

W&T

www.WuT.de

Manual

Startup and application

Microwall

Valid for the following models:

#55211: Microwall VPN

Firmware 1.36 or higher

#55212: Microwall IO

Firmware 1.12 or higher

Release 1.07 04/2023

© 04/2023 by Wiesemann und Theis GmbH

Microsoft and Windows are registered trademarks of Microsoft Corporation.

WireGuard and the WireGuard logo are registered trademarks of Jason A. Donenfeld

Subject to error and alteration:

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. For more information, refer to your device.

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.

Introduction

The Microwall VPN and Microwall IO are industrial-grade IPv4 router with two 1000BaseT network connections, integrated whitelist-based firewall and a WireGuard VPN access. They connect a network island, e.g. with automation components, to a higher-level local network. Parallel to this, secure remote access to the participants of the island network can take place via the Wireguard VPN as a client or server. Suitable filter rules at TCP/IP level protect all networks from unauthorized, undesired and harmful communication.

The Microwall IO has 2 digital inputs and 2 digital outputs, which allow the control of router/firewall functions and the evaluation of messages in automation environments.

Content

1	Legal information and safety	7
1.1	Legal notices	8
1.2	Safety notices	10
2	Hardware, interfaces and displays	13
2.1	Hardware installation	14
2.2	Power supply	15
2.2.1	PoE- supply	15
2.2.2	External power supply	15
2.3	Network Interfaces	16
2.4	System and Error LED	18
2.4.1	System LED ☺ (green)	18
2.4.2	Service LED ⚠ (red)	18
2.5	Service button	19
3	Start-up	21
3.1	IP assignment via DHCP	22
3.2	Initial assignment of IP parameters with WuTility	23
3.3	Start-up via the default IP address	26
3.4	Initial web page	27
4	Web based management	31
4.1	Start and navigation concept of the WBM	32
4.2	Login/Logout	33
4.3	Help and description texts	34
5	DHCP server & Discover assistant	35
5.1	DHCP server	36
5.2	Discover assistant	38
6	Operating modes and rule configuration	39
6.1	Mode NAT router	40
6.2	Mode Standard router	42
6.3	Mode Standard router with static NAT	44
6.4	IP inventories	46
6.4.1	Scan of Network 2	47
6.5	Creating firewall rules	48
6.5.1	Using hostnames as the target of a rule	51
6.6	Examples Firewall rules	52
6.6.1	Mode Standard router, Network 2 to Network 1	52
6.6.2	Mode NAT-Router, Network 1 to Network 2	54

W&T

7 Wireguard VPN server	57
7.1 Overview WireGuard VPN Server	58
7.2 Configuring the VPN environment	59
7.3 VPN client inventory	61
7.3.1 New VPN clients - Standard configuration	61
7.3.2 New VPN clients - Advanced configuration	63
7.4 VPN rules	65
7.5 Step by step: VPN access for a mobile device	68
8 Wireguard VPN client	75
8.1 Overview WireGuard VPN-Client	76
8.2 VPN client	77
9 Wireguard-VPN Box-to-Box	81
9.1 Overview WireGuard VPN Box-to-Box	82
9.1.1 Configuration example VPN Box-to-Box	82
10 Digital inputs and outputs (only Microwall IO)	89
10.1 Digital inputs	90
10.1.1 Wiring of the digital inputs	90
10.2 Digital outputs	92
10.2.1 Wiring of the digital outputs	92
11 Security & Maintenance	93
11.1 Security notes	94
11.1.1 Function and typical use	94
11.1.2 Requirements for integrators and operators	94
11.1.3 Installation location	95
11.1.4 Commissioning	95
11.1.5 Operation and configuration	96
11.1.6 Service, maintenance and decommissioning	99
11.2 Up-/Download Configuration data	100
11.3 Firmware updates	102
11.3.1 Where is the latest firmware available?	102
11.3.2 Firmware update with WuTility	103
11.3.3 Firmware Update via Web-Based Management	104
11.4 Individual certificates	106
11.5 Emergency access to the Microwall	108
11.6 Reset to default settings	110
Appendix	111
Technical data and form factor	112
Microwall VPN, #55211	112
Microwall IO, #55212	113
Index	114

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.

W&T

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 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 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 client/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.

The Microwall IO has 2 digital inputs and 2 digital outputs, which allow the control of router/firewall functions and the evaluation of messages in automation environments

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

Electrical safety

WARNING

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

The Microwall 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

W&T

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 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 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 to the network.

In this case the Microwall 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.

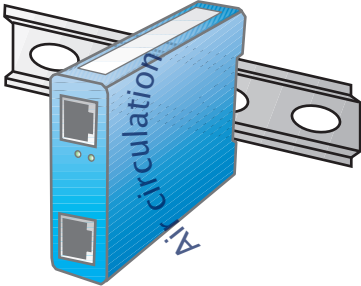
The complete Declarations of Conformity for the devices described in the manual can be found on the corresponding Internet page at the W&T homepage: <http://www.wut.de>.

2 Hardware, interfaces and displays

- Hardware installation
- Power supply
- Network interfaces
- Service button
- Digital IOs (only Microwall IO)

2.1 Hardware installation

The Microwall 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.



i *The installation site must be adapted to the security requirements of the respective system environment. Physical access to the Microwall 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 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.

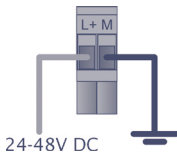
2.2.1 PoE- supply

The Microwall 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 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%)



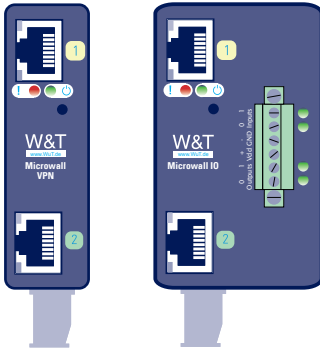
⚠WARNING

Only a floating power supply unit may be used for the external supply of the Microwall. 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 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 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

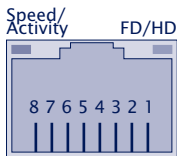
There is an electrical isolation of at least 500Vrms from the supply voltage

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



System LED

Service LED

2.4.1 System LED 🟢 (green)

ON: Signals normal operational readiness.

Flashing: The Microwall 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.

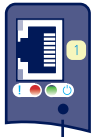
Slow flashing: The service button was pressed between 3.5s and 10s. The emergency access of the Microwall is activated.

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

i *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 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



Service button

The service button is accessible recessed on the front side of the Microwall 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.

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 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*.

i *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.

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

3.1 IP assignment via DHCP

In network environments with DHCP support and a dynamic address pool, the Microwall automatically receives the following basic IP parameters via the *Network 1* port.

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

The additional parameters required for the initial commissioning are set with the help of a browser after the IP assignment via the initial web page. For more information, refer to the chapter *Initial Web Page*.

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


i *For operational use of the Microwall, we recommend operation with a static IP address. Especially in the Standard Router mode, a change of IP address by the DHCP server otherwise requires an adjustment of all static routes in the hosts communicating via the Microwall. For more information, refer to the chapter Standard Router Mode.*

3.2 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

- 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 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 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*

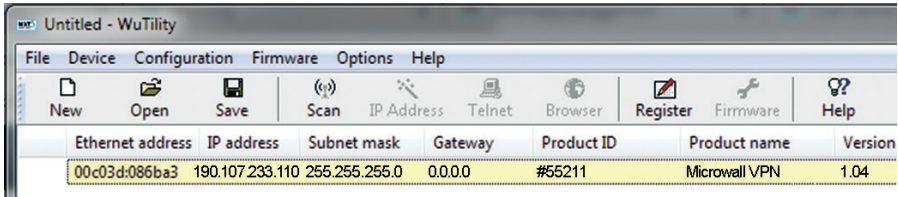
Start of the assignment dialog

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:



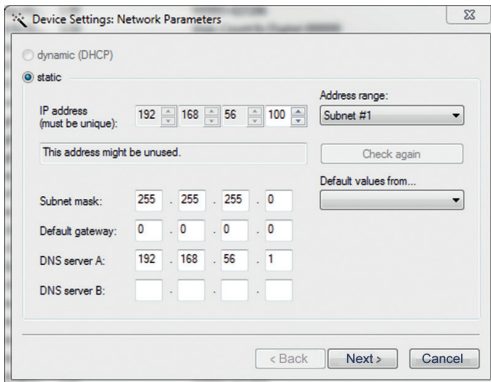
Within the inventory list, the desired Microwall can be identified via its MAC address. The default IP address is 190.107.233.110.



