For USB-Servers the IP address is listed here. For USB devices the vendor and product ID are shown instead.

Port
For USB-Servers the TCP port used for USB data exchange is shown (factory setting is 32032). For USB devices the physical USB-tree location of the device is shown.

Description
For USB-Servers the system name is indicated here. The system name is configurable using Web Based Management and is set to *USB-Server-* followed by the last three places of the MAC address (e.g.. USB-Server-040506) by default. For USB devices the description read out via USB is shown.

Annotation
In the USB-Server setup you can assign comments to a port number (see Port column). This makes it possible to differentiate USB devices (e.g. license dongles) having the same system descriptions and same vendor/product IDs.

Any comment entered is exclusively associated with the port number and not the USB device. This means if another USB device is connected to the respective port, any previously entered comments remain intact.

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.

State
Error and status messages for the respective USB device.

4.3.1 Automatic inventory list creation

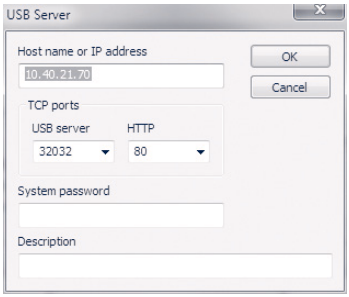
Here the local subnet is automatically scanned for W&T USB-Servers and USB devices connected to them. The inventory is done in two phases: first the W&T USB-Servers are found using a UDP broadcast (port 8513). Then any connected USB devices are queried using a TCP connection to the UsbServerPort (default setting 32032). If the UsbServerPort was reconfigured via Web Based Management on the USB-Server, the specified 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.

i **Inventory scan port**
The automatic inventory scan uses the UDP-Port 8513 as well as the configurable USB-Server TCP Port (default 32032). Should you have firewall or security software installed on your workstation, please ensure that the inventory scan is not hindered by them

4.3.2 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. In such cases, the entry in the inventory list must be added manually. The menu path Devices → Insert new opens the following dialog:



Enter the IP address or the host name of the desired USB-Server. The local TCP port on the USB-Server used for further communication defaults to 32032. If the UsbServerPort was reconfigured via Web Based Management on the USB-Server, the specified TCP-Port has to be changed accordingly in the Properties dialog box.

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

4.3.3 Saving and opening inventory lists

Especially in routed environments with manually added USB-Servers it is often usefull to save created inventory lists.

The configuration will always load the last known inventory file on startup and check the listed USB-Servers for connected devices. In additon, the local network is always scanned for new devices.

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

5. Claiming USB devices

Connections to USB devices are managed by the USB Redirector. Integrating the desired USB device incorporates it into the Plug & Play system in Windows, and the necessary drivers are installed and loaded. Afterwards, the device can be used just as if it were locally connected.

- **Quick connection of USB devices**
- **Advanced claiming of USB devices**
- **Releasing USB devices**
- **Script-controlled integration of USB devices**

5.1 System behaviour and conflict resolution

A USB device can only be used by one PC at any given time. Only after the prior connection has been closed can a new connection to the device be opened 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. In other words, integration can be accomplished in the USB Redirector even if the desired USB device is currently being used by another station. 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 to different USB ports on the same USB-Server from two different workstations does not pose a problem.

5.2 Quick claiming of USB devices

Select the desired USB device in the inventory list of the configuration tool and click the Claim button:

An immediate connection to the selected USB device is opened without any further configuration dialog. After initial installation of the USB Redirector this is done without any special options, and the connection remains open until either the Release button is activated or the configuration tool is closed.

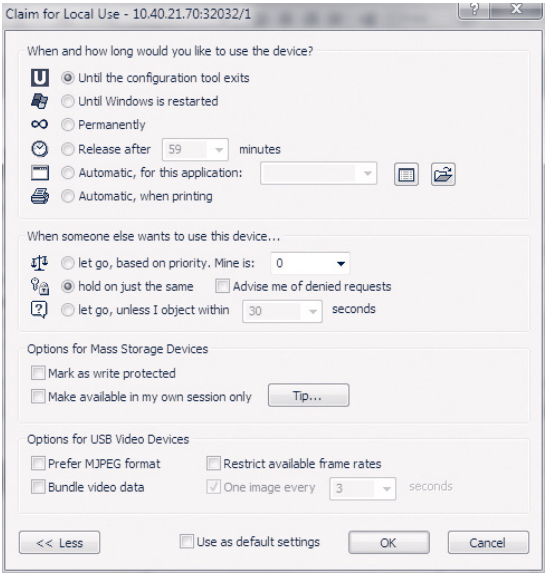
The type of connection initiated by the Claim button can be adjusted to special requirements. To do this, activate the desired options in the Advanced dialog and then check *Use as standard* at the bottom of the window.

