W&T

www.WuT.de

Manual

Startup and application

Microwall VPN

Valid for the following models:

#55211: Microwall VPN

Release 1.01 04/2020

Irrtum und Änderung vorbehalten:

Since we can make mistakes, none of our statements may be used unchecked. Please report any errors or misunderstandings you become aware of so that we can identify and correct them as quickly as possible.

Only carry out work on or with W&T products if you are described here and have read and understood the instructions completely. Unauthorized action can cause dangers. We are not liable for the consequences of arbitrary action. In case of doubt, please ask us or your dealer again!

This device contains software components that are licensed under one or more open source licenses. Copies of these licenses are included in the appendix of this document as well as the following website where the corresponding source code can also be downloaded free of charge.

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

You can also obtain the source text from us in the form of a data carrier at cost price for a period of three years after the last delivery. Please contact us for this purpose at info@wut.de.

This offer applies to every recipient of this information.

Introduction

The Microwall VPN is an industrial-grade IPv4 router with two 1000BaseT network connections, integrated whitelist-based firewall and a WireGuard VPN server. It connects a network island, e.g. with automation components, to a higher-level local network. At the same time, secure remote access to the participants of the island network can be provided via the WireGuard VPN. Suitable filter rules on TCP/IP level protect all networks from unauthorized, undesired and harmful communication.

Inhalt

1 Legal information and safety

1.1 Legal notices

Warning concept

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 results 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.

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.

Disposal

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

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

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.

1.2 Safety notices

General notices

This manual is intended for the installer of the Microwall VPN described in the manual and must be read and understood before starting work. The devices are to be installed and put in operation only by qualified personnel.

Intended use

⚠DANGER

The Microwall VPN is an industrial-grade IPv4 router with two 1000BaseT network ports, integrated whitelist-based firewall and a Wireguard VPN server. It connects a network island to a superordinate local network. At the same time, secure remote access to the participants of the island network can be provided via the WireGuard VPN. Suitable filter rules on TCP/IP level protect all networks from unauthorized, undesired and harmful communication.

Any other use or modification of the described devices is not intended.

Electrical safety

⚠WARNING

Before beginning any kind of work on the Microwall VPN you must completely disconnect it from power. Be sure that the device cannot be inadvertently turned on again!

The Microwall VPN may be used only in enclosed and dry rooms.

The device should not be subjected to high ambient temperatures or direct sunlight, and it should be kept away from heat sources. Please observe the limits with respect to maximum ambient temperature.

Ventilation openings must be clear of any obstacles. A distance of 10-15 cm between the Microwall VPN and nearby heat sources must be maintained.

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

When installing be sure that no stray wires stick out through the ventilation slit of the Microwall VPN into the housing. Ensure that no individual wires stand off from leads, that the lead is fully contained in the clamp and that the screws are tightly fastened. Fully tighten screws on unused terminals.

The power supply used for the Microwall VPN must absolutely ensure safe isolation of the low-voltage side from the supply mains according to EN62368-1 and must have “LPS“ designation.

EMV

⚠NOTE

Only shielded network cables may be used for connecting the Microwall VPN to the network.

In this case the Microwall VPN meet 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.

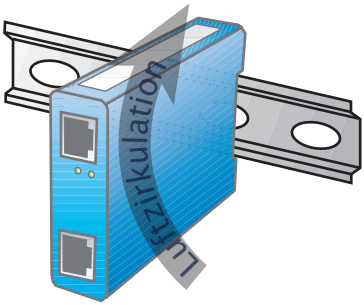
The complete Declarations of Conformity for the devices described in the manual can be found on the corresponding Internet page at the W&T homepage: http://www.wut.de.

2 Hardware, interfaces and displays

- Hardware installation
- Power supply
- Network interfaces
- Service button

2.1 Hardware installation

The Microwall VPN is mechanically designed for mounting on a standard DIN rail. In this case, as well as with alternative mounting methods, the outlined air circulation must be guaranteed.



The installation site must be adapted to the security requirements of the respective system environment. Physical access to the Microwall VPN enables a potential attacker to take the device out of operation or to replace the password via the service button.

2.2 Power supply

The power supply of the Microwall VPN is alternatively via PoE or an external power supply. Simultaneous connection of both power supplies is not permitted. The current consumption can be taken from the technical data.

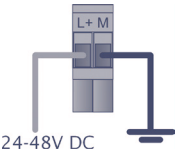
2.2.1 PoE- supply

The Microwall VPN can be supplied via the interface Network 1 (yellow) via PoE according to IEEE802.3af. It is a PoE power class 2 device (power consumption from 3.84W to 6.49W).

2.2.2 External power supply

As an alternative to the PoE supply, the Microwall VPN can be supplied externally via the pluggable screw terminal located on the underside of the housing. The DC voltage used must be within the following range and the polarity must be observed:

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



⚠WARNING

Only a floating power supply unit may be used for the external supply of the Microwall VPN 55211. Its reference ground for the output voltage must not have a direct connection to the protective conductor.

The power supply unit used to supply the Microwall VPN must guarantee a safe separation of the low voltage side from the supply network according to EN62368-1 and must have „LPS“ characteristics.

2.3 Network Interfaces

The Microwall VPN has two network interfaces: Network 1 (yellow) and Network 2 (green).

Network 1 (yellow) is used for connection to the higher-level network in which the island network is to be integrated at the *Network 2* (green) connection.

Commissioning with the factory settings and a possible supply via PoE is only possible via *Network 1* (yellow).

2.3.1 Gigabit Ethernet Features

Both Gigabit Ethernet connections have the following features:

RJ45 jack, shielded
Connections to the network infrastructure are via shielded patch cables with a maximum length of 100m

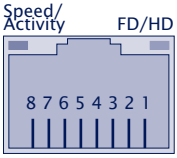
Autocrossing / Auto MDI-X
The transmit/receive lines of the connected device are automatically detected. Both 1:1 wired and crossed patch cables can be used.

Galvanic isolation
There is an electrical isolation of at least 500Vrms from the supply voltage

Auto-Negotiation
The transmission speed and duplex method are automatically negotiated with the connected device. To avoid problems such as duplex mismatch, we recommend that the connected devices are also operated in auto-negotiation mode.

2.3.2 Link state

The link status is indicated by LEDs integrated in the RJ45 sockets.



Speed/Activity (green/orange)
Green = 1000MBit/s Link
Green flashing = 1000MBit/s Link und Datenverkehr

Orange = 100MBit/s Link
Orange blinken = 100MBit/s Link and data traffic

FD/HD (yellow)
ON = Full duplex
OFF = Half duplex

2.4 System- and Error LED

2.4.1 System LED ⏻ (green)

ON: Signals normal operational readiness.

Flashing: The Microwall VPN performs a reboot or receives a new firmware.

2.4.2 Service LED ⓘ (red)

The service LED is used to signal the *emergency access* and *factory default reset* functions that can be controlled via the service button.

Slow flashing: The service button was pressed between 3.5s and 10s. The emergency access of the Microwall VPN is activated.

Further information on emergency access can be found in the chapter on *emergency access.*

The emergency access opens a non-password-protected HTTPS access (TCP port 446) with the possibility to overwrite the current password. Therefore, only start the emergency access in an appropriately secure environment (e.g. direct connection to a configuration PC).

Fast flashing: The service button was pressed for longer than 10s and the Microwall VPN is preparing a reset to the factory settings. If the service button is still pressed, a reset to the factory settings is performed after a total of 20s.

2.5 Service button

The service button is accessible recessed on the front side of the Microwall VPN to avoid operating errors. It is operated with a suitable, pointed object (e.g. paper clip).

The following actions are triggered via the service button:

Reset/Restart
Pressing the button briefly between 0.2 and 3.5s triggers a restart of the Microwall VPN.

Starting the emergency access
After pressing the button for more than 3.5s, the error LED starts flashing slowly. If the button is released during this phase and before 10s have elapsed, the emergency access of the Microwall VPN is activated on both network connections via TCP port 446. Pressing the button again briefly performs a reset and ends the emergency access.

Further information on emergency access can be found in the chapter *emergency access*.

The emergency access opens a non-password-protected HTTPS access (TCP port 446) with the possibility to overwrite the current password. Therefore, only start the emergency access in an appropriately secure environment (e.g. direct connection to a configuration PC).

Reset to factory settings
If the service button is pressed for more than 10s, the service LED starts flashing rapidly and signals preparation for a factory default reset. If the button is held down further, the Microwall is reset to the factory default after 20s. Releasing the service button while the service LED is flashing rapidly (time window 10-20s) will cause the factory default reset to be

aborted. The Microwall continues with the standard operation of the current configuration.

A reset to the factory setting causes all settings (filter rules, IP parameters, log files, etc.) to be lost. Recommissioning must be carried out as described in the chapter Start-up.

3 Start-up

The commissioning of the can only be done via the interface *Network 1* (yellow). In the first step, the IP address required for initial access is assigned. Subsequent browser access leads to the initial web page for configuration of the basic parameters required for operation, including the system password.

- Setting the IP address with the WuTility management tool
- Changing the IP parameters via Web-Based Management
- Initial access via browser

3.1 Initial assignment of IP parameters with WuTility

From version 4.52, the Windows tool *WuTility* supports the inventory and management of the basic network parameters of the Microwall VPN

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

WuTility versions >= 4.52 must be used.