Select the desired Microwall and then press the *IP 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.

The IP assignment with WuTility can be repeated until the Microwall 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*.

3.3 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.

i *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 occurs until the password is assigned on the initial web page (e.g. by commissioning with a direct connection to the respective PC).*

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

On the computer side, the following requirement 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.

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*.

3.4 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.

i *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 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 and click on the Browser button:



If access is to take place via the default IP address of the Microwall, 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.

Initialization

Login password

Login password	<input type="password"/> Password * <input type="password"/> Repeat password *
----------------	---

Network 1

IP settings intranet	<input type="radio"/> DHCP <input checked="" type="radio"/> statisch
	Network name * Network 1
	IP address * 192.168.0.10
	Subnet mask * 255.255.255.0
	Default gateway 192.168.0.1

Network 2

IP settings island	<input type="radio"/> DHCP <input checked="" type="radio"/> statisch
	Network name * Network 2 (Island)
	IP address * 10.10.0.1
	Subnet mask * 255.255.0.0

Router mode


Router mode	<input type="radio"/> Standard router <input checked="" type="radio"/> NAT router
-------------	---

Configuration backup

Configuration backup	<input type="password"/> Backup password <input type="button" value="UPLOAD CONFIGURATION"/>
----------------------	---

Login password (mandatory)


Assign the password for all configuration/control accesses of the Microwall. 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)

Specify whether the connection works with a static IP address or whether the IP parameters are obtained via DHCP.

In static operation, assign the IP parameters for the *Network 1* connection (yellow).

 *For operational use of the Microwall, we recommend operation with a static IP address. Especially in the Standard Router mode, a change of IP address by the DHCP server otherwise requires an adjustment of all static routes in the hosts communicating via the microwall. For more information, refer to the chapter Standard Router Mode.*

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. 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.

Configuration backup

Allows you to upload a configuration backup previously secured by another Microwall. 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 Micro-wall operates with the new parameters after an automatic restart.

 *Backup files also contain the new IP address of the Micro-wall. To avoid an IP conflict, make sure that the original or a previously programmed Microwall 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 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, you need an up-to-date Internet browser. Session-Cookies, Javascript and Websockets 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

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

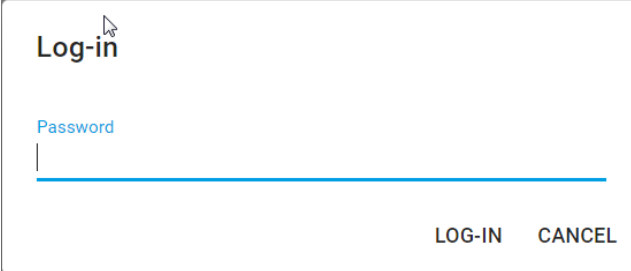
After login, any changes made are immediately applied by clicking the *Save* button on the respective page. If a restart of the Microwall is required to accept the parameters, a corresponding message is displayed after pressing *Save*.

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

A screenshot of a login form. At the top left, the text "Log-in" is displayed in a bold, black font, with a mouse cursor hovering over it. Below this, the word "Password" is written in a light blue font above a horizontal blue input field. At the bottom right of the form, there are two buttons: "LOG-IN" and "CANCEL", both in a light blue font.

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

i *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 DHCP server & Discover assistant

- DHCP server for *Network 2*
- Static and dynamic leases
- Controlled commissioning of new or third-party devices
- Identification of unwanted connections

5.1 DHCP server

The Microwall can work as a DHCP server in *Network 2*. The DHCP server is activated and configured in the menu branch *Basic settings -> DHCP server*.

Dynamic leases in case of service

Exclusively for service applications, e.g. for the quick connection of a notebook, the DHCP server supports the dynamic assignment of IP addresses from a configurable address pool.


The Microwall DHCP server does not create a binding between a dynamically assigned IP address and the MAC address of the respective client. In response to new requests, the first free address from the pool is always assigned, regardless of whether the host may have been previously assigned a different address.

For this reason, static leases must be created for DHCP clients that are used in release rules during operation.


Static leases

To support static DHCP leases, the Microwall provides on 3 lists.


DHCP lease requests

All requests received by the Microwall on network 2 for which no static lease has yet been assigned are listed here. The button  starts the dialog for creating a static lease for the respective device.

Static DHCP leases

All created static leases are listed here and can be edited. The button  allows you to create a new lease manually.

As a default for the DNS server, the Microwall assigns its IP address in Network 2 and works there as a DNS proxy.

 *The assignment of the Microwall as DNS proxy for the clients is the prerequisite for the use of the Discover mode. When using external DNS servers that can be reached via*

Network 1, it must also be noted that a corresponding firewall rule is required.

Current DHCP leases

Listing of all devices provided with a lease by Microwall.

5.2 Discover assistant

The Discover assistant allows the controlled commissioning of new devices in *Network 2* (green). Outgoing connection attempts of selected hosts are recorded and displayed together with the previously resolved host name. However, the connections remain blocked until a corresponding release rule is generated for the desired communication by mouse click.

Discover assistant

Monitor communication attempts and allow desired connections with a mouse click.

Mode

inventory entry

custom IP

Enter IP address

10.120.0.78

▶ START

all devices

Communication attempts

Timestamp	Destination (Intranet)	Source (Island)	Firewall rules
06/14/2022 12:04:14 PM	www.wut.de (92.204.239.49) TCP/80	10.120.0.78 TCP/47018	<i>new rule</i> ⊕
06/14/2022 12:04:17 PM	virenschleuder.de (217.160.231.199) TCP/443	10.120.0.78 TCP/33970	<i>new rule</i> ⊕

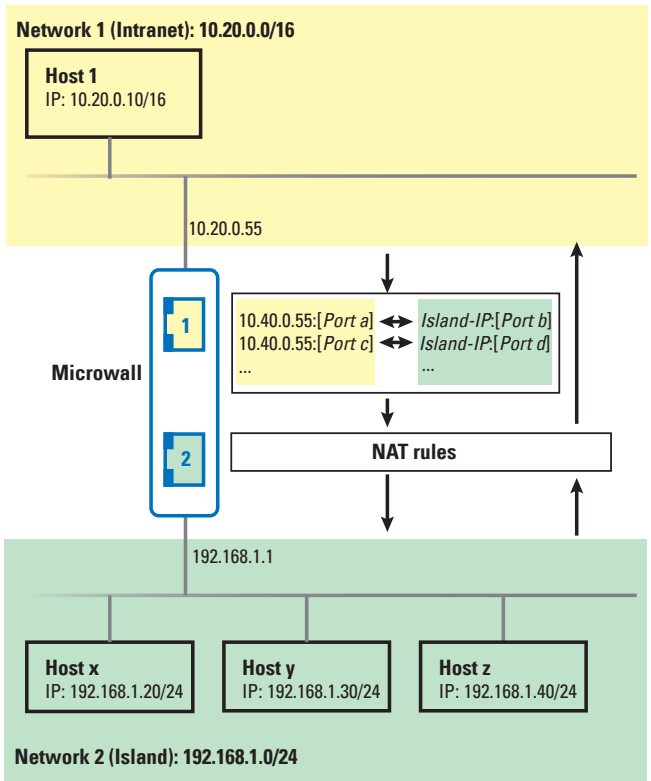
6 Operating modes and rule configuration

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

6.1 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 super-ordinate network by the local IP address of the Microwall 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) to the local interfaces and the forwarding of other ICMP datagrams..

Operation mode

Configure the operation mode and ping behaviour here.