Application examples
Application examples such as operation of dongles or cameras can be found in the appendix

5.3 Advanced claiming of USB devices

Select the desired USB device in the inventory list of the configuration tool and click the Advanced button:

Divided into the following four function groups, the Advanced dialog allows you to activate various options for claiming the USB device.



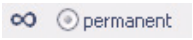
5.3.1 When/for how long do you want to use the device?

- 

The USB device remains connected until the connection is manually closed or the configuration tool is closed.

- 

The device remains linked in the system until Windows is restarted. The configuration tool can be closed without affecting the connection to the device.

- 

The USB device is linked permanently. When the computer is restarted an attempt is automatically made to link the device again on startup. Due to the implementation as a core driver, no Windows user login is necessary.

- 

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 users.

- 

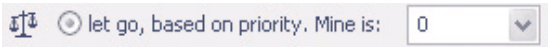
  Incorporation of the USB device is linked to the start of another application. When the specified program is started the connection is opened. Closing the application releases the device.

- 

  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 released.

5.3.2 If someone else wants to use the device

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.

- 

  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.

- 

  With this option the USB Redirector will reject any take-over attempts by competing users. Only after the connection is closed is the USB device available to other applications or users.

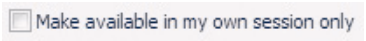
- 

  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. If the configured time expires without response the device take-over is automatically approved.

5.3.3 Options for the mass storage devices

- 

  This option designates mass storage devices as write-protected. This is only an attribute flag on the Windows level, i.e. the write access is not blocked on the USB level. In our experience, Windows system components (file system, data medium management) do, however, observe write protection activated using this method.

- 

  This option only has meaning if the USB Redirector is installed on a terminal server and the user wants to claim USB devices in terminal sessions independent of each other.

---

i **Limiting connection to own session**

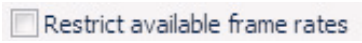
This is not a security but rather only a convenience function. It limits the visibility of devices in other sessions but cannot effectively prevent undesired cross session accesses.

5.3.4 Options for video devices

Transmission of isochronous video data streams may require a very high transmission bandwidth depending on the selected resolution and frame rate, which may exceed the available network bandwidth. For applications which do not permit suitable adjustments on the user side (frame rate, compression etc.) the USB Redirector provides the following options for bandwidth management.

- 

  If this option is activated, the USB Redirector will filter out all uncompressed video modes of the video camera and only leave compressed video descriptors available to the system.

- 

  If this option is activated, the USB Redirector will filter out video settings with a high resolution and high frame rate from the video descriptors.

- 

  In this mode the USB Server temporarily stores the individual camera frames and the USB Redirector retrieves them individually. As soon as one frame is fully received the next one is requested. As a consequence of this buffering technique, the frame rate configured in the application is reduced by about a third.

i **Bundling video data**

Bundle Video Data mode can only be activated for one port on the USB Server.

- 

  This option is only available if Bundle Video Data mode is activated. Camera frames are only retrieved at the specified frame rate. Especially for narrow-band network connections, e.g. via VPN over the internet, this option can help to prevent complete utilization of the network connection.

5.4 Releasing connections

Select the desired USB device from the inventory list of the configuration tool and click the Release button:

Clicking the button will trigger the unplug event in the Windows Plug&Play system, just like removing the USB device from a local USB port would.

5.5 Script based device claiming

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

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

Calling *usbcontrol /?* provides an overview of the available commands and brief examples.

Command line commands

```
usbcontrol /ADD [/P] <server> <port> [/MASTER <server> <port>] [/PRI
<pri>] [/IHO <sec>]
```

/ADD → Add a USB device

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

/MASTER <server> <port> → Optional parameter for incorporating as a backup device for the USP Server denoted with <server> as IP address or host name. <port> refers to the desired USB port on this Master-USB-Server (1 or 2).

/PRI <pri> → Permits a priority-based takeover of the USB device by another computer. If the competing access has higher priority, the first connection is closed and the USB device is connected to the second computer instead.