When the interface Network 1 *is connected to the network, the initial web page for assigning the system password can be reached via the default IP or the IP address assigned via WuTility. Make sure that no unauthorized access to the Microwall VPN occurs until the password is assigned on the initial web page (e.g. by commissioning with a direct connection to the respective PC).*

To assign the IP address, the PC and the Interface *Network 1* of the Microwall VPN must be located in the same physical network.

Installing WuTility
The download link for the Windows installation package of the latest version of *WuTility* can be found on our website

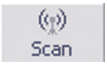
https://www.wut.de/wutility

After the installation the start takes place via

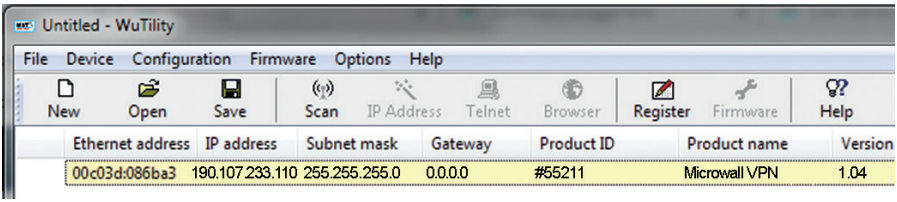
Start → Programs → Wutility Version 4 → WuTility

Start of the assignment dialog
Make sure that the Interface *Network 1* of the Microwall VPN and the computer used are connected to the same physical network. When starting *WuTility* automatically scans the local network for connected W&T network devices and creates an inventory list. This search process can be repeated as often as

required by pressing the Scan button:

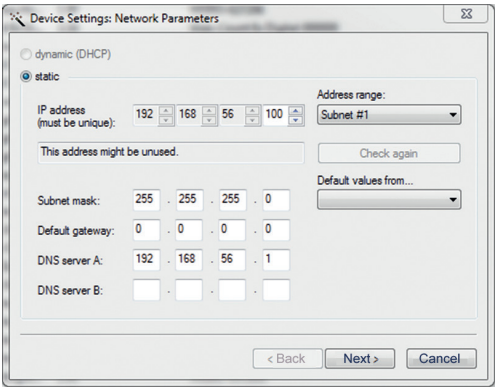


Within the inventory list, the desired Microwall VPN can be identified via its MAC address. The default IP address is 190.107.233.110.



Select the desired Microwall VPN and then press the I*P address* button:

Enter the desired values for IP address, subnet mask, gateway and DNS server.



When you click *Next*, the network parameters are saved by the Microwall VPN.

The IP assignment with WuTility can be repeated until the Microwall VPN has received a system password via the initial

web page. Afterwards, the IP parameters can only be changed using standard web-based management.

The additional parameters required for initial commissioning are set via an initial web page using a browser. For more information, refer to the chapter *Initial Web Page*.

3.2 Start-up via the default IP address

In the delivery state and after a reset to the factory settings, the default IP address of the interface *Network 1* is 190.107.233.110.

When the interface Network 1 *is connected to the network, the initial web page for assigning the system password can be reached via the default IP or the IP address assigned by WuTility. Make sure that no unauthorized access to the Microwall VPN occurs until the password is assigned on the initial web page (e.g. by commissioning with a direct connection to the respective PC).*

The commissioning of several Microwalls via their default IP can only take place one after the other. Only after one Microwall VPN has received a new IP address may the next Microwall VPN be connected to the network.

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

- The network connection of the computer used must have an IP address in the range 190.107.233.0/24. Changing the IP address of the computer requires administrator rights. Clarify IP changes in advance with the responsible network administrator.

- The computer in use temporarily receives a fixed route which redirects the IP address 190.107.233.110 to the local network. Setting up such a route requires administrator rights. The command for creating a fixed route under Windows is:

```
route ADD 190.107.233.110 MASK 255.255.255.255 [IP-Adresse PC]
```

All other parameters required for initial commissioning are then assigned via the initial web page using a browser. For more information, refer to the chapter *Initial Web Page.*

3.2 Initial web page

After the IP assignment, only the initial web page is available during the initial commissioning. Here, the password of the Microwall required for all further configuration accesses must be assigned. At the same time, the IP basic parameters of both network interfaces and the operating mode can be determined.

Saving the initial web page does not involve any communication permissions. These must then be formulated in the form of explicit whitelist rules.

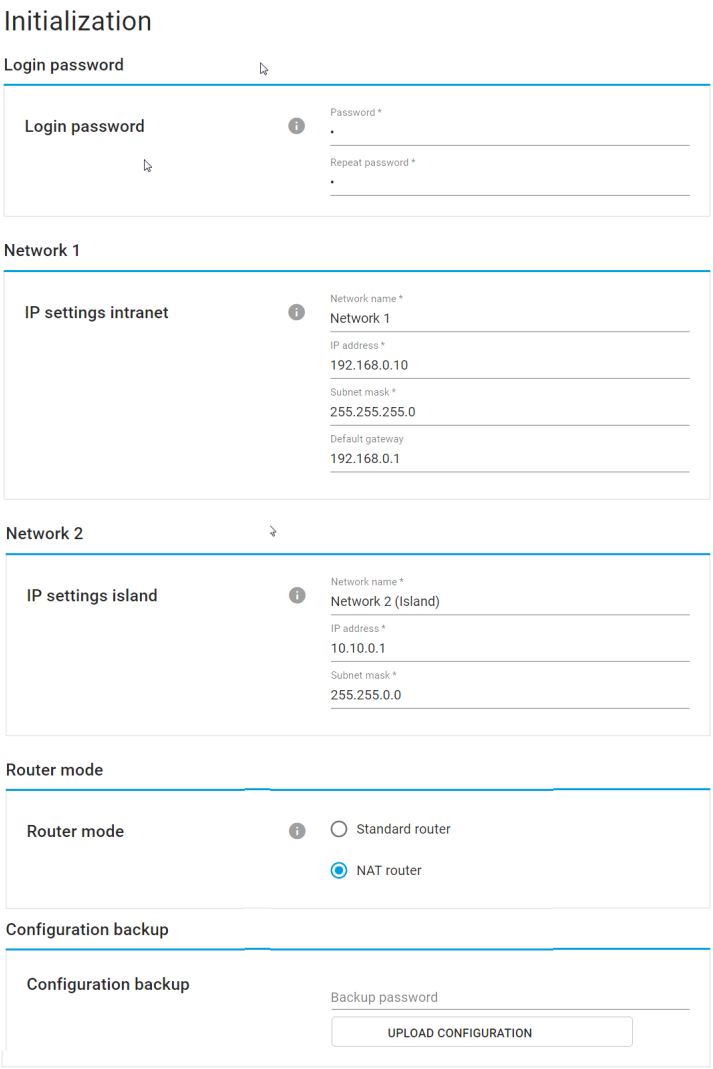
When the interface Network 1 *is connected to the network, the initial web page for assigning the system password can be reached via the default IP or the IP address assigned by WuTility. Make sure that no unauthorized access to the Microwall VPN occurs until the password is assigned on the initial web page (e.g. by commissioning with a direct connection to the respective PC).*

If the IP address was assigned using the *WuTility* tool, select the desired Microwall VPN and click on the Browser button:

If access is to take place via the default IP address of the Microwall VPN, start a browser on the PC prepared from an IP viewpoint. Enter the following URL in the address line: *https://190.107.233.110*

The Microwall is equipped ex works with a self-signed certificate. Corresponding warnings of the browser must be ignored and/or acknowledged when the initial web page is called. After commissioning, the default certificate can be replaced by an individual certificate.

All settings of the initial web page can be changed later via the standard web-based management.



Login password (mandatory)

Assign the password for all configuration/control accesses of the Microwall VPN. We recommend passwords with a minimum length of 15 characters, consisting of upper and lower case letters, numbers and special characters. The maximum length of the password is 51 characters. Operation without a password is not possible.

There is no default or master password. A lost password can only be reset to the factory settings via the emergency access that can be activated by means of the service button or a reset.

Network 1 (yellow)
Assign the IP parameters for the connection *Network 1* (yellow).

The specification of DNS servers is only necessary if the time servers are configured as host names for the NTP client of the Microwall VPN.

Network 2 (green)
Assign the IP parameters for the connection *Network 2* (green). The Net-IDs of *Network 1* and *Network 2* must be different.

If there are additional routers in *Network 2* in remote networks, these can be configured later in the network settings of the Web-based management using static routes.

Operation mode (mandatory)
Select the desired operating mode of the Microwall VPN. For more information, refer to the chapter Operating Modes and Rule Configuration.

After correct entry of all parameters, the Save button is activated and the entries can be saved. You are automatically redirected to the start page of the Microwall VPN.

Configuration backup
Allows you to upload a configuration backup previously secured by another Microwall VPN. If the backup file is secured with a password, this must be entered in the Backup Password field before the Upload button is pressed. After the file has been successfully checked, its content is accepted and the Microwall VPN operates with the new parameters after an automatic restart.

Backup files also contain the new IP address of the Microwall VPN. To avoid an IP conflict, make sure that the original or a previously programmed Microwall VPN is no longer connected to the network before uploading.