The screenshot shows a configuration window with the following content:

- Router mode:** Two radio buttons. The first is labeled "Standard router" and is unselected. The second is labeled "NAT router" and is selected (indicated by a blue dot).
- ICMP:** Two checkboxes. The first is labeled "Allow ping to local interfaces" and is unselected. The second is labeled "Allow *Network 2* -> *Network 1*" and is unselected.
- At the bottom right of the window, there are two circular buttons: a blue "Save" button and a grey "Refresh" button.

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

To allow communication between nodes from the intranet and the island network after enabling the *NAT router* mode, explicit allow rules must be configured in the following submenu. There are no factory default rules.

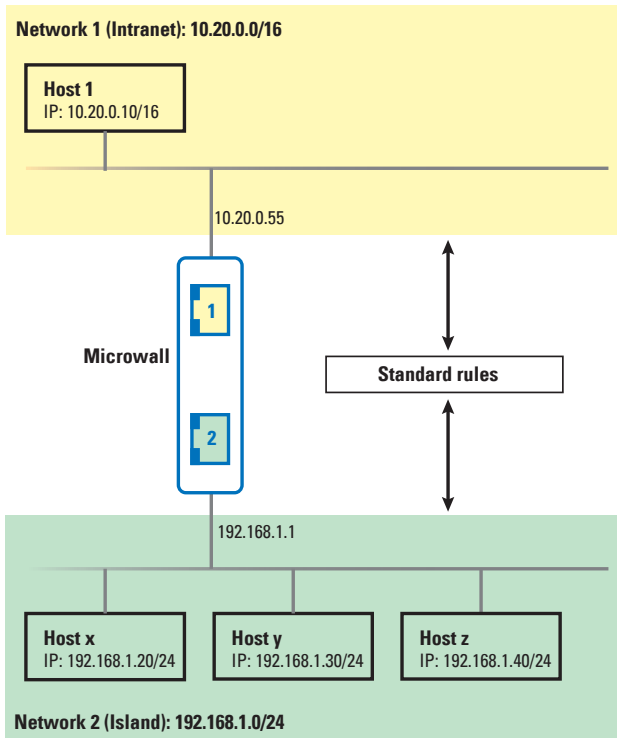
- Firewall settings ^
 - Operation mode
 - Standard rules
 - NAT rules
-

6.2 Mode Standard router

In standard router mode, the Microwall 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 Microwall 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) to the local interfaces and the forwarding of other ICMP datagrams..

Operation mode

Configure the operation mode and ping behaviour here.

Router mode	<input checked="" type="radio"/> Standard router	<input type="radio"/> NAT router
ICMP	<input type="checkbox"/>	Allow ping to local interfaces
	<input type="checkbox"/>	Allow "Network 2" -> "Network 1"
	<input type="checkbox"/>	Allow "Network 1" -> "Network 2"

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

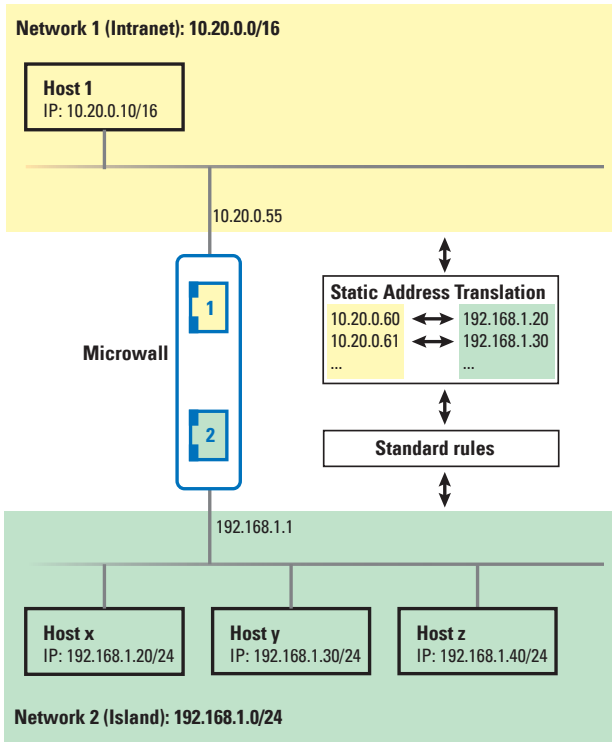
To allow communication between nodes from the intranet and the island network after enabling the *Standard router* mode, explicit allow rules must be configured in the following sub-menu. There are no factory default rules.

- Firewall settings ^
- Operation mode
- Standard rules

6.3 Mode Standard router with static NAT

The Standard Router mode offers the option of a fixed 1:1 assignment of IP addresses from the corporate intranet at the Network 1 (yellow) port to IP addresses from the island network. For this purpose, the Microwall receives additional secondary addresses from the intranet in addition to the primary IP address from the intranet. In the translation table for the Static NAT, these are assigned to the desired hosts in the island. The secondary IP addresses do not provide access to Microwall services (WBM, Update, Ping, etc.).

With the help of static NAT, island hosts appear on the intranet as if they were members of the local network. Suitable firewall rules must be configured for communication with the island hosts. No modification of the intranet-side routing concept is required.



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) to the local interfaces and the forwarding of other ICMP datagrams..

Operation mode

Configure the operation mode and ping behaviour here.

Router mode ⓘ Standard router NAT router

ICMP ⓘ

- Allow ping to local interfaces
- Allow "Network 2" -> "Network 1"
- Allow "Network 1" -> "Network 2"

⏏ ⏪ ⏩

The *Plus* button at the top right of the Static NAT table opens the dialog for creating new mappings. In the following dialog, determine which IP address of the intranet (*Network 1, yellow*) should be assigned to the desired IP address in the island network (*Network 2, green*).

Static NAT (1-to-1) +

<input type="checkbox"/> Device IP (intranet)	Target IP (island)
No data available...	

Please note that you must also define corresponding firewall rules to actually access the target IP(s).


The *Save* button activates the *Standard Router* mode with the associated table for the Static NAT and loads the associated rule set.


To allow communication between nodes from the intranet and the island network after enabling the *Standard router* mode, explicit allow rules must be configured in the following sub-menu. There are no factory default rules.







- Firewall settings ^
- Operation mode
- Standard rules



6.4 IP inventories







In the menu branch *Firewall Settings* -> *IP Address Inventory*, the Microwall 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.

MicrowallVPN-08B7B2 / Firewall settings / IP address inventory LOG-OUT 

Network "Network 1" 

<input type="checkbox"/> IP address(es)	Name Description		In use
<input type="checkbox"/> ANY	Any	1	 
<input type="checkbox"/> 192.168.10.1	DNS	1	 
<input type="checkbox"/> 192.168.10.254	Srv-1	0	 

Network "Network 2 (Island)"  

<input type="checkbox"/> IP address(es)	Name Description		In use
<input type="checkbox"/> 10.10.0.0/16	Subnet Island	3	 
<input type="checkbox"/> 10.10.0.78	SRV-2	3	 
<input type="checkbox"/> 10.10.0.200	hp switch	2	 

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

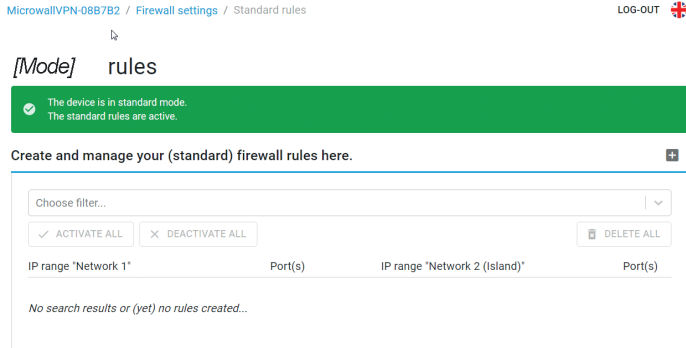
- *any*
Keyword for any IP address
- *single IP address*
IP address in dot notation (e.g. 10.20.0.4)
- *Comma-separated IP address list*
List of IP addresses in dot notation (e.g. 10.10.10.1, 20.20.20.2)
- *IP range*
Continuous IP range in the form „from-to“ (e.g. 10.10.10.1 - 10.10.10.20)
- *IP- range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

6.4.1 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*.