/IHO <sec> → Permits an interactive takeover of the USB device managed by the graphical configuration tool of the USB Redirector by a different computer. The current user of the connection is notified of the competing connection request by a balloon notification. Within the time specified by <sec> this attempt may be rejected or allowed by the configuration tool. To do this, right-click on the corresponding USB device in the inventory list and select accept or reject device handover. If the configured time expires without reply the device takeover is automatically accepted.

```
usbcontrol /DEL <server> <port> [/MASTER <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.

/MASTER <server> <port> → Optional parameter if the previous incorporation as backup device for the USB Server was done for the pool indicated with <server> as IP address or host name. <port> indicates the desired USB port of the master (1 or 2).

```
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>.

```
usbcontrol /SUSPEND <server> <port>
```

/SUSPEND <server> <port> → Suspends the incorporation of a USB device until the next Windows restart or until the option /RESUME is invoked. <server> indicates the IP address or host name of the USB server. <port> determines the USB port to which the USB device is connected (1 or 2). Instead of <server> and <port> a * can be entered as a wildcard. In this case all current incorporations of USB devices are suspended.

```
usbcontrol /RESUME <server> <port>
```

/RESUME <server> <port> → Undoes a previous /SUSPEND action and reincorporates the USB device. Instead of <server> and <port> a * can be entered as a wildcard. In this case all suspended incorporations of USB devices are restored.

i **Inventory**

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

Example 1

Incorporate a USB device, wait 5 seconds and then release the device again.

```
UsbControl /ADD  10.70.41.18  1
UsbControl /SLEEP  5000
UsbControl /DEL  10.70.41.18  1
```

Example 2

Incorporate a USB device and further incorporate another device as a backup device.

```
UsbControl /ADD  10.40.41.18  1
UsbControl /ADD  10.40.41.18  2  /MASTER  10.40.41.18  1
```

Example 3

Establishes a permanent incorporation of the USB device and subsequent suspension of all connections to incorporated USB devices. When Windows is restarted the connections to all permanently incorporated USB devices are automatically restored.

```
UsbControl /ADD /P   10.40.41.18  1
UsbControl /SUSPEND  *
```

6. Web Based Management

The W&T USB-Server configuration is Web-based and can be opened using any modern web browser. The WBM (Web-Based Management) is session-oriented. Any changes made on a page can be applied using the save button. The changes then take immediate effect and are stored in the persistent memory of the USB Server.

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

6.1 Starting and navigating the WBM

To access the WBM of the USB server, you need a current Internet browser. Session cookies, Javascript and WebSockets must be supported and activated. Start your internet browser and navigate to the IP address of the USB server and, if necessary, enter the port number to be used in the address bar:

http://[IP-address]:[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.

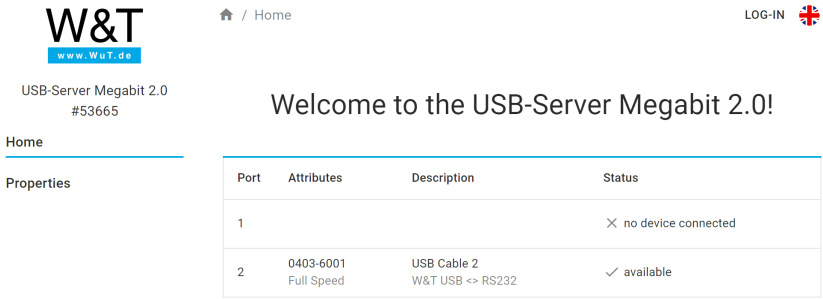
6.1.1 Navigation concept of the USB-Server

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 changes during a configuration session. Using the *save* button all changes on the current page are applied and written to the persistent storage.

You can exit a configuration session at any time by clicking on the *Logout* button in the upper right area of the page.

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.

Without logging in you can view a list of the connected USB devices with their associated information. In addition, device-specific information is available via the Properties menu branch.

After a successful login, the Start page also gives you the option of performing a reset specifically for each of the two USB ports. The reset turns off power to the corresponding port for approximately 3 seconds.

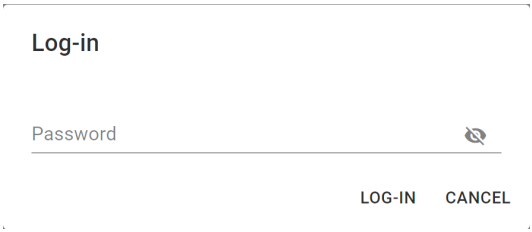
6.2 Configuration session

Settings 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 any given time.