For details on configuration backups, see the chapter *Up-/Downloading Configuration Backups*

4 Web based management

The configuration of the Microwall VPN is only possible encrypted via HTTPS. The WBM (Web based management) works session-oriented. Changes made on the respective pages are immediately saved and validated by pressing the *Save* button.

- Navigation within WBM

4.1 Start and navigation concept of the WBM

To access the WBM of the Microwall VPN, you need an up-to-date Internet browser. Session-Cookies, Javascript and Web-sockets must be supported or activated.

The configuration is only possible encrypted via HTTPS. The standard port 443 is preconfigured ex works.

Start your browser and enter the IP address of the Microwall VPN and, if necessary, the port number to be used.

https://[IP address]:[Port no.]

4.1.1 Navigation concept of the Microwall VPN

The WBM of the Microwall VPN works session-oriented via a password protected login. Operation without password is not possible.

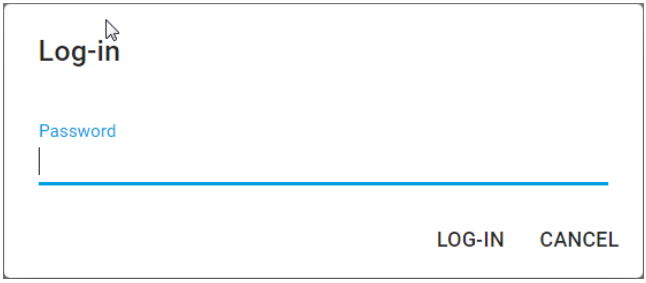
After login, any changes made are immediately applied by clicking the *Save* button on the respective page. If a restart of the Microwall is required to accept the parameters, a corresponding message is displayed after pressing Save.

To end a configuration session, click on the *Logout* button.

4.2 Login/Logout

The start page of the Microwall only offers the possibility to enter the password for login and to switch the interface language via the flag symbol.

4.2.1 Login



Enter the password and press the *Log in* button. After successful login the extended navigation tree with all configuration options is available.

To protect against brute force attacks, password entry is protected with an escalating timeout. After each incorrect password entry, the password can only be re-entered after a timeout that doubles with each attempt.

4.2.2 Logout

To end a configuration session press the *Logout* button.

4.3 Help and description texts

If the individual configuration items are not self-explanatory, the assigned info symbols contain the necessary descriptions, explanations and notes.

For detailed information on the operating modes, release rules and VPN setup, refer to the chapter *Operating Modes and Rule Configuration* in this manual.

5 Operating modes and rule configuration

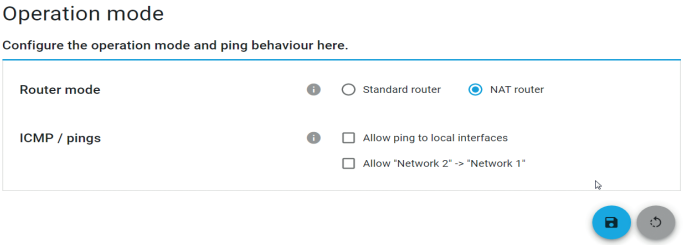
- Mode NAT router
- Mode Standard router
- Rule configuration and labels
- IP inventories

5.1 Mode NAT router

In NAT router mode, the Microwall connects the island network to the Network 2 port (green) via a fixed IP address of the higher-level network to the Network 1 port (yellow). The operating mode is comparable to many standard DSL routers, which connect the home network to the Internet using only one public IP address.

The IP addresses of the island hosts are replaced in the superordinate network by the local IP address of the Microwall VPN and are therefore not visible in the intranet at any time. The island IP range can be selected completely freely in NAT mode. Even several islands with identical IP ranges can be connected to the company intranet simultaneously in this way. An intervention in its routing concept is not necessary.

Activate the *NAT router* operating mode via the menu tree under *Firewall settings -> Operating mode* and define the handling of ICMP echo requests/replies (ping).



The Save button activates the *NAT Router* mode and the corresponding rule set is loaded.

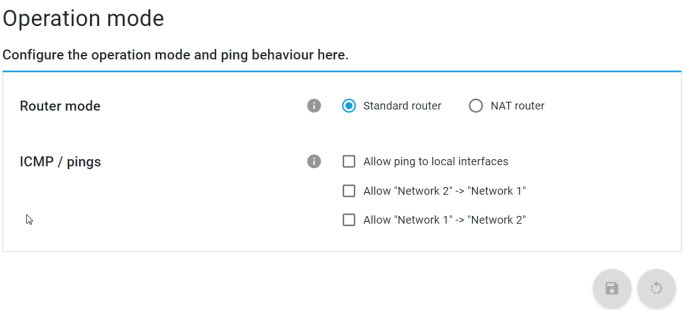
5.2 Mode Standard router

In standard router mode, the Microwall VPN disconnects the island network at the *Network 2* port (green) from the corporate intranet at the *Network 1* port (yellow). The island network becomes an official subnet of the intranet-side infrastructure.

On the intranet side, the path to the island network must be made known to the participating hosts, usually as a static route.

If the island network is a marginal network without connection to further networks, the local IP address of the Mircowall VPN is configured as default gateway on the island hosts. If further routers to other networks exist in the island network, then these paths must be made known to all island hosts as a static route.

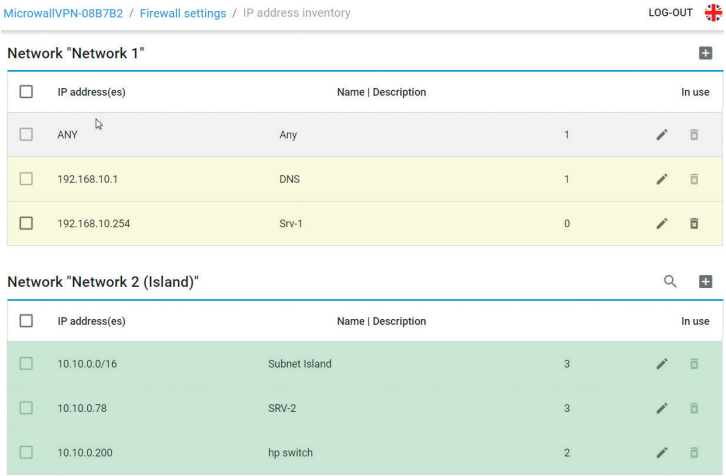
Activate the *Standard router* operating mode via the menu tree under *Firewall settings -> Operating mode* and define the handling of ICMP echo requests/replies (ping).



The Save button activates the *Standard Router* mode and the corresponding rule set is loaded.

5.3 IP inventories

In the menu branch *Firewall Settings -> IP Address Inventory*, the Microwall VPN provides a separate address inventory for each network. The configuration of the destination/source address(es) when creating firewall rules is always done from these address inventories.



Inventory entries can consist of individual IP addresses, as well as areas or lists. The following entries are permitted:

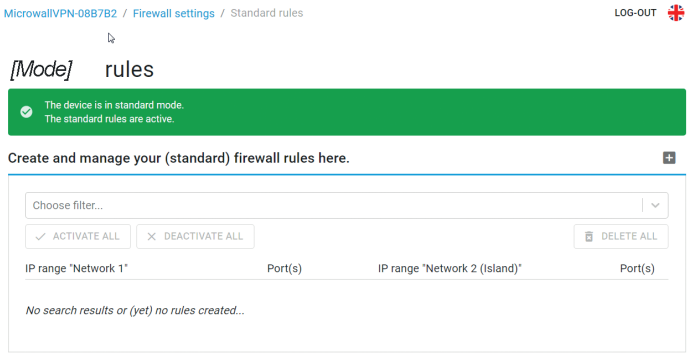
- *any*
  Keyword for any IP address
- *single IP address*
  IP address in dot notation (e.g. 10.20.0.4)
- *Comma-separated IP address list*
  List of IP addresses in dot notation (e.g. 10.10.10.1, 20.20.20.2)
- *IP range*
  Continuous IP range in the form „from-to“ (e.g. 10.10.10.1 - 10.10.10.20)
- *IP- range CIDR notation*
  CIDR listed IP range (e.g. 10.10.0.0/16)

5.3.1 Scan of Network 2

Using the magnifying glass in the area of *Network 2*, it is possible to search the island network for participants. Newly found stations found during a scan can then be automatically added to the inventory list of *Network 2*.

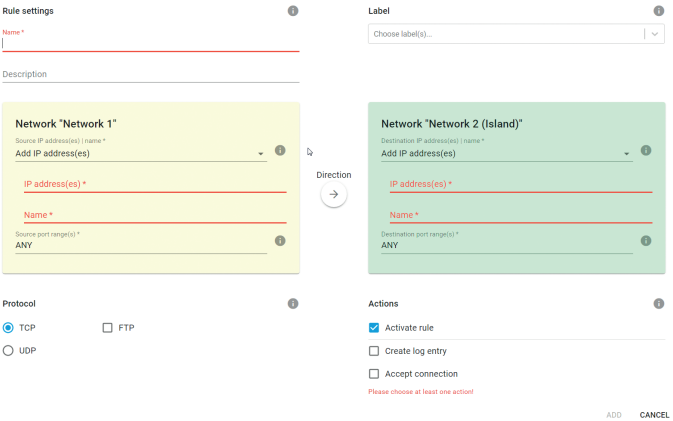
5.4 Creating firewall rules

Creating firewall rules for the current mode is done on the page *Firewall settings -> Firewall rules*. The overview contains information about the existing rules with the possibility to activate and deactivate them using the respective slide switch.