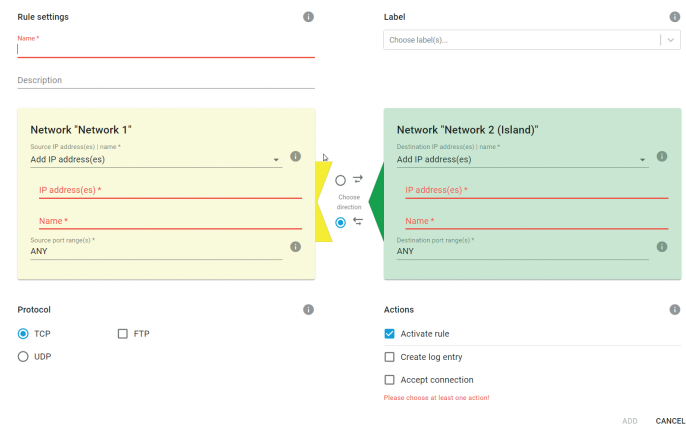
6.5 Creating firewall rules

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.

i Rule examples for many standard applications can be found on our website at <https://www.wut.de/ruleexamples>.



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 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 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.

6.5.1 Using hostnames as the target of a rule

In rules that enable connections in the direction of *Network 1*, the destination can also be specified in the form of a host name (e.g. *www.wut.de*). The prerequisite for this is that the initiating participants in *Network 2* use the IP address of the microwall there as the DNS server.

 *If the microwall works as a DNS proxy for users in Network 2, the DNS server configured on Network 1 must be accessible for correct query response.*

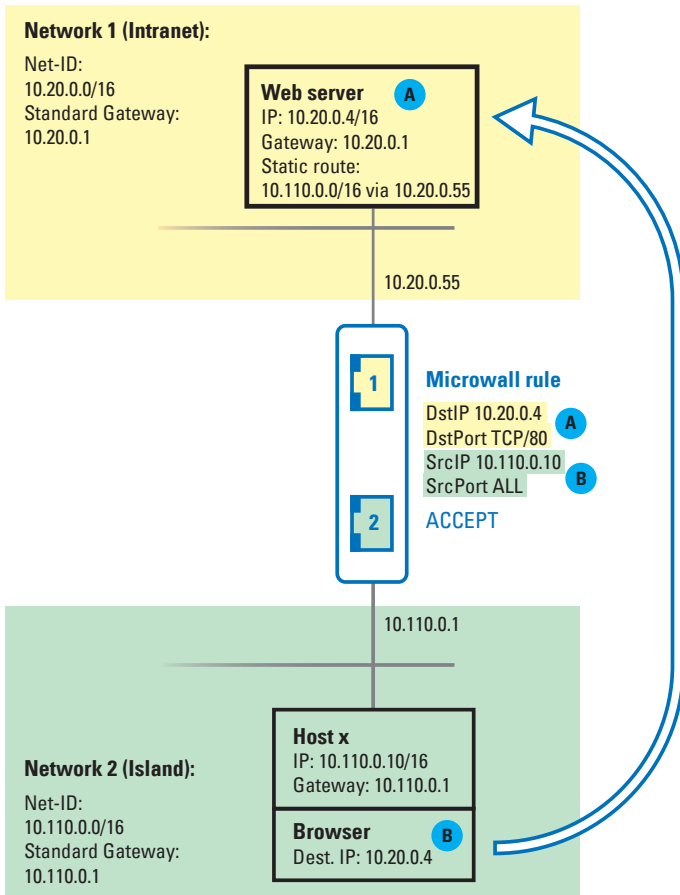
Individual host names as well as comma-separated host lists can be used (e.g. *www.wut.de, www.timeair.de*).

The * character can be used as a wildcard in a hostname. Within a hostname, one wildcard is allowed and it must be at the beginning (e.g. **.wut.de*). Within name lists this applies to every hostname.

6.6 Examples Firewall rules

6.6.1 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 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*.



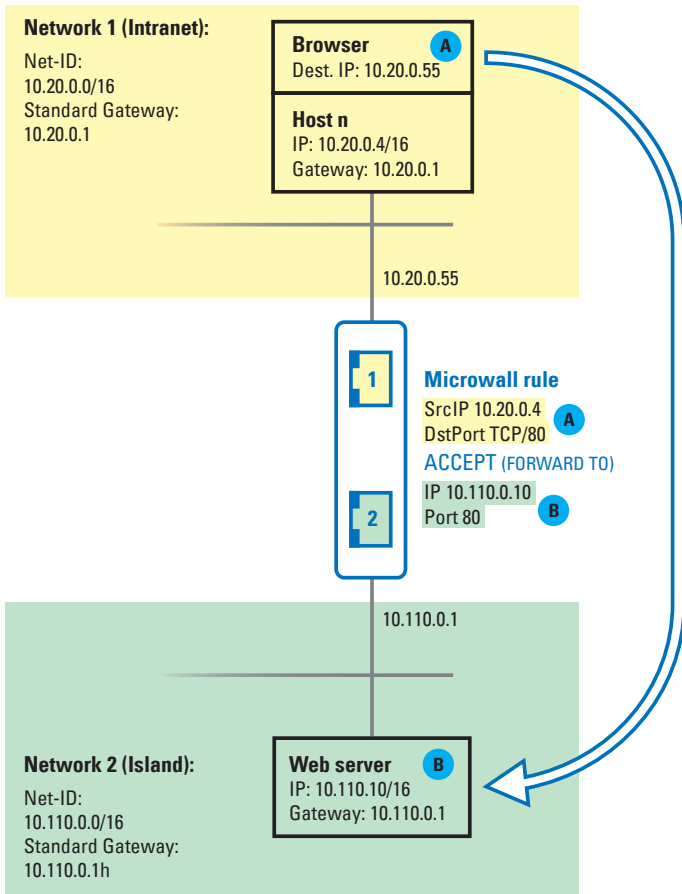
The rule dialog to be filled out for this example:

The screenshot shows a rule configuration dialog with the following sections:

- Rule settings**: Name "Example Web access", Description field.
- Label**: "Normal mode".
- Direction**: A central button with a left-pointing arrow.
- Source Network (Network 1)**: IP address(es) "10.20.0.4", Name "Intranet server", Source port range(s) "80".
- Destination Network (Network 2 (Island))**: IP address(es) "10.110.0.10", Name "Island browser", Destination port range(s) "ANY".
- Protocol**: Radio buttons for TCP (selected) and UDP, and checkbox for FTP.
- Actions**: Checkboxes for "Activate rule" (checked), "Create log entry", and "Accept connection" (checked).
- Buttons**: "ADD" and "CANCEL" at the bottom right.

6.6.2 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 itself is integrated into the networks with the IPs 10.110.0.1 and 10.20.0.55. The intranet IP of the Microwall 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:

The screenshot shows a rule configuration dialog with the following sections:

- Rule settings:** Name: Example Web access; Description: (empty).
- Label:** Choose label(s)...
- Network "Network 1" (Source):** IP address(es): 10.20.0.4; Name: Browser intranet; NAT port: 80.
- Network "Network 2 (Island)" (Destination):** IP address: 10.110.0.10; Name: Island server; Destination port: 80.
- Protocol:** TCP (selected), FTP, UDP.
- Actions:** Activate rule (checked), Create log entry, Accept connection (checked).

Buttons: ADD, CANCEL

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

7 Wireguard VPN server

- Configuration of the microwall as VPN server with permitted clients
- Creating firewall rules for the VPN server mode

7.1 Overview WireGuard VPN Server

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 the 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 all common operating systems (Windows, Linux, Android, IOS, MacOS).

<https://www.wireguard.com>

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.

WireGuard Server mode

The microwall provides a WireGuard server on the LAN side, on which registered VPN clients can connect and get secure access to participants of the island network. All connections to the island network must be explicitly allowed via a whitelist-based firewall.

Application example

External WireGuard clients under Windows, Linux, Android or IOS build up a VPN tunnel to the Microwall in order to connect to participants of the island network, e.g. for remote maintenance.

7.2 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.