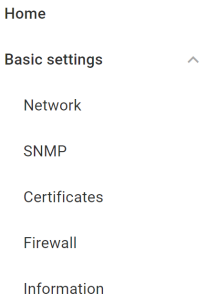
6.2.1 Login

Using the *Login* button in the upper right area of the web interface, the login prompt can be opened.

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



After successful login an expanded configuration tree is shown.



6.2.2 Logout

A configuration session can be closed by using the *Logout* button in the upper right area of the web interface.

6.3 Password settings

The password may be up to 29 characters long and protects the following configuration accesses to the W&T USB-Server.

- Web Based Management
- Up-/Download of configuration files
- Firmware-Update
- Reset Port
- Settings via WuTility

i **Password reset**

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

Basic Settings → *Password* in the navigation tree takes you to the Web page for assigning or changing the password.

To change or create a password, first click the *Change Password* button. The new password must then be entered identically in both input fields. Using the *save* button, the password is applied to the system settings and written to the persistent storage.

6.4 Network parameters

Basic settings → *Network* in the navigation tree takes you to the page with the network-side basic parameters.

i Connection loss when changing network 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.

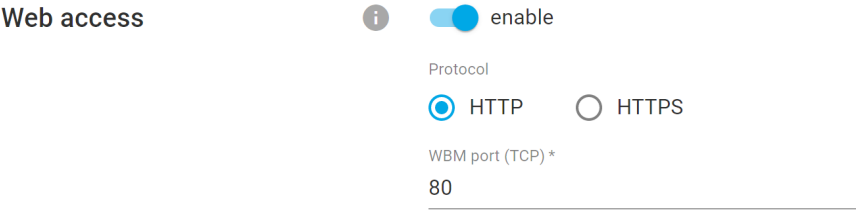
The IP settings can be used to switch between DHCP mode operation and static IP operation.

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 *
190.107.233.110
Subnet mask *
255.255.255.0
Gateway
0.0.0.0

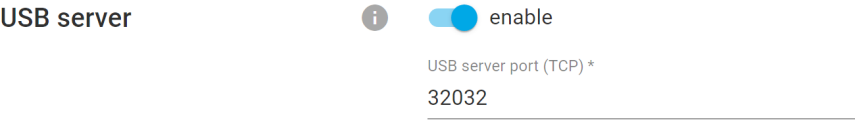
i Changing the IP-Address
When changing the network parameters, note that the device changes the IP address when the input data is saved. As a result, the WBM of the device is also only available under the newly assigned address.

i Valid network parameters
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.



Access to the WBM can be activated and deactivated via the Web access setting. In addition, web access can be configured between unencrypted HTTP and encrypted HTTPS. You can use the WBM port input field to select a free port via which the WBM can be accessed.

i **WBM Access**
Please note that after deactivating the web access further configuration of the device is only possible via a hardware reset of the USB-Server to its default settings.



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 the one used in the USB Redirector. Once the service is deactivated, plugging of connected USB devices is no longer possible.

The reset function via TCP connections can be activated or deactivated via the reset port option. In addition, the TCP port to be used can be set.

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.

WuTility management

enable

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

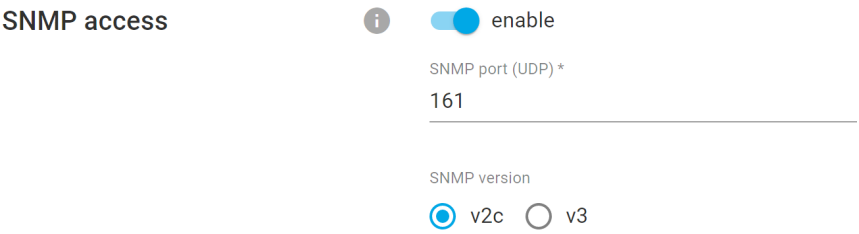
WuTility firmware update

enable

This setting can be used to configure whether firmware updates can be applied via the WuTility tool.

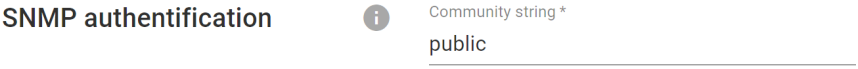
6.5 SNMP

In the menu branch *Basic settings* → *SNMP* the SNMP service of the USB server can be configured. The USB server works as an SNMP agent that provides information about the current operating status.



By activating the slide switch for the SNMP service, further settings are displayed. In addition to the UDP port, it is also possible to switch between the supported SNMP versions 2c and version 3 here. By selecting the version, the appropriate settings for the selected version are displayed.

Version 2c



To configure the operation in with SNMP version 2c, only the community string has to be entered in addition to the UDP port.