The *Plus* button at the upper right edge of the table opens the dialog for creating new rules.

Rule examples for many standard applications can be found on our website at https://www.wut.de/rule-examples.



Name

Freely assignable name of the rule.

Description

Optional additional description of the rule.

Label

For a more clearly arranged display or display filtering in the rule overview, one or more labels can be assigned to the rule. The labels Normal mode and Service are created ex works. The Label Inventory page can be used to create additional labels.

Direction

Clicking on the direction arrow sets the direction for the rule from the point of view of establishing a TCP connection. For UDP the direction is determined by the initial UDP datagram.

Network 1 (yellow) & Network 2 (green)

Configuration of the destination/source IP addresses and destination/source port numbers used for the rule. Which network the source or destination is on is determined dynamically by the selected direction of the rule. Depending on the current operating mode, either only individual addresses and/or ports can be configured or entire ranges

and lists can be configured. Details can be found in the respective help texts that can be called up via the *Info* button.

The *destination IP address(es) | source IP addresses* can either be selected from the inventory lists via the select box or specified directly numerically. If specified numerically, the new host or address range is automatically transferred to the respective IP inventory for *Network1* or *Network2* with the name specified under *Name*.

Permissible entries and formats of addresses and address ranges:

- *any*
  Keyword for any IP address
- *single IP address*
  IP address in dot notation (e.g. 10.20.0.4)
- *Comma-separated IP address list*
  List of IP addresses in dot notation (e.g. 10.10.10.1, 20.20.20.2)
- *IP range*
  Continuous IP range in the form „from-to“ (e.g. 10.10.10.1 - 10.10.10.20)
- *IP- range CIDR notation*
  CIDR listed IP range (e.g. 10.10.0.0/16)

Different input forms and concatenation of IP ranges within one input field are not possible. This means that „10.20.0.4, 10.20.0.10-10.20.0.20“ or „10.20.0.0/16, 10.10.0.0/16“ are invalid entries.

Permissible entries and formats of port numbers and port number ranges:

- *any*
  Keyword for any port number
- *Single port number*
  e.g. 8000
- *Comma-separated port number list*
  e.g. 80,443,8000
- *Port number range*
  e.g. 100-1000

Different input forms cannot be combined. This means, for example, „8000, 10-1000“ is an invalid inpu

Protocol

Specifies whether the rule applies to TCP or UDP.

The TCP option *FTP* must be activated when the rule for FTP connections is formulated. Parallel TCP connections negotiated during the protocol process are automatically allowed and blocked.

UDP is a connectionless protocol which, however, often works on a request-reply principle (e.g. DNS). In these cases the option *Allow response in reverse direction* must be activated. The Microwall will automatically accept an incoming reply datagram within a timeout.

Actions

Activate rule activates the rule immediately after pressing the *Save* button. If the option is not set, the rule is created but not applied when you click *Save*. Data traffic according to the rule is not possible. The rule can also be activated later in the rule overview.

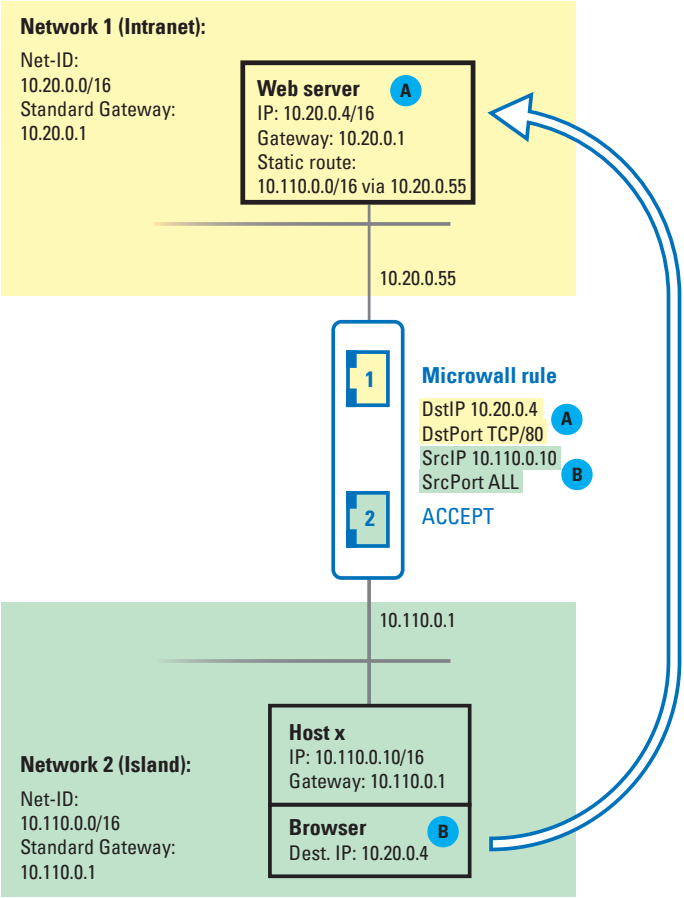
Create log entry creates an entry in the log file of the Microwall for each connection establishment according to the rule.

Accept connection allows the data traffic defined by the rule.

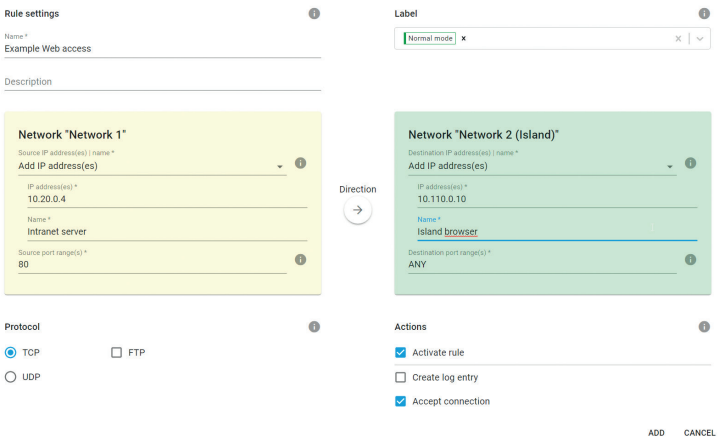
5.5 Examples Firewall rules

5.5.1 Mode Standard router, Network 2 to Network 1

Island host B 10.110.0.10/16 at the *Network 2* port is to access the Intranet Web Server A 10.20.0.4/16, TCP/80 at the *Network 1* port via browser. The respective local IP addresses of the Microwall VPN are 10.110.0.1 and 10.20.0.55. For view filtering in the rule overview, the rule is marked with the label *Normal mode*.

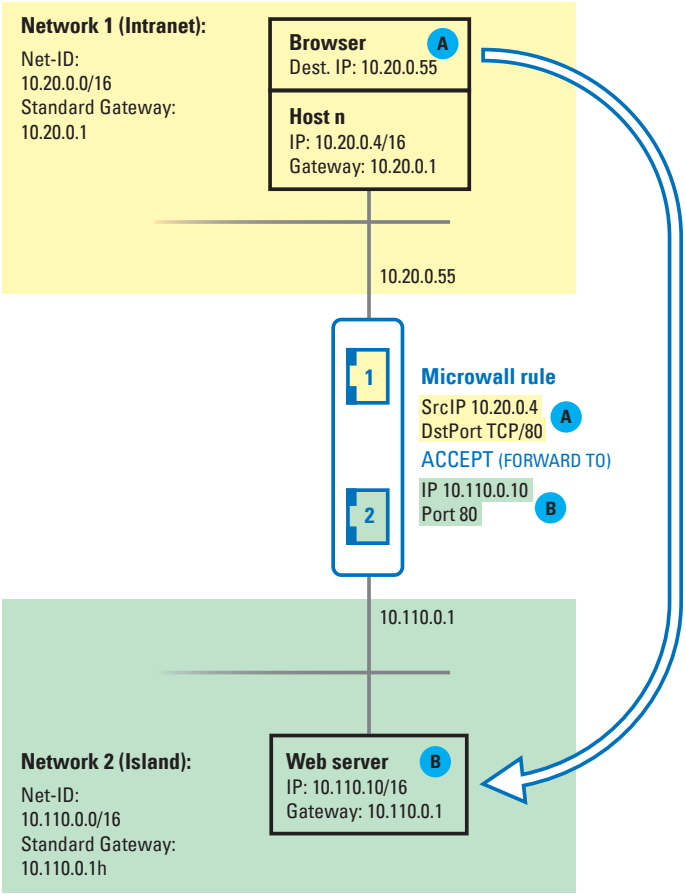


The rule dialog to be filled out for this example:

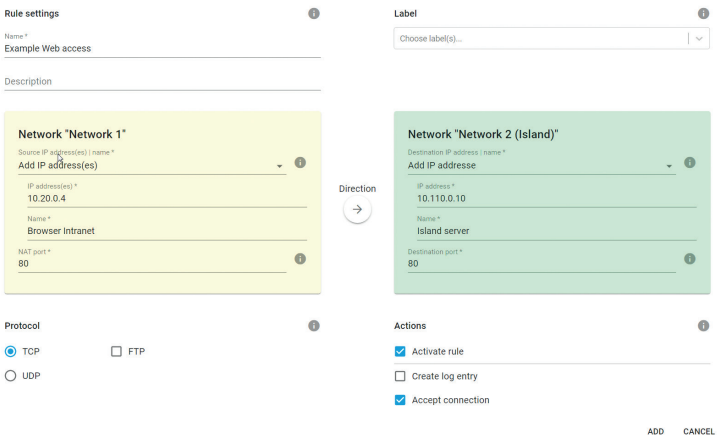


Mode NAT-Router, Network 1 to Network 2

Intranet host A 10.20.0.4/16 should access the island web server B 10.110.0.10/16, TCP/80 via browser. The Microwall VPN itself is integrated into the networks with the IPs 10.110.0.1 and 10.20.0.55. The intranet IP of the Microwall VPN is used as the destination address in the browser, where it is usually replaced by the island IP 10.110.0.10.