MicrowallVPN-08B7B2 / [VPN settings](#) / VPN environment

LOG-OUT 

VPN environment

VPN server

Activate VPN

VPN server settings

enable

VPN server public key
h0qf/kNvgEsMr8gWF09ah+QqbzS0SXbkJAEefXAVdm0=

NEW KEY

Virtual IP/subnet *
10.3.3.1/16

UDP listen port *
10001

Wireguard version
1.0.20200401


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.

Activated Clients

VPN clients

Enable clients	
<input checked="" type="checkbox"/>	10.3.3.2 (Clt-10) 
<input checked="" type="checkbox"/>	10.3.3.3 (Clt-20) 
<input type="checkbox"/>	10.3.3.5 (Clt-30) 

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.

7.3 VPN client inventory

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





MicrowallVPN-08B7B2 / VPN settings / Client inventory


LOG-OUT 

Client inventory

VPN clients



<input type="checkbox"/>	Virtual IP address	Name Description		In use
<input type="checkbox"/>	10.3.3.2  Client is active	Clt-10	1	 
<input type="checkbox"/>	10.3.3.3  Client is active	Clt-20	2	 

 *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.*

7.3.1 New VPN clients - Standard configuration

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

Add VPN client

Virtual IP address/subnet of the VPN server: 10.10.10.10/24

Virtual IP address (of the VPN client) *

10.3.3.11 i

Warning: The specified virtual IP address does not match the subnet of the VPN server.

Name *

Clt-55

Description

Public key i

Site-to-site IP range i

Pre shared key (PSK) i

 GENERATE PSK

Enable access to this web configuration interface

Enabled VPN client i

Advanced configuration

ADD CANCEL

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.

Site-to-site IP range

If the VPN client is to be used for a site-to-site connection to another Microwall, the Net-ID of the client island must be specified here.

Client configuration – Pre-shared Key (PSK)

The PSK additionally encrypts the VPN communication. The PSK must be identical on the VPN client and the VPN server. Like the public/private key, the syntax of the PSK is WireGuard-specific and cannot be freely selected. It is usually generated on the VPN server or on a third-party system using the WireGuard tools.

Option: Enable access to this web configuration interface


Activating this option allows the VPN client to access the configuration pages of the Microwall.

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.

7.3.2 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 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 Micro-wall 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.

7.4 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.

7.5 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.

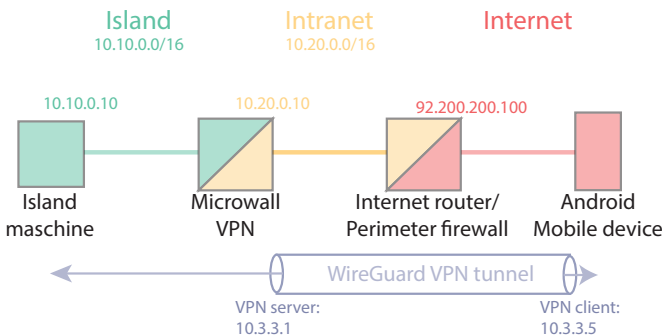
The example assumes that the Microwall is already set up as a NAT router between the intranet at *Network 1* (yellow) and the network island at *Network 2* (green).

1. Preparations

Android WireGuard APP - This must be installed on the Android mobile device. To do this, enter „Wireguard“ in the Play-store 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 intra-net-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*:


MicrowallVPN-08B7B2 / VPN settings / VPN environment

LOG-OUT 

VPN environment

VPN server

Activate VPN	1  <input checked="" type="checkbox"/> enable
VPN server settings	2  VPN server public key h0qf/kNvgEsMr8gWF09ah+QqbzS0SXBUAEefXAVdm0= <input type="text" value="NEW KEY"/>
	3 Virtual IP/subnet * 10.3.3.1/16
	4 UDP listen port * 10001
	Wireguard version 1.0.20200401

- 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.

Add VPN client

Virtual IP address/subnet of the VPN server: 10.3.3.1/16

Virtual IP address (of the VPN client) *	①	i
10.3.3.5		
Name *	②	
Android Service 1		
Description		
Public key		i
Site-to-site IP range		i
Pre shared key (PSK)	<input type="button" value="GENERATE PSK"/>	i
<input checked="" type="checkbox"/> Enable access to this web configuration interface		
<input checked="" type="checkbox"/> Enabled VPN client	③	i
<input checked="" type="checkbox"/> Advanced configuration	④	

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

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

Advanced configuration

You can generate a private/public key pair here and thus generate a complete configuration file or QR code to directly import those information into a Wireguard client (Windows, Android, iOS).

Especially the private key must not fall into the wrong hands!

Please use this variant only if you can transfer the configuration file to your end device in a secure way.

Private key * 5
 kFMcMjODLIW7qQQQibHa4GtiAOmq9nif91Kt GENERATE KEYS i

Endpoint (VPN server) 6
 92.200.200.100:10001 i

Allowed IPs 7
 10.3.3.1/32, 10.10.0.0/16 i


Keep-alive 8
 20 i


9 DOWNLOAD CONFIG FILE SHOW QR CODE

10 ADD CANCEL


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.

 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.

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

 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.

 *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.
- 8 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`

8 Wireguard VPN client

- Configuration of the microwall as VPN client

8.1 Overview WireGuard VPN-Client

WireGuard is a VPN architecture whose focus is not only on high security requirements through modern cryptography but also on 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.


<https://www.wireguard.com>

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.

WireGuard client mode

As an alternative to server mode, the Microwall can also be operated as a WireGuard client on the Network 1 port. It establishes the VPN tunnel to a WireGuard VPN server.

 *The Microwall VPN does not have its own firewall for access to the island network in VPN client mode. Access restrictions may have to be implemented on the VPN server side.*

Application example

The microwall insulates an internal machine or plant network. In case of service or maintenance, the microwall should establish a VPN connection to the manufacturer.

8.2 VPN client

The VPN Client menu branch contains the basic settings of the VPN Client mode.

[MicrowallVPN-08F142](#) / VPN client

Configure the VPN client of the microwall here.

Enable client	<input checked="" type="checkbox"/> enable
	[Status Tunnel]
Client settings	<p>Public key (VPN client) 5VN/B3v66PnHQFmyVJS2jjNkNFVxW+JbjznMnk/zAms= <input type="text" value="NEW KEY"/></p> <p>Virtual client IP address (CIDR) *</p> <p>VPN server IP address/hostname *</p> <p>VPN server UDP port *</p> <p>VPN server public key *</p> <p>Allowed IPs *</p> <p>Keep alive * 20</p> <p>Pre shared key (PSK)</p> <p><input checked="" type="checkbox"/> Allow access to the WBM via the VPN connection</p>
Import configuration	<input type="text" value="UPLOAD"/>
Configuration template	<input type="text" value="DOWNLOAD"/>

Enable client

The checkbox activates the VPN connection to the WireGuard VPN server with the specified parameters.

If the VPN tunnel is activated, the line below the checkbox contains the current status and the amount of transferred data. Due to the connectionless UDP protocol used by WireGuard, the update of the tunnel status can be delayed up to about 3 minutes.

Client settings → New Key

The button *New Key* generates a new key pair for the client mode of the Mircrowall. The displayed public key is required for the configuration of the VPN server and must be communicated to it.

Client settings → Virtual client IP address (CIDR)

The virtual IP address of the client within the VPN environment. Usually you will receive this address from the operator of the VPN server and must enter it here.

Client settings → VPN server IP address/hostname

IP address/host name under which the WireGuard VPN server is reached. Usually you will receive this address from the operator of the VPN server and must enter it here.

Client settings → VPN server UDP port

UDP port number under which the WireGuard VPN server can be reached. Usually you will receive the port number from the operator of the VPN server and must enter it here.

Client settings → VPN server public key

Public key of the WireGuard VPN server. You will receive it from the operator of the VPN server and must enter it here.

Client settings → Allowed IPs

List of IP addresses or address ranges (CIDR notation) that are allowed within the VPN tunnel. The microwall VPN automatically enters the virtual IP address of the VPN server, the Net-ID of the island network (see Basic settings → Network) and the Net-ID of the LAN on the VPN server side.