Version 3

SNMP authentification

Registration procedure

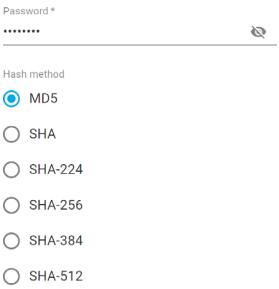
- (•) username only (noauth)
- ( ) Username and password (auth)
- ( ) Username and password encrypted (private)

Username *

snmp

The configuration of SNMP version 3 differs fundamentally according to the desired authentication mode. In *noauth* mode, only the desired user name has to be entered in the corresponding input field.

If authorization by password is desired instead, the password and the hash method to be used can also be set using *auth* mode.



If the data is also to be transmitted encrypted, the password for the encryption and the desired encryption algorithm can also be selected using the *priv* mode

6.6 Certificate

In the menu branch *Basic Settings* → *Certificate* you can adjust the certificate that the USB server uses for HTTPS communication. In the default settings the USB server uses a self-signed certificate. If an externally signed certificate is desired instead, a Certificate Signing Request (CSR) can be created via the web interface. This allows the certificate authority to sign the certificate without the secret key having to leave the device.

In addition to the Common Name, in which the IP address or the host name of the USB server is to be entered, the other fields of the certificate subject can also be freely adjusted.

After pressing the *Create* button a new key pair is generated on the USB server and the CSR is created, which can then be transferred from the USB server to the computer via the Download button.

After the CSR has been created, a self-signed certificate with the specified information can be installed. To do this, click the *Install* button under „Self signed certificate".

i **Installing a self signed certificate**
Note that the *Install* button becomes active only after a CSR has been successfully created.

Alternatively, you can upload the signed certificate and, if applicable, the associated certificate chain provided to you by your certification authority to the USB server using the *Upload* button and then install it.

i **Installing an externally signed certificate**
Note that the Upload and Install buttons for externally signed certificates become active only after the created CSR has been downloaded from the USB server's web interface.

Under the heading „Current certificate" at the top of the page you can check whether the certificate has been correctly adopted.

6.6 Device Information and WBM configuration

From *Basic settings* → *Information* you can adapt non-functional texts and descriptions (location, service contact, installer etc,) for the USB-Server.

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

6.6.1 System name

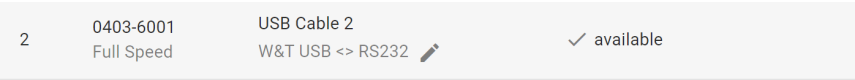
From *Basic settings* → *Information* you can change the system name of the USB Server. This is invoked and used by the following applications and services:

- 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.

6.6.2 USB Port Description

A freely modifiable annotation can be assigned to a USB port in the menu branch USB devices. This annotation is then also displayed in the USB Redirector.



This option is convenient when multiple connected USB devices do not differ in their descriptors, i.e. have the same system names and same vendor/product IDs.

The description entered here is assigned exclusively to the port number indicated in the Port column - not the connected device. This means if the USB devices are later moved, the description text does not move with the USB device but rather stays with the original port.

6.7 Firewall

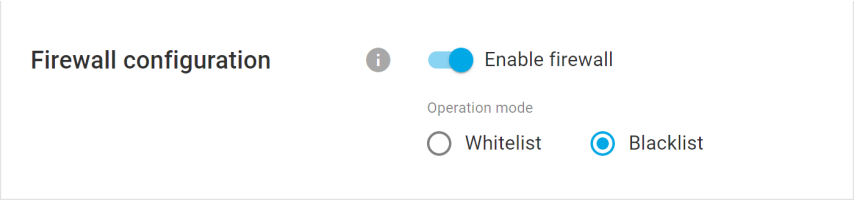
The firewall function allows to restrict the IP-based access to the USB server. It is possible to choose between a whitelist with explicit allowed IP addresses or a blacklist with explicitly blocked IP addresses.

The firewall controls all IP-based traffic. Besides access to the USB devices via the USB Redirector, all other services (ping, web-based management, firmware updates, etc.) are also affected. For example, when using the whitelist, only the explicitly named hosts can access the device's web pages or the connected USB devices.

i **Accessibility of the USB server**
When configuring the firewall, take special care to ensure that the connection to your workstation is not prevented by the new settings. An incorrectly configured firewall can only be deactivated by resetting to factory settings, except from IP addresses that can still be reached.