The rule dialog to be filled out for this example:



Further control examples for many standard applications can be found on our website at https://www.wut.de/rule-examples.

6 Wireguard VPN

- Remote access/maintenance Island host
- Configuration of VPN access
- Configuration of VPN clients
- Creating VPN rules

6.1 Introduction & System Integration

WireGuard is a VPN architecture whose focus is on high security requirements through modern cryptography as well as simple configuration at high speed.

Details as well as current information on concept, function and development status of this open source project can be found under the following link. There you will also find download options for WireGuard VPN clients of many common operating systems.

https://www.wireguard.com

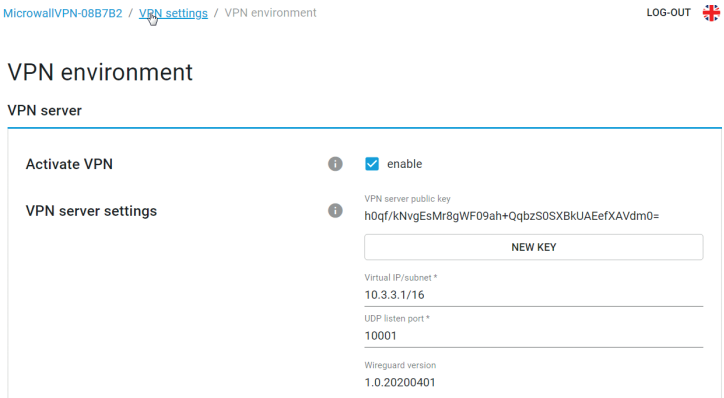
The Microwall provides a WIreGuard server on the LAN side, which enables registered VPN clients to securely access participants in the island network. All accesses must be explicitly permitted via a whitelist-based firewall.

WireGuard functionality
WireGuard tunnels IP packets through an encrypted UDP channel between the VPN client and VPN server in a virtual IP subnet. Encryption and mutual authentication are carried out asymmetrically using key pairs with public and private parts (public key/private key). The public keys of a VPN server and client must be mutually known.

6.2 Configuring the VPN environment

On the page *VPN settings -> VPN environment* the basic settings of the *VPN server* and the activation of the VPN clients are made.

6.2.1 Section VPN Server



Activate VPN
The check box activates the VPN server with the set parameters on *Network 1* (yellow) of the Microwall VPN.

VPN server settings -> Public Key/New Key
The displayed public key of the VPN server must be known to every VPN client and can be copied here from the text field, e.g. into a file.

The button *New Key* generates a new key pair (private key and public key) for the VPN server.

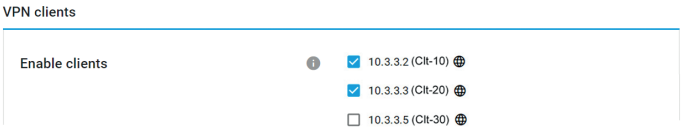
Within an existing VPN environment, the public key of a newly generated key pair must be rolled out to all VPN clients. Communication via the old key pair is no longer possible.

VPN server settings -> Virtual IP/subnet
The virtual IP address and subnet mask of the VPN server in CIDR notation defines the NetID of the entire VPN. The IP addresses of all VPN clients must be located in the same subnet. The IP range of the VPN must not collide with the address ranges of *Network1* and *Network 2*. The conflict with the IP range(s) on the VPN client side must also be prevented.

VPN server settings -> UDP listen port
Defines the UDP list port on which the VPN server accepts connections from VPN clients. The UDP port configured here must be used as the destination port in all VPN clients.

If VPN clients connect via a router or a perimeter firewall upstream of the server, this port number with the IP address of Network 2 must be enabled via a firewall or NAT rule.

6.2.2 Section VPN clients

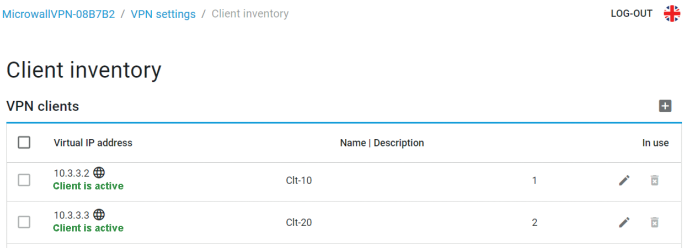


This section contains all VPN Clients created in the VPN Client inventory. The checkbox activates the respective client and allows the connection to the VPN server. For connections to participants in the island network, corresponding approvals / rules are additionally required on the *VPN Rules* page.

The globe behind a client entry indicates that the client is allowed to access the configuration pages of the Microwall VPN.

6.3 VPN client inventory

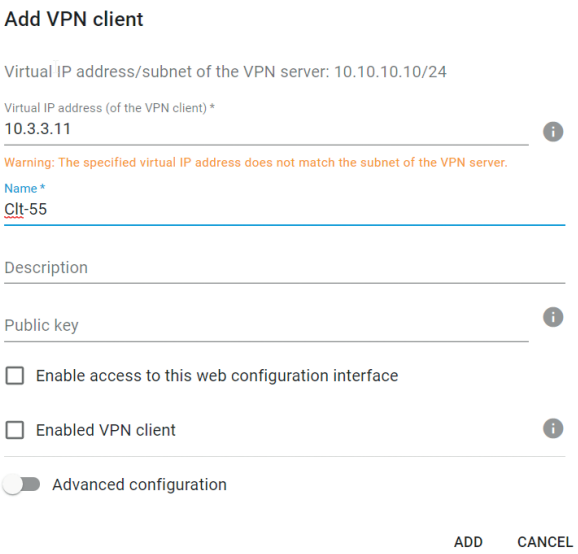
The page allows the creation, deletion and administration of VPN clients.



The VPN Client Inventory page is only used to manage the VPN clients. Activation for actual VPN connections is done on the page VPN Environment.

6.3.1 New VPN clients - Standard configuration

The button ⊞ at the upper right edge of the table starts the dialog for creating new VPN clients.



The standard configuration assumes that the VPN configuration of the client is created manually and that a key pair has already been generated there.

Virtual IP address of the VPN client
The virtual IP address entered here must be in the same subnet of the VPN server. It must not collide with the address of other VPN clients.

Name & Description
Freely selectable name(s) (mandatory) and description of the VPN client.

Public key
Public key of the key pair generated on the VPN client.

Option: Enable access to this web configuration interface
Activating this option allows the VPN client to access the configuration pages of the Microwall VPN.

Option: Enable VPN client
If this option is activated, the created VPN client is immediately activated by clicking the *Add* button. For access to participants of the island network, corresponding rules must be created under VPN rules.

6.3.2 New VPN clients - Advanced configuration

Enabling the *Advanced configuration* option allows you to create a complete configuration file for the new VPN client. WireGuard clients for Windows, Android and IOS allow the import of such configurations as a file or via QR code.

In this case, the key pair for the new VPN client is generated by the Microwall VPN and the sensitive private key is part of the configuration file. This method may therefore only be used if the file can be transferred to the client in a secure way.

Private key and Button Generate *Keys*

The *Generate Keys* button generates a key pair for use in the VPN client. The public key required for the subsequent authentication of the client is automatically stored by the Microwall VPN. The associated private key is only available until the configuration file is generated and is deleted when the dialog is closed.

Endpoint (VPN server)

The address information required from the perspective of the VPN client for the connection to the VPN server in the following format:

[URL|IP address]:[UDP listen port]

The default is the IP address of *Network 1* and the *UDP list port* configured in the *VPN environment*.

Allowed IPs

A comma-separated list of IP addresses in CIDR notation from which incoming traffic is allowed for this peer and to which outgoing traffic is forwarded for this peer.

The default is the virtual IP range of the VPN and the IP range of the island network to Network 2. Changes and extensions are only necessary in exceptional cases, e.g. if other networks are accessible via routers located in the island network.

Keep alive

Specifies the interval in seconds at which the VPN client generates Wireguard-Keep-Alive packets to keep the UDP tunnel open in any routers located in the infrastructure.

6.4 VPN rules

The participants and services in the island network with which an active VPN client may communicate must be explicitly permitted by corresponding VPN rules. Such firewall rules for the VPN are created on the page VPN settings -> VPN rules. In addition to an overview of the existing rules, new rules can be created and defined using the button ➕.

Name

Freely selectable name of the rule.

Description

Optional freely selectable description of the rule.

Label

For a clearer display or display filtering in the rule overview, one or more labels can be assigned to the rule. The labels Normal mode and Service are created ex works. The Label Inventory page can be used to create additional labels.