Client settings → Keep-Alive

At the interval in seconds configured here, keep alive packets are sent from the VPN client to the VPN server to keep the UDP channel required for the VPN open. The cycle time for Keep-Alive packets also influences the update of the tunnel status, so we recommend a value of 20s.

Client settings → Pre-shared Key (PSK)

The PSK additionally encrypts the VPN communication. The PSK must be identical on the VPN client and the VPN server. Like the public/private key, the syntax of the PSK is WireGuard-specific and cannot be freely selected. It is usually generated on the VPN server or on a third-party system using the WireGuard tools.

Client settings → Access to WBM via the VPN connection


Activating this option allows access to the web-based management of the Microwall through the tunnel connection.

Import configuration

The entire configuration of the VPN client including the private key can also be generated externally in a config file and loaded into the microwall VPN.

Configuration template

A configuration template can be downloaded, which can be used to configure the VPN client externally. Configuration files created in this way can be loaded into the Microwall by clicking on the Import configuration button.

 *The Microwall VPN does not have its own firewall for access to the island network in VPN client mode. Access restrictions may have to be implemented on the VPN server side.*

9 Wireguard-VPN Box-to-Box

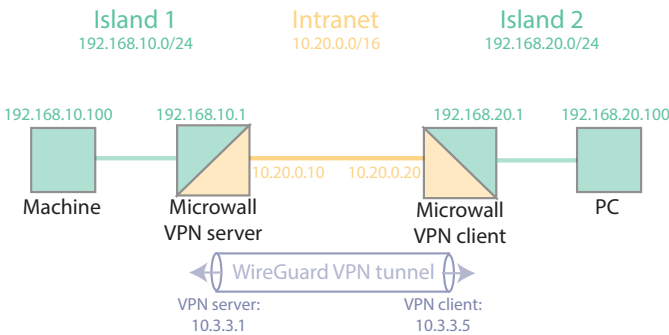
- VPN tunnels between island networks
- Configuring the server Microwall
- Configuring the client Microwall

9.1 Overview WireGuard VPN Box-to-Box

In the Box-to-Box operating mode, a WireGuard tunnel is established between two microwalls, through which the island networks communicate in an encrypted and authenticated manner.

In Box-to-Box-VPN, one microwall operates as a VPN server to which other microwalls configured as VPN clients connect.

9.1.1 Configuration example VPN Box-to-Box



Requirements

The microwalls are preconfigured with the addresses shown in the sketch and can be reached via browser from the intranet. The local microwall is set as the gateway in the network participants of the island networks.

i In this example, the configuration file for the VPN client is created on the VPN server microwall. This file contains the client's private key and any preshared key used and must be kept confidential. For critical applications, it is recommended to perform the client configuration manually via the web interface. In this case, the private key cannot be read.

i If you use IP ranges other than those used here, note that all networks must have different Net IDs.

1. Basic settings & key exchange VPN server

In a browser, open the website of the Microwall working as a VPN server and log in.

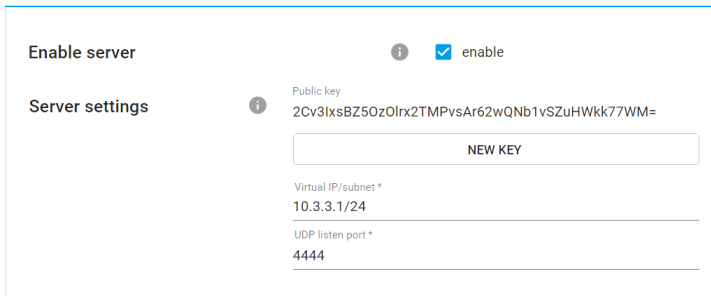
Navigate to the page

VPN server → VPN environment

Make the following settings and copy the displayed public key to paste it into the configuration of the VPN client later:

VPN environment

VPN server



Enable server enable

Server settings

Public key
2Cv3lxsBZ5OzOlrX2TMPvsAr62wQNb1vSZuHWkk77WM=

Virtual IP/subnet*
10.3.3.1/24

UDP listen port*
4444

Save the changes by clicking 

2. Basic settings & key exchange VPN client

In a browser, open the website of the Microwall working as a VPN client and log in.

Navigate to the page

VPN client

To add a new VPN client, click on  and make the following settings: To generate the keys, click the corresponding button next to the input fields.

Add VPN client

Virtual IP address/subnet of the VPN server: 10.3.3.1/24

Virtual IP address (of the VPN client) *

10.3.3.5



Name *

Client 1

Description

Public key *

LDmqxYwkUe6jlxT1cl9+pGhQo00Xzi8V+RxTqi68Lic=



Site-to-site IP range

192.168.20.0/24



Pre shared key (PSK)

ujnc0AtFctlahlqSYnsWJoPN7UNjC5Zvo+KWC

GENERATE PSK



Enable access to this web configuration interface

Enabled VPN client



Advanced configuration

You can generate a private/public key pair here and thus generate a complete configuration file or QR code to directly import those information into a Wireguard client (Windows, Android, iOS).

Especially the private key must not fall into the wrong hands!

Please use this variant only if you can transfer the configuration file to your end device in a secure way.

Private key *

OGGs12+841fMdGsuKP70mqtBs8u6lNc/QjP

GENERATE KEYS



Endpoint (VPN server)

10.20.0.10:4444



Allowed IPs

192.168.10.0/24



Keep-alive

20



DOWNLOAD CONFIG FILE

SHOW QR CODE



ADD CANCEL

Download the configuration file via the corresponding button and save it. This file contains the private key of the client as well as the preshared key, if used, and must be kept confidential.

Click on *Add* to return to the inventory overview.

Client inventory

VPN clients +

<input type="checkbox"/>	Virtual IP address ^{HF}	Name Description	In use	
<input type="checkbox"/>	10.3.3.5	Client 1	0	 

Save the changes by clicking  .

3. Basic settings VPN client

In a browser, open the website of the Microwall working as a VPN client and log in.

Navigate to the page



VPN client

Under *Import configuration*, click the *Upload* button and send the configuration file generated on the VPN server to the VPN client.

All input fields will be filled in automatically and you only need to click the *Activate Client* option.

VPN client

Configure the VPN client of the microwall here.

Enable client	 <input checked="" type="checkbox"/> enable
	Recently active (5.4 KB received, 21.9 KB sent). VPN tunnel state: open
Client settings	 Public key (VPN client) p6fdMUWYmS3EeXdPBUBGdeyR5bk67pSUMOhW0EILhCE=
	<input type="button" value="NEW KEY"/>
	Virtual client IP address (CIDR) * 10.3.3.5/24
	VPN server IP address/hostname * 10.20.0.10
	VPN server UDP port * 4444
	VPN server public key * xBt1GNTxCvDTxnFz0sVHWtHolmL6W6Ok6N0zszKH3EE=
	Allowed IPs * 192.168.10.0/24
	Keep alive * 20
	Pre shared key (PSK) QJpl94auyji13xDVoSZui7cc+/DpUL2wJijm7HQEV/U=

Save the changes by clicking  .

The configuration of the VPN client is now complete.

The VPN tunnel is now established and both sent and received data are displayed in the status after a few seconds.

Switch to the web page with the configuration session of the VPN server and navigate to the page

4. Configuration of the static routes

The island network of the respective opposite side must be made known to both the VPN server and the VPN client in the form of a static route.

In the VPN server and VPN client, navigate to the pages

Basic settings → Network

Under Static Routes click on  and make the following settings:

VPN server:

Add route

Net ID *

192.168.20.0

Subnet mask *

255.255.255.0

Gateway *

10.3.3.1

HINZUFÜGEN ABBRECHEN

VPN client:

Add route

Net ID *

192.168.10.0

Subnet mask *

255.255.255.0

Gateway *

10.3.3.5

ADD CANCEL

In the VPN server and VPN client, save the changes by clicking



5. Creating the whitelist rule in the VPN server

All communication connections between the two island networks must be explicitly permitted in the VPN firewall in the form of a corresponding rule.