6.7.1 Activating the firewall

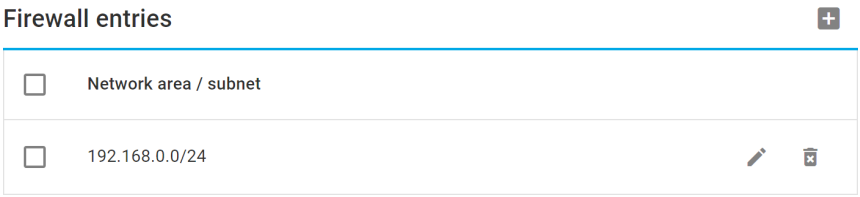
When the firewall function is activated, the blacklist or whitelist options are enabled.



6.7.2 Editing firewall entries

The lower part of the page contains the list of IP addresses or IP address ranges currently entered in the firewall. The existing entries can be edited using the *Edit* and *Delete* buttons within the list. Adding new entries is possible via the *plus* on the right side above the list.

The IP addresses are displayed in CIDR notation and also allow entire subnets to be entered in the list with a single entry.



6.7.3 Example

In the image section above shows the entry

```
192.168.0.0/24
```

The /24 suffix indicates that the IP addresses that match in the first 24 bits of the address apply to this entry. In this case, this would be all IP addresses in the form 192.168.0.xxx.

If the firewall is operated in whitelist mode this would mean that only devices within this IP range can access the USB server, i.e. access from 192.168.1.10 is **not** possible, access from 192.168.0.10 **is** possible.

Conversely, if the firewall is operated in blacklist mode, this means that accesses within this IP range to the USB server are blocked, i.e. access from 192.168.1.10 **is** possible, access from 192.168.0.10 is **not** possible.

6.8 Maintenance

The USB server offers various maintenance options via the *Maintenance* menu branch.

Restart

The USB server performs a hardware reset via the *restart* button. The configuration is kept, but the complete system is initialized from scratch.

Restore / Factory Default

This menu item can be used to reset the configuration of the USB server to the factory default. After the factory default reset, the USB server performs a restart and can be reached under the default IP 190.107.233.110.

Firmware update
As an alternative to updating the USB server via WuTility, this button can be used to upload a new firmware version via the web interface. The current firmware file for this can be found at

https://www.wut.de/53663

Configuration backup
This menu item can be used to backup the entire configuration of the USB server or to restore an old backup to the USB server.

---

i **Backup file**
Please note that the backup files are compatible only with higher or equal firmware versions than the one from which they were created.

6.9 System log

Via the System log menu branch, the USB server displays various events, such as the plugging in and unplugging of USB devices or logon actions on the WBM.

In addition, a syslog server can be configured, to which all log messages are forwarded at the time of the event.

7. Appendix

- Firmware-Update
- Reset to factory defaults
- Used ports and network security
- Technical data

7.1 Application example: Dongle device pool

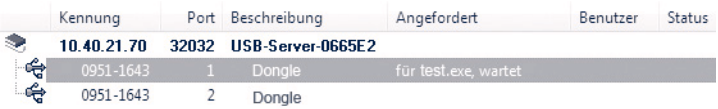
When working with multiple licensed dongles of the same type which are needed by different users in the network, you can use a USB device pool. Beginning with the start of a particular program, the USB Redirector claims the next unused dongle in the device pool.

A USB device pool is always based on a master device and one or more backup dongles associated with this master unit. When the triggering program is started, the USB Redirector begins to open the connection to one of the dongles assigned to the pool.

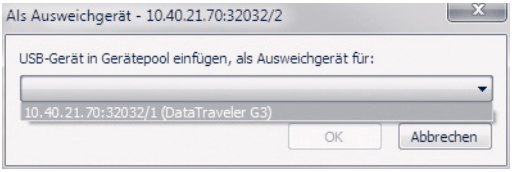
Example: Setting up a device pool with two dongles

1. First connect both dongles to the USB Server(s) in the network and refresh the inventory list for the USB Redirector. USB Servers not located in the local subnet may have to be manually added using Devices → Insert new.

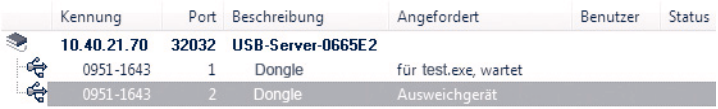
2. Select one of the dongles and click on the Advanced button. In the following dialog select the option automatic, for this application, select the program protected by the dongle and confirm with OK.