Direction

Clicking on the direction arrow sets the direction for the rule from the point of view of the tunneled connection. For TCP, the direction is determined by the connection setup. For UDP it is determined by the initial UDP datagram.

VPN client Network 1 (yellow) & Network 2 (green)

Configuration of the communication connections permitted within the VPN tunnel between the VPN client and island participants. In which network the source or destination is located is determined dynamically by the selected direction of the rule.

When selecting the VPN client in *Network 1* (yellow), only a VPN client previously created in the corresponding inventory can be selected. Its communication partner in the island network at *Network 2* (green) can either be selected from the inventory lists via the select box or specified directly numerically. If you enter a numerical value, the new

host or address range is automatically transferred to the IP inventory for *Network 2* with the name entered under *Name*.

Permissible entries and formats of addresses and address ranges:

- *any*
  Keyword for any IP address
- *single IPa address*
  IP address in dot notation (e.g. 10.20.0.4)
- *Comma-separated IP address list*
  List of IP addresses in dot notation (e.g. 10.10.10.1, 20.20.20.2)
- *IP range*
  Continuous IP range in the form „from-to“ (e.g. 10.10.10.1 - 10.10.10.20)
- *IP range CIDR notation*
  CIDR listed IP range (e.g. 10.10.0.0/16)

Different input forms and concatenation of IP ranges within one input field are not possible. This means that „10.20.0.4, 10.20.0.10-10.20.0.20“ or „10.20.0.0/16, 10.10.0.0/16“ are invalid entries.

Permissible entries and formats of port numbers and port number ranges:

- *any*
  Keyword for any port number
- *Single port number*
  e.g. 8000
- *Comma-separated port number list*
  e.g. 80,443,8000
- *Port number range*
  e.g. 100-1000

Different input forms cannot be combined. This means, for example, „8000, 10-1000“ is an invalid input.

Protocol

Specifies whether the rule applies to TCP or UDP.

The TCP option *FTP* must be activated when the rule for FTP connections is formulated. Parallel TCP connections negotiated during an FTP session are automatically allowed and blocked.

UDP is a connectionless protocol which, however, often works on a request-reply principle (e.g. DNS). In these cases the option *Allow response in reverse direction* must be activated. The Microwall will automatically accept an incoming reply datagram within a timeout.

Actions

Activate rule activates the rule immediately after pressing the *Save* button. If the option is not set, the rule is created but not applied when you click Save. Data traffic according to the rule is not possible. The rule can be activated later in the rule overview.

Create log entry creates an entry in the log file of the Microwall VPN for each connection establishment according to the rule.

Accept connection allows the data traffic defined by the rule.

6.5 Step by step: VPN access for a mobile device

There is a machine in the island network whose internal web interface is to be accessed via the Internet from an Android mobile device.

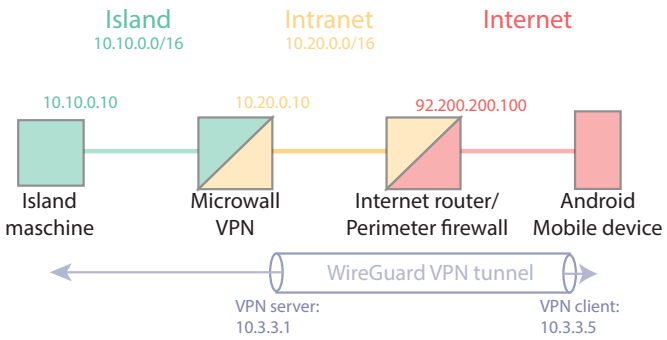
The example assumes that the Microwall VPN is already set up as a NAT router between the intranet at *Network1* (yellow) and the network island at *Network 2* (green).

1. Preparations

Android WireGuard APP - This must be installed on the Android mobile device. To do this, enter „Wireguard“ in the Playstore search.

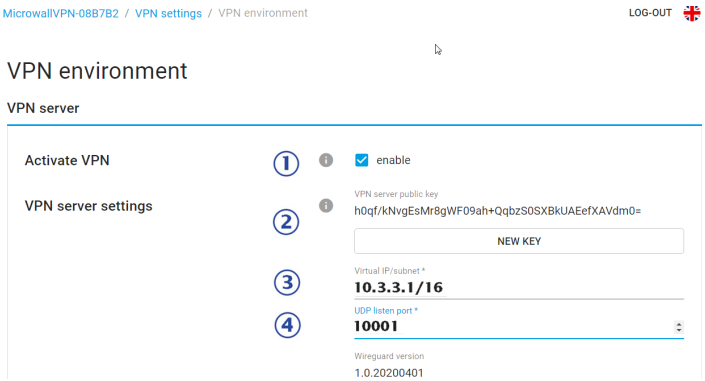
Internet router/perimeter firewall - A NAT rule is required in the perimeter firewall (possibly a DSL router) responsible for connecting the intranet to the Internet or other higher-level network. This must forward incoming UDP packets from the Internet side with the destination port 10001 to the intranet-side IP address of the Microwall VPN.

Dynamic IP addresses - If the Internet connection of the intranet only has dynamic IP addresses of the provider on the WAN side, the service of a DynDNS provider must be used. In this case, the IP address must be replaced by the corresponding host name as the end point in the VPN client configuration.



2. Setting up the VPN server environment

Switch to the page *VPN settings -> VPN environment*:



1 Activate the VPN server

2 Create a key pair for the VPN server. The public part of the key (public key) is displayed.

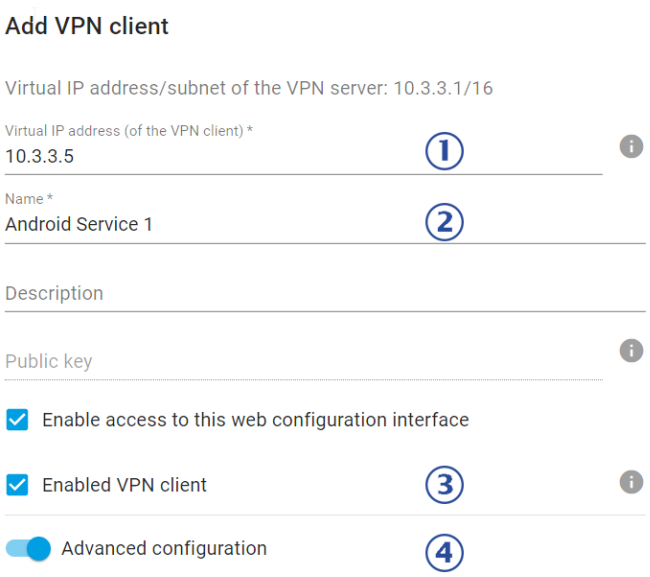
3 10.3.3.1/24
Defines the IP address of the VPN server and Net-ID for the virtual VPN network The range is largely freely selectable, but must not collide with any of the other ranges involved.

4 10001
The UDP list port on which the VPN server accepts incoming client connections.

saves and activates the changes.

3. Creating the VPN Client in the inventory

Switch to the page *VPN Settings -> VPN Inventory* and click on the button ➕ in the upper right corner of the table.



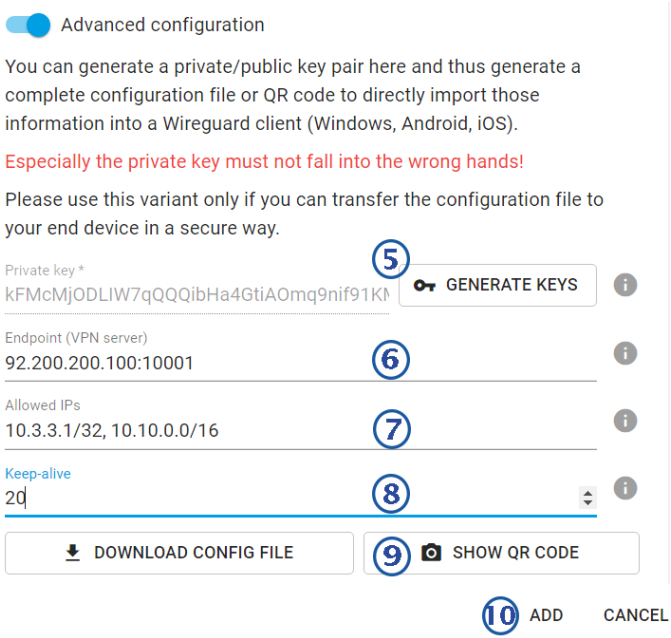
1 10.3.3.5
The IP address of the VPN client from the virtual VPN network area.

2 Android Service 1
Freely selectable name of the VPN client.

3 The VPN client should have access to the configuration interface of the Microwall VPN and should be activated immediately after creation. Therefore activate both options.

4 The Microwall VPN should generate the entire configuration file for the VPN client. To do this, activate the *Advanced configuration* check box.

This way should only be chosen if it can be guaranteed that the configuration file can be transmitted safely to the client.



5 The *Generate Keys* button creates a key pair for the VPN client. The private key is saved by the Microwall VPN exclusively for the duration of this creation dialog and then deleted.

6 92.200.200.100:10001
End point under which the VPN server can be reached. In this example, this is the WAN-side official IP address of the DSL router that connects the intranet to the Internet. Colon-separated, the UDP list port of the VPN server must be specified.