In the VPN server, navigate to the page

VPN server → *VPN rules*

Click on  in the rules overview and make the following settings:

Rule settings

Name*
PC to Machine

Description

Network "Network 1" (VPN)

Source IP address(es) / VPN client | name *

IP address(es) *
192.168.20.100

Source port range(s) *
ANY

Protocol

TCP FTP

UDP

Label

Choose label(s)...

Network "Network 2 (Island)"

Destination IP address(es) | name *

192.168.10.100 | Machine Island 1

Destination port range(s) *
443

Name *
Machine Island 1

Destination port range(s) *
443

Actions

Activate rule

Create log entry


Accept connection

ADD CANCEL

Choose direction

→
 ←

This rule allows an incoming TCP connection from 192.168.20.100 to the machine 192.168.10.100 connected in the island network on port TCP/443 at the VPN server via the VPN.

Click on *Add* and in the rule overview on  to save and activate the rule.

10 Digital inputs and outputs (only Microwall IO)

- Wiring of the inputs/outputs
- Functions of the digital inputs
- Functions of the digital outputs

The following chapter is exclusively valid for the Microwall IO and its digital inputs and outputs.

10.1 Digital inputs

The Microwall IO has 2 screw terminal accessible digital inputs with the following electrical properties:

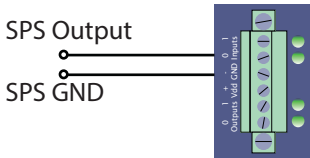
- Permissible input voltage -30VDC - +30VDC
- Switching threshold 8V +/-1,5V
- Current drawing (current ON approx. 2,2 mA)

The current status of the inputs is indicated by two associated LEDs.

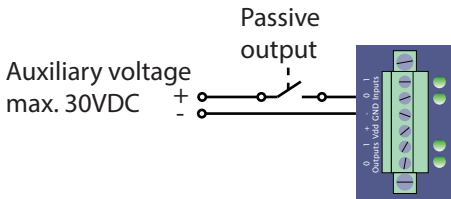
10.1.1 Wiring of the digital inputs

Both inputs are current drawing and must be assigned with active outputs, which must supply at least 2.2mA current.

Example: Connection of active PLC output



Example: Connection of potential-free output/switch



10.1.2 Available actions of the digital inputs

The assignment of the actions to be executed in the event of a status change of the input signal is made in the WBM menu branch *I/O events*. The events are differentiated according to rising and falling edge. Several actions can be assigned to each event.

The following actions are available:

- Activation/deactivation of the VPN tunnel as client or server
- Activation/deactivation of the network interface
- Activation/deactivation of firewall rules with specific labels

10.2 Digital outputs

The Microwall IO has 2 screw terminal accessible digital outputs with the following electrical properties:

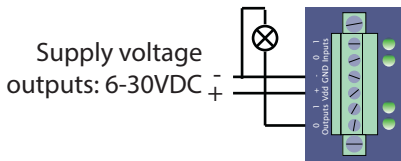
- Separate output voltage 6-30VDC
- max. current 500mA/output, short-circuit protected

The current status of the outputs is indicated by two associated LEDs.

10.2.1 Wiring of the digital outputs

The outputs have a separate supply voltage and switch through the voltage applied to the *Vdd* terminal in the ON status.

Example wiring output



10.2.2 Available actions of the digital outputs

The assignment of which internal event of the Microwall switches which output is made in the WBM menu branch I/O events. Events can switch an output on, off or toggle it.

The following triggering events are currently available:.

- Active/deactive VPN tunnel (client or server)
- Active/deactive configuration session WBM
- Active/deactive emergency access

11 Security & Maintenance

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

11.1 Security notes

The following sections contain information and recommendations relevant from an IT security perspective for commissioning, configuring, operating and maintaining the Microwall.

11.1.1 Function and typical use

The Microwall is a strictly whitelist-based small firewall designed as an IPv4 router with two Ethernet ports and an integrated WireGuard VPN access, which can be used either as a client (outgoing) or as a server (incoming).

The typical application is to logically decouple a network island from a higher-level intranet. It thus supports the operator in segmenting the network as a basic measure of many IT security concepts. The intranet side of the microwall (*Network 1, yellow*) can be connected to the Internet via additional routers and perimeter firewalls. From the perspective of a defense-in-depth strategy, the microwall is therefore always deployed behind at least one perimeter firewall and outside a DMZ.

For the purpose of remote maintenance, the Microwall has a WireGuard VPN endpoint on the intranet side (*Network 1, yellow*). As a client or server, this enables encrypted, authenticated remote access to subscribers in the island network, which is protected by its own firewall. Cross-access to the intranet at the Network 1 port via the VPN is not possible.

11.1.2 Requirements for integrators and operators

The factory settings of the Microwall are oriented towards a universal and preferably barrier-free initial start-up in an intranet.

Depending on the individual network environment and the security requirements, these specifications must be checked for operational use. Changes and/or additional measures may be required by the integrator or operator. These include in particular:

- Choice of a secure password in terms of length and composition
- Deactivation of unneeded services or limitation of their availability to the required network interface
- Firewall rules formulated as narrowly as possible (e.g., avoidance of Any/Any shares)
- Installation of an individual device certificate within a PKI environment
- Secure management of WireGuard communication partners and secure handling of associated keys.
- Protection of the Microwall against unauthorized physical access

Further details can be found in the following of this chapter as well as in the preceding function-specific chapters of this manual.

11.1.3 Installation location

The installation location of the Microwall must ensure that no unauthorized physical access can occur (e.g., suitably secured room, network cabinet, etc.). Physical access to the Microwall involves 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 of the Microwall emergency access via the service button and thus deactivation or change of the password. An attacker gains full access to the management interface and is able, for example, to create firewall rules or create unauthorized VPN clients.

11.1.4 Commissioning

The commissioning of a Microwall is divided into the assignment of an IP address via DHCP or with the tool WuTility and the subsequent call of the initial web page. This is where the

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

IP assignment

During initial commissioning, ensure that there is no unauthorized access to the Microwall until the password has been assigned on the initial web page. A suitable measure is, for example, to perform the commissioning via a point-to-point connection with the configuring computer. Only then is the Microwall connected to the actual target networks.

Password

Operational use of the Microwall without a password is not possible. The password is the central protection against unauthorized access to the configuration and management of the Microwall. We recommend using a secure password with a length of at least 15 characters, consisting of upper and lower case letters, digits and special characters.

Registration for security-related information

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

11.1.5 Operation and configuration

Individuelles Geräte-Zertifikat

Web-based management can only be accessed in encrypted form via HTTPS. A device-specific, 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 your own individual certificate to protect against man-in-the-middle attacks.

Deactivation of services not required

The Microwall supports the following incoming and outgoing services:

Portno.	Service	Pass-word?	Configurable/can be deactivated?
Incoming:			
443 (TCP)	HTTPS management Default: activated/Network1	yes	yes/yes
8513 (UDP)	Inventory WuTility Default: activated/Network1	no	no/yes
5555 (TCP)	Firmw. update WuTility Default: activated/Network 1	yes	no/yes
446 (TCP)	HTTPS emergency access Default: deactivated, (Manual activation via service button)	no	no/yes
161 (UDP)	SNMP Default: deactivated (Activation via Web-Management, read-only)	yes (SNMPv3)	yes/yes
ICMP	Echo request Default: deactivated	-	no/yes
Outgoing:			
123 (UDP)	NTP timeserver Default: deactivated	-	no/yes
53 (UDP)	DNS client Default: deactivated (Activation automatically on demand)	-	no/no
514 (UDP)	Syslog client Default: deactivated	-	yes/yes
67 (UDP)	DHCP client Default: activated (Deactivation by static IP)	-	no/yes

Configuration and activation/deactivation of outgoing services are 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 can be useful to partially or completely deactivate these services after setting up the communication rules during operation. If changes are required later, HTTPS access can be reactivated as needed at any time via the emergency access accessible via service button (see section Emergency access via service button).

Formulation of the whitelist rules

The Microwall does not have any release rules except works for communication between the two network ports or for a VPN client. When formulating rules, we recommend formulating them as narrowly as possible according to the need-to-know principle. For example, using a unicast address provides greater security than an IP range.