3. Now select the desired backup device by right-clicking and select the option *Add To Device Pool*.



Select the previously claimed master unit and confirm with OK.



Kennung	Port	Beschreibung	Angefordert	Benutzer	Status
10.40.21.70	**32032**	**USB-Server-0665E2**			
0951-1643	1	Dongle	für test.exe, wartet		
0951-1643	2	Dongle	Ausweichgerät		

4. Define any additional backup devices as described under 3.

7.2 Application example: USB cameras

The bandwidth required by the USB cameras depends on the selected resolution and frame rate as well as whether the transmission is compressed or uncompressed. The following table lists some typical single-frame sizes:

Resolution	approx. data usage [MBit / frame]	
	YUY2	MJPEG
1920x1080	34.4	5.7
800x600	7.7	3.3
640x480	5.0	2.0
320x240	1.3	0.5

Typical frame sizes for Microsoft LifeCam Studio, black/white grid

Ignoring any additional data load, a 100BaseT network provides nearly 80 Mbps (~10MB/s). This means that compared with the local USB port at 480 Mbps not all combinations of resolution, frame rate and compression offered by the camera will be possible.

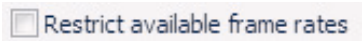
i **Showing performance data**
The actual performance data for an active connection can be viewed in the USB Redirector by right-clicking on the desired USB device and selecting the menu item Performance Data.

Resolution/frame rate/compression & network bandwidth
USB cameras provide the responsible camera driver with information about the supported operating modes and resolutions in the form of USB descriptors. These are passed on to the video applications after they are read out. Both the passing of supported modes from the device driver to the video application and the corresponding configuration dialog for the user may be incomplete.

The USB Redirector provides the possibility of bandwidth management especially for such cases in combination with relatively narrow-band connections (e.g. DSL, VPN etc.). This allows the camera mode consisting of resolution, frame rate and compression to be adjusted to the actually available bandwidth.

- 

  If this option is activated, the USB Redirector will filter out all uncompressed video modes of the video camera and only leave compressed video descriptors available to the system.

- 

  If this option is activated, the USB Redirector will filter out video settings with a high resolution and high frame rate from the video descriptors.

- 

  In this mode the USB Server temporarily stores the individual camera frames and the USB Redirector retrieves them individually. As soon as one frame is fully received the next one is requested. As a consequence of this buffering technique, the frame rate configured in the application is reduced by about a third.

i **Bundling video data**

Bundle Video Data mode can only be activated for one port on the USB Server.

- 

  This option is only available if Bundle Video Data mode is activated. Camera frames are only retrieved at the specified frame rate. Especially for narrow-band network connections, e.g. via VPN over the internet, this option can help to prevent complete utilization of the network connection.

7.4 Firmware Update

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

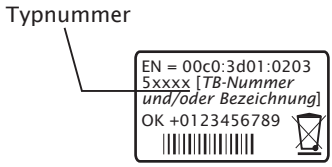
7.4.1 Where is the current firmware available?

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.

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.



7.4.2 Firmware update under Windows

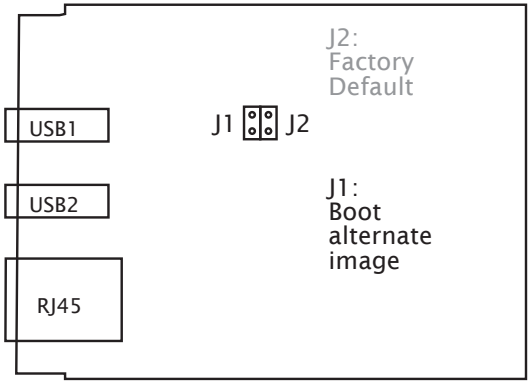
A firmware update requires that the services Enable firmware update and WuTility-Management be activated in the USB Server (see section WBM - Network services). No other preparation is needed for the USB Server.

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.

7.4.3 Interrupted updates, alternate image

If a firmware update is unsuccessfully aborted, 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. To start the new firmware for normal operation open jumper J1 and perform a reset of the USB Server.



7.5 Resetting the USB-Server

Restarting the USB Server (comparable with a power-down reset) can be done using the TCP reset port on the USB Server. The factory default setting for this is TCP/8888. Web-Based-Management can be used to deactivate this service or configure the port number.

A reset using this service has no effect on the saved configuration of the USB Server. Only connections to connected USB devices which are open at this point in time are closed.

The reset can for example be performed using the configuration tool of the USB Redirector. Right-click on the desired USB Server and then select Reset Device.