Please also note the NAT rule of the perimeter firewall of the intranet described in the Preparations *section.*

⑦ 10.3.3.1/32,10.10.0.0/16
IP addresses and IP ranges in CIDR notation, which occur and should be accepted within the VPN connection. If the desired communication partner is located directly in the island network, it is usually not necessary to change the specifications.

⑧ 20
Interval in which the WireGuard VPN client generates Keep Alive packets to maintain the UDP tunnel in the participating routers.

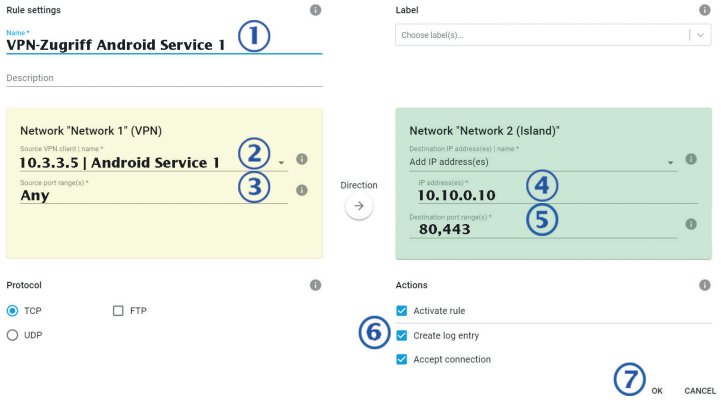
⑨ Finally, the button *Show QR Code* generates the QR Code with the content of the VPN Client configuration. Start the WireGuard app on the mobile device and select the Import from QR Code option. If the QR Code was read successfully, assign a name for the new VPN connection.

⑩ *Add* closes the configuration dialog and takes you to the overview page of the VPN client inventory.

saves and activates the changes.

4. VPN rule for access to the island device

Switch to the page *VPN settings -> VPN rules* and click on the button ➕ in the upper right corner of the table.



① VPN access Android Service 1
Freely selectable name of the VPN rule

② 10.3.3.5 | Android Service 1
Selection of the VPN client from the VPN inventory as source of the TCP connection to be released.

③ Any
The source port of the TCP connection is arbitrary.

④ 10.10.0.10
Select the destination host in the island network as the destination of the TCP connection to be released.

⑤ 80,443
The destination port of the TCP connection. The Web service on the target system is addressed via TCP ports 80 or 443.

⑥ The protocol of the connection is TCP. Connections according to the settings should be accepted and documented in the log file of the Microwall VPN. The formulated

rule should be activated immediately.

7 *Add* closes the rules dialog and takes you to the overview page of the VPN rules.

saves and activates the changes.

5. Testing the VPN connection

On the Android device, open the WireGuard app and activate the VPN tunnel you created earlier. In the Android status bar a key symbol should now signal the VPN connection. Start a browser and enter the IP address of the island host in the address line:

http(s)://10.10.0.10

To access the configuration pages of the Microwall VPN, use the virtual IP address of the VPN server as destination:

https://10.3.3.1

7 Security & Maintenance

- Security and operating notes
- Firmware updates
- Individual certificates
- Emergency access via service button
- Reset to factory defaults

7.1 Security notes

The following sections contain relevant notes and recommendations from an IT security perspective for commissioning, configuration, operation and maintenance of the Microwall VPN.

7.1.1 Function

The Microwall VPN is a small firewall designed as a router with two Ethernet ports and an integrated WireGuard VPN server. The typical application is to decouple a network island from a higher-level intranet and to allow only connections that are explicitly permitted by a whilelist-based firewall. For the purpose of remote maintenance, it is possible to allow access to participants on the network island and the management interface of the Microwall VPN via the VPN server.

7.1.2 Installation location

The installation location of the Microwall VPN must ensure that no unauthorized physical access can occur (e.g. suitably secured room or network cabinet). Physical access to the Microwall VPN entails the following risks, for example:

- Decommissioning of the device (removal of network cable, power supply ...) and loss of all connections to the participants of the island network

- Start emergency access of the Microwall VPN via the service button and thus deactivate or change the password. An attacker gets full access to the management interface and is able to create firewall rules or create unauthorized VPN clients.

7.1.3 Start-up

The start-up of a Microwall VPN is divided into the assignment of an IP address with the WuTility tool and the subsequent call of the initial web page with the configuration of the password

and the network-side basic parameters. Only after this step is access to the management interface of the Microwall VPN protected by the password.

IP allocation and password assignment
During initial start-up, make sure that no unauthorized access to the Microwall VPN occurs until the password is assigned on the initial web page. A suitable measure is, for example, to perform the commissioning steps via a point-to-point connection with the configuring computer. Only then is the Microwall VPN connected to the target networks.

Password
The Microwall VPN password is the central protection against unauthorized access to the configuration and management of the Microwall VPN. We recommend the use of a secure password with a length of at least 15 characters consisting of upper and lower case letters, numbers and special characters.

Registration for security relevant information
Devices can be registered with W&T via the inventory tool. In case of security relevant updates and/or information you will be informed immediately by email. In addition to the personal data provided, device-specific data is also stored during registration.

7.1.4 Operation and configuratiuon

Individual device certificate
Access to the Web-based management can only be encrypted via HTTPS. A self-signed default certificate is used ex works for this purpose, for which an exception must be set up in the browser used during commissioning. For access during operation, we recommend replacing the default certificate with an individual certificate of your own.

Deactivation of not needed services
With the factory settings, the Microwall VPN provides the following incoming own services after commissioning:

Port/Socke number	Application	System-pass-word?	Configu-rable/ deactivata-ble?
443 (TCP)	HTTPS management	yes	yes/yes
8513 (UDP)	Inventory e.g. with WuTility	no	no/yes
5555 (TCP)	Firmware update with WuTility	yes	no/yes
446 (TCP)	HTTPS emergency access (only after manual activation via the service button)	no	no/yes

Configuration and activation/deactivation of these services is done in the menu tree under *Settings -> Network*. For each service it can be determined on which port it is available. For web-based management, the TCP port used can also be changed.

In environments with increased security requirements, it may make sense to deactivate some or all of these services after the communication rules have been set up during operation. For any changes that may become necessary at a later date, HTTPS access can be reactivated as required at any time via the emergency access accessible via the service button. (see chapter *Emergency access to the Microwall VPN*).

Formulating the whitelist rules

The Microwall VPN has no default rules for communication between the two network connections or for a VPN client. When formulating rules, we recommend that they be as concise as possible according to the need-to-know principle. For example, the use of a unicast address offers a higher level of security than an IP range.

Confidentiality of private keys
Asymmetric encryption with the corresponding public/private key pairs are used in the Microwall VPN for the TLS protocol for web accesses as well as for authentication within the WireGuard VPN protocol. Both private keys of the Microwall VPN cannot be read out.

When setting up WireGuard VPN clients, there is an optional option to have the key pair of the new client generated by the Microwall VPN for reasons of user-friendliness. Only choose this method if you can guarantee a confidential transmission of this key to the VPN client. For applications with increased protection requirements, we recommend generating the key pair on the VPN client and then transmitting the uncritical public key to the Microwall VPN in another way.

7.1.5 Service and maintenance

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

- Backup/storage of the device configuration
- Provision of a replacement unit if necessary
- Documentation of the procedure for exchanging devices

7.2 Up-/Download of configuration backups

On the *Maintenance* page, it is possible to save the current configuration of the Microwall VPN or to write back a previously downloaded backup file.

Configuration or backup files contain not only the operative parameters (firewall/VPN rules, VPN keys, inventory lists, etc.) but also the data relevant for administrative access to the Microwall VPN (IP parameters, system password, certificate, etc.). For this reason, backup files are encrypted and cannot be edited. For extended protection, we recommend that you also provide the file with an individual backup password. This password must then be known when uploading the file to a Microwall VPN.

Download configuration
The *Download configuration* button starts the download of all current configuration parameters of the Microwall VPN. If the file is to receive an individual backup password, this must be entered in the Backup Password field before the download.

DUploading a backup file with a password is only possible if you know this password. You should therefore save the password in a suitable form separately from the backup file.

Upload configuration
Uploading a backup file is possible in two places:

- Standard WBM -> Maintenance
- Initial web page in the course of commissioning

If the backup file is protected with a password, this must be entered in the Backup Password field. The *Upload Configuration* button starts the file selection dialog and the transfer. After the file has been successfully checked, its contents are accepted and the Microwall VPN operates with the new parameters after an automatic restart.

Backup files also contain the new IP address of the Microwall VPN. To avoid an IP conflict, make sure that the original or a previously programmed Microwall VPN is no longer connected to the network before uploading.

7.3 Firmware updates

The firmware can be updated either using the WuTility management tool or via the web-based management of the Microwall VPN.

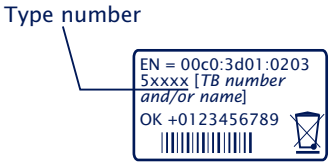
7.3.1 Where is the latest firmware available?

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

https://www.wut.de

The easiest way to navigate from there is to use the search function on the page. First enter the type number of your device in the input field.

If you do not know the type number, you can find it on the sticker on the narrow side of the housing, which also contains the Ethernet address.