Confidentiality of Private Keys

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

When setting up WireGuard VPN clients, there is an optional option for ease of use to have the Microwall generate the key pair of the new client. Only choose this path if you can guarantee 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 transferring the non-critical public key to the Microwall by other means.

11.1.6 Service, maintenance and decommissioning

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
- If necessary, provision of a replacement device
- Documentation of the procedure for device replacement

During decommissioning, all confidential information stored in the Microwall (IP ranges, sharing rules, VPN accesses, etc.) should be reset to the factory settings to protect them. This can be done either via the web-based management or the service button.


11.2 Up-/Download Configuration data

On the web page Maintenance there is a possibility to backup the current configuration of the Microwall or to restore a previously downloaded backup file.

Configuration or backup files contain operational parameters (firewall/VPN rules, VPN keys, inventory lists, etc.) as well as data relevant for administrative access to the microwall (IP parameters, system password, certificate, etc.). Backup files are encrypted for this reason and cannot be edited. For extended protection, we recommend additionally providing the file with an individual backup password. This must then be known for a later upload to another microwall.

Download configuration

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


 *The upload of a password-provided backup file is only possible with knowledge of this password. 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 website during 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 transferred and the Microwall works with the new parameters after an automatic restart.

 *Backup files also contain the new IP address of the Microwall. To avoid an IP conflict, make sure that the original*

or a previously programmed Microwall are no longer connected to the network before uploading.

11.3 Firmware updates

W&T publishes firmware updates for the Microwall in order to eliminate functional errors, possibly discovered vulnerabilities or also to extend functions. The upload to the device is carried out either with the help of the WuTility management tool or via the Microwall's web-based management.

To protect against manipulation of the firmware files and thus possible compromise of the devices, all update files for the Microwall are encrypted and signed by W&T.

Update files always contain the entire firmware or the entire system of the Microwall. For this reason, firmware updates are always associated with a restart of the Microwall and thus also an interruption of the operational mode. Individual configuration data (IP parameters, firewall rules, etc.) are not affected by a firmware update and remain intact.

11.3.1 Where is the latest firmware available?

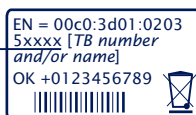
The latest firmware including the available update tools and a revision list is published on our website at the following address

<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.

Type number




On the Microwall 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.

11.3.2 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. With the factory settings, the update with WuTility is only possible via the interface Network 1.

Web access

 enable

Enable access from:


Network 1

Network 2 (Island)

HTTPS port *

443

WuTility management


 enable (UDP/8513)

Enable access from:

Network 1

Network 2 (Island)


Firmware update

 enable (TCP/5555)

Enable access from:

Network 1

Network 2 (Island)

 *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, 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 decrypts the firmware file, checks the signature and writes the firmware to its internal flash. Finally, a restart is performed automatically and the Microwall is ready for operation again.





11.3.3 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 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.

Maintenance

Trigger restarts and other maintenance tasks from here.

Restart		<input type="button" value="REBOOT DEVICE"/>
Restore		<input type="button" value="FACTORY DEFAULTS"/>
Service button features		<input checked="" type="checkbox"/> HTTPS emergency access <input checked="" type="checkbox"/> Reset to factory defaults
Firmware update		<input type="button" value="UPLOAD FILE"/> <small>No file uploaded (yet)... Current firmware revision: 1.06</small> <input type="button" value="INSTALL UPDATE"/> <input type="button" value="DISCARD UPLOAD"/>
Configuration backup		<small>Backup password</small> <input type="button" value="UPLOAD CONFIGURATION"/> <input type="button" value="DOWNLOAD CONFIGURATION"/>

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.

11.4 Individual certificates

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

The Microwall'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
- Download the CSR and external signature to a certificate by a trusted certificate authority.
- Upload and installation of the certificate into the Microwall

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 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 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 using the corresponding upload buttons. All files must be in PEM format.

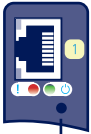
After a formal check, the certificate is integrated into the system by clicking on *Install* under *Externally signed certificate* and used for all web accesses.

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.

11.5 Emergency access to the Microwall

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.

i *The emergency access activates a non-password-protected web page on the Microwall 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 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.

11.6 Reset to default settings

A reset to the factory settings of the Microwall 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 3.5s 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 must now be put into operation again. For more information, please refer to the chapter *Start-up*.

Appendix

- Technical data and form factor

Technical data and form factor

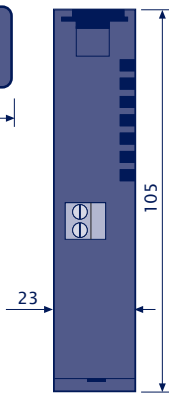
Microwall VPN, #55211

Power supply ...	
Power-over-Ethernet:	37-57V DC from PSE
External power supply, screw terminal	DC 24-48V (+/-10%)
Current consumption ...	
Power-over-Ethernet:	PoE Class 2 (3,84 W - 6,49W)
Ext. supply	typ. 150mA@24V DC max. 200mA@24V DC
Galvanic isolation	Network interfaces: min 500V
LAN-Port Network 1	10/100/1000BaseT, RJ45, au- tosensing, autocrossing, PoE
LAN-Port Network 2	10/100/1000BaseT, RJ45, autosensing, autocrossing
Permissible ambient temperature ...	
... Storage	-40 ... +85°C
... Operation, non-cascaded	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

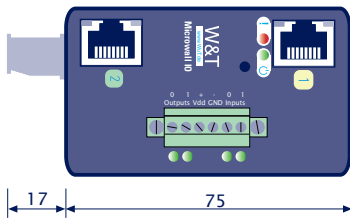


Measure in mm. +/-1 mm

Microwall IO, #55212

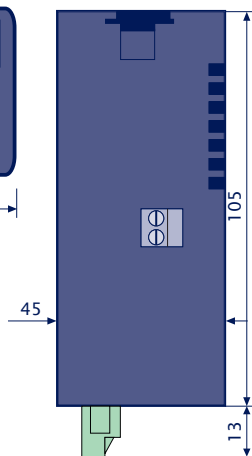
Power supply ...	
Power-over-Ethernet:	37-57V DC from PSE
External power supply, screw terminal	DC 24-48V (+/-10%)
Current consumption ...	
Power-over-Ethernet:	PoE Class 2 (3,84 W - 6,49W)
Ext. supply	typ. 150mA@24V DC max. 200mA@24V DC
Galvanic isolation	Network interfaces: min 500V
LAN-Port Network 1	10/100/1000BaseT, RJ45, au- tosensing, autocrossing, PoE
LAN-Port Network 2	10/100/1000BaseT, RJ45, autosensing, autocrossing
Digital inputs	2 x on screw terminal input voltage +/-30VDC switch threshold 8V+/-1,5V inout current min 2,2mA
Digital outputs	2 x on screw terminal 6-30VDC, 500mA/output
Permissible ambient temperature ...	
... Storage	-40 ... +85°C
... Operation, non-cascaded	0 ... +50°C
Permissible rel. humidity	0 - 95% (non-condensing)
Dimensions	105 x 75 x 45mm
Weight	ca. 180g

Front view 55212



Measure in mm, +/- 1mm

Bottom side 55212



Index**C**

certificates 106
Certificate Signing Request
106
Configuration backup 29

D

default IP address 26
DHCP 22
DHCP server 36
Digitale inputs 82, 90
Digital outputs 92
Discover-Assistent 38

E

Emergencies access 108

F

firewall rules 48
form factor 112

H

Hardware installation 14
hostnames 51

I

Initial web page 27
IP inventories 46

K

Konfigurationsdateien 100

L

Link state 17
Login 33
Logout 33

N

NAT router 40

navigation concept 32
Network Interfaces 16

P

PoE 15
Power supply 15
Preshared Key 63, 79
PSK 63, 79

R

Reset 19

S

Security 93
service button 108
Standard router 42
static NAT 44
System- and Error LED 18

V

VPN clients 60
VPN rules 65

W

Web-Based-Management 31
Wiring digital inputs 90
WuTility 23