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 systen password within this time, it 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.

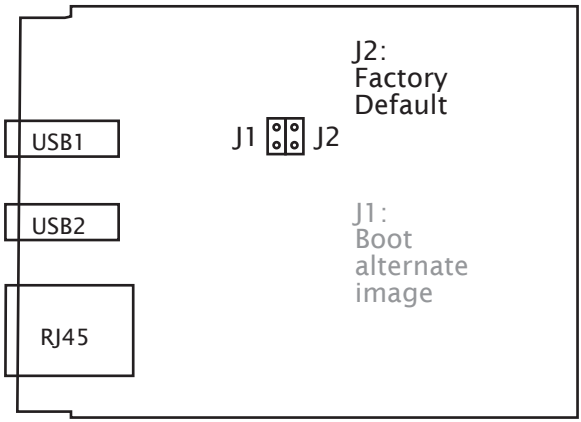
7.6 Factory Default Settings

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

7.6.1 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 system LED flashes green rapidly until the reset is completed. If the flashing sequence of the system LED changes to a slow green flashing, open jumper J2 again and perform a power-down reset. All parameters of the USB server are now back to their factory defaults.



Opening the device

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.

7.6.2 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 Maintenance menu branch.

7.7 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 number	Application	Password protected	Configurable / Optional
32032 (TCP)	USB Server Service	no	yes/yes
80 (TCP)	HTTP Server	yes	yes/yes
8888 (TCP)	Reset port	yes	yes/yes
8513 (UDP)	Inventory	no	no/yes
2682 (TCP)	FW-Update Initialization	yes	no/yes
69 (UDP)	FW-Update Data	yes	no/yes

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

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, functionaltiy 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.

Access concept of the USB Server

Network access to the USB Server can be controlled by an IP-based firewall. By default no firewall rules are configured, so that any network device can access the Server. Access restrictions are formulated in the form of a whitelist (authorized hosts) or blacklist (unauthorized hosts) and stored in the USB Server. Details can be found

in the corresponding section 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.

In some situations, 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).

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.

- **Inventory 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.

- **SNMP**
  To incorporate the USB-Servers into an SNMP-based network management system, parts of the MIB2 are accessible using SNMP. When using SNMP V3 this communication can be protected and encrypted using a password.

- **Firmware-Update**
  The firmware update is initialized via TCP port 2682 and the data is uploaded via UDP port 69. Both ports are protected by the system password. During the firmware update, the password is trasmitted in an unencrypted form. Neither port is configurable, but both can be disabled.

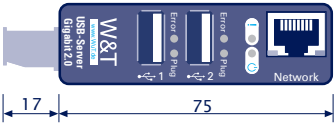
  USB-Server Reset
  (see section Resetting the USB-Server)
  TCP port 8888 permits a complete reset of the USB-Server. The port is configurable, can be disabled and is password protected.

- **USB-Server Service**
  The USB data is transmitted via TCP-Port 32032. Due to the high data throughput and need for low latency, this communication is unencrypted and not protected by a password.

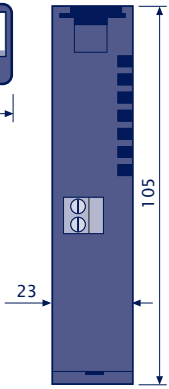
7.8 Technical data

Property	Value
Power supply	
Power-over-Ethernet	37-57VDC from PSE
External Supply, Screw Terminal	24-48VDC (+/- 10%)
Current draw	
Power-over-Ethernet	PoE Class 3 (6,49-12,95W)
Ext. Supply, no USB-Load	120mA (typ) @ 24VDC
Ext. Supply, 2x 2,5W USB-Load	420mA (typ) @ 24VDC
USB ports	2x Typ A
USB speed	480Mbit/s
Permissible ambient temperature	
Storage	-40 to +85°C
operation, non cascaded	0 to +50°C
Permissible relative humidity	0 to 95% (non condensing)
Dimensions	23 x 105 x 75 (H x D x W) [mm]
Weight	approx. 200g

Front view53663



Bottom side 53662



Measure in mm, +/-1mm

7.9 Licenses

The USB-Server uses open source components that are distributed under various licences. A full list of applicable licenses and their full text alongside information on how to aquire the source code can be downloaded directly from the USB-Server according to the respective firmware version.

The download can be started via the link „License information“ under the menu item „Properties“ on the web interface.

Wiesemann & Theis GmbH
Porschestraße 12
D-42279 Wuppertal

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

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