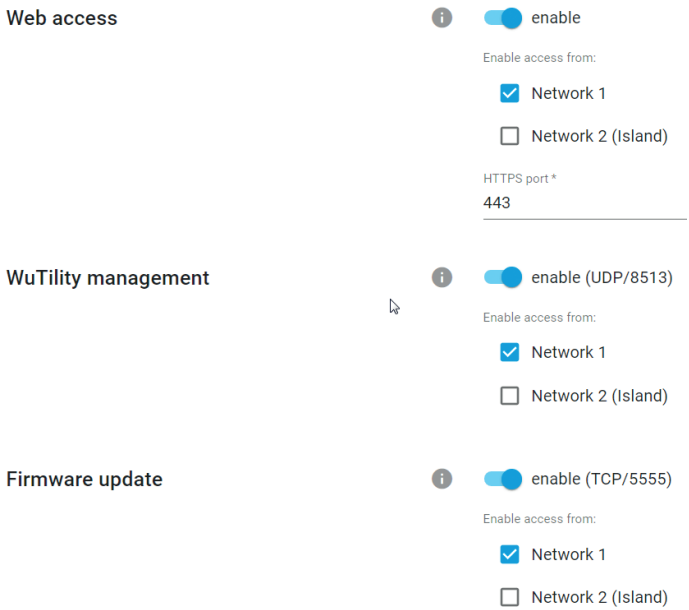


On the Microwall VPN web data sheet, follow the *Firmware* link and start the download of the desired version. Before uploading to the Microwall, the actual firmware file must be unpacked from the zip archive.

7.3.2 Firmware update with WuTility

For the firmware update with WuTility, it must be installed on a Windows PC. Its IP settings must allow communication with the Microwall and its current IP parameters.

A prerequisite for firmware updates with WuTility is the activated update service to TCP/5555 in the Microwall VPN. With the factory settings, the update with WuTility is only possible via the interface Network 1.



The network communication during the transmission of the system password and also the actual upload is encrypted and therefore confidential.

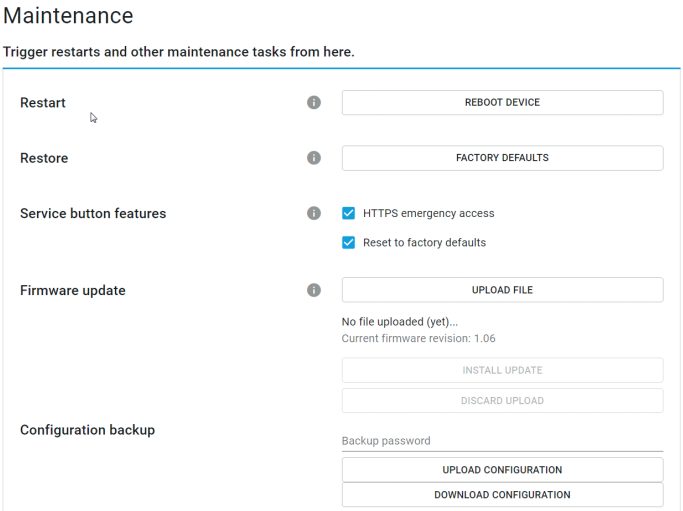
To transfer the new firmware to the Microwall VPN, select the desired Microwall in the WuTility inventory list and click on the *Firmware* button.

In the following dialog select the firmware file (*.uhd) to be transferred and click on the *Next* button. After the successful transfer, the Microwall VPN decrypts the firmware file, checks the signature and writes the firmware to its internal flash. Finally, a restart is performed automatically and the Microwall VPN is ready for operation again.

7.2.3 Firmware Update via Web-Based Management

In network environments that do not permit the use of WuTility or in which the update service in the Microwall VPN has been deactivated for security reasons, the firmware update can be performed from the Web-based management.

Switch to the *Maintenance* page in the menu tree of the Microwall VPN.



The *Upload File* button starts the selection dialog for the firmware file. Select here the previously downloaded and unzipped firmware file (*.uhd). After the upload, the *Install Update* button starts the actual installation of the new firmware.

7.4 Individual certificates

For security reasons, access to the web-based management of the Microwall VPN is only possible in encrypted form using the HTTPS protocol.

The Microwall VPN's self-signed certificate, which is pre-installed ex works, generates corresponding security warnings for current browsers. These must be acknowledged for WBM accesses and/or confirmed with suitable exception rules.

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

Generation, signature and installation of an individual certificate are divided into the following rough steps:

- Generation of a CSR (Certificate Signing Request) with associated private key in the Microwall VPN
- Download the CSR and external signature to a certificate by a trusted certificate authority.
- Upload and installation of the certificate into the Microwall VPN

Navigate in the menu tree to the page *Basic settings -> Certificate*. In addition to information on the currently installed certificate, all functions for handling individual certificates are included here:

Create a Certificate Signing Request (CSR)
Fill in all the required information in the CSR form. The only mandatory field is the *Common Name*, under which the web pages of the Microwall VPN will later be called up in the browser. Additional names, IP addresses and also wildcard names can be entered under *Alternative Names*. The name entered in *Common Name* is automatically transferred to the *Alternative Names*.

By clicking on *Create*, the Microwall VPN generates a pair of keys and creates a CSR from the information entered.

Installing a self-signed certificate

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

Externally signed certificate

The generated signing request can be downloaded from the Microwall VPN using the *Download* button for external signature. The download is in PEM format

After the signature by a trustworthy certification authority (CA), the certificate and any certificate chain that may be required can be loaded into the Microwall VPN using the corresponding upload buttons. All files must be in PEM format.

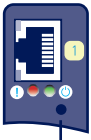
After a formal check, the certificate is integrated into the system by clicking on *Install* under *Externally signed certificate* and used for all web accesses.

Information and expiry of certificates

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

7.5 Emergencies access to the Microwall VPN

In case of a forgotten password or if web-based management has been deactivated for security reasons, emergency access can be activated via the recessed mounted service button on the front panel.



Service button

Start emergency access
Press the button with a suitable pointed object (e.g. paper clip) and keep it pressed until the error LED flashes slowly after approx. 3.5s. If you release the button now, the emergency access is activated.

The router/firewall function is completely retained in this state.

The emergency access activates a non-password-protected web page on the Microwall VPN with the possibility to overwrite the current password. You should therefore take appropriate measures against unauthorized access in advance.

Calling and function of the emergency access
Emergency access is provided by browser with HTTPS via TCP port 446:

https://[IP address|hostname]:446

Without a password request you can access the website with the following options:

Overwriting the current password
By activating the *Change password* option, you have the possibility to change the current password for access to the web management.

We recommend passwords with a minimum length of 15 characters, consisting of upper and lower case letters, numbers and special characters. The maximum length of the password is 51 characters.

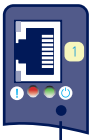
Activating standard Web-Based Management
Under Management, define on which connection and under which port the web management of the Microwall VPN should subsequently be accessible.

Terminating the emergency access
Changes are applied with a click on *Apply* and the Microwall restarts the affected services. Afterwards, access to the password-protected standard web interface is possible via the previously configured TCP port.

A click on *Cancel* discards any changes made and the Microwall restarts the required services. The password protected standard web interface can then be accessed via the configured TCP port.

7.6 Reset to default settings

A reset to the factory settings of the Microwall VPN can be performed using the recessed mounted service button on the front panel.



Service button

Press the service button with a suitable pointed object (e.g. paper clip) and keep it pressed for at least 20s. After 3.5 the error LED starts flashing slowly and after approx. 10s it starts flashing fast. After a total of approx. 20s, the device is reset to the factory settings. If the service button is released while the service LED is flashing quickly within a time window of 10-20s, the factory default reset is aborted and the Microwall continues with standard operation according to the current configuration.

The reset is completed as soon as the system LED is permanently lit again. The Microwall VPN must now be put into operation again. For more information, please refer to the chapter *Start-up*.

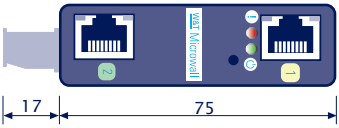
8 Appendix

- Technical data and form factor
- Licenses

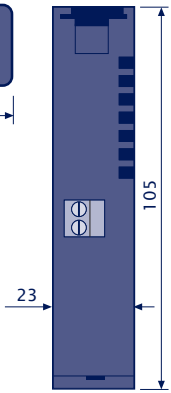
8.1 Technical data and form factor

Power supply ... Power-over-Ethernet: External power supply, screw terminal	 37-57V DC from PSE DC 24-48V (+/-10%)
Current consumption ... Power-over-Ethernet: Ext. supply	 PoE Class 2 (3,84 W - 6,49W) typ. 150mA@24V DC max. 200mA@24V DC
Galvanic isolation	Network interfaces: min 500V
LAN-Port *Network 1*	10/100/1000BaseT, RJ45, autosensing, autocrossing, PoE
LAN-Port *Network 2*	10/100/1000BaseT, RJ45, autosensing, autocrossing
Permissible ambient temperature ... ... Storage ... Operation, non-cascaded	 -40 ... +85°C 0 ... +50°C
Permissible rel. humidity	0 - 95% (non-condensing)
Dimensions	105 x 75 x 22mm
Weight	ca. 120g

Front view 55211



Bottom side 55211



Measure in mm, +/- 1mm

8.2 Licenses

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

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