W&T

www.WuT.de

Manual

Startup and application

Microwall Gigabit

valid for the following models:

#55210: Microwall Gigabit

Release 1.00 10/2018

© 10/2018 by Wiesemann and Theis GmbH

Microsoft, MS-DOS, Windows, Winsock and Visual Basic are registered trademarks of Microsoft Corporation.

Subject to change without notice:

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

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

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

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

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

This offer applies to every recipient of this information.

Introduction

The Microwall Gigabit is an industrial IPv4 router with two 1000BaseT network ports and integrated whitelist-based firewall. It connects a network island, e.g. with automation components, to a higher-level network. Appropriate filter rules at TCP/IP level protect both networks against unauthorized, unwanted and harmful communication.

Inhalt

1 Legal information and security 7
1.1 Legal notices 8
Warning concept 8
Qualified personnel 8
Disposal 9
Symbols on the product 9
1.2 Safety notices 10
General notices 10
Intended use 10
Electrical safety 10
EMC 11

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 Externe 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 Initial assignment of IP parameters with WuTility 22
3.2 Start-up via the default IP address 25
3.2 Initial website of start-up 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 Operation modes and rule configuration 35
5.1 Functionality of the Microwall Gigabit 36
5.2 Operating modes & changeover 37
5.2.1 Mode NAT router 37
5.2.2 Mode Standard router 37
5.2.3 Switching the operating modes 37
5.3 Rule Overviews & Labels 39
5.3.1 Label 39
5.3.2 Create and manage labels 40
5.4 Create firewall rules 41
5.5 Creating Firewall NAT Rules 47

6 Security & maintenance 53
6.1 Firmware updates 54
6.1.2 Firmware update with WuTility 54
6.1.2 Firmware update per Web-Based-Management 55
6.2 Individual Certificates 57
6.3 Deactivation of unneeded services. 60
6.4 Emergency access of the Microwall Gigabit 61
6.5 Factory settings 63

7 Appendix 65
7.1 Technical data and dimensions 66
7.2 Licenses 67
Index 74

W&T

1 Legal information and safety

1.1 Legal notices

Warning concept

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

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

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

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

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

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

Qualified personnel

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

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

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

Disposal

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

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

Symbols on the product

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

1.2 Safety notices

General notices

This manual is intended for the installer of the Web-IOs 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 from Wiesemann & Theis is an IPv4 router with two 1000BaseT network connections and integrated white-list-based firewall. It connects a network island to a higher-level network. Suitable filter rules on TCP/IP level protect both networks against unauthorized and unwanted communication.

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

Electrical safety

⚠WARNING

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

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

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

Ventilation openings must be clear of any obstacles. A distance of 10-15 cm between the Web-IO and nearby heat sourc-

es 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 Gigabit 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 Gigabit must absolutely ensure safe isolation of the low-voltage side from the supply mains according to EN60950-1 and must have “LPS“ designation.

EMC

⚠NOTE
Only shielded network cables may be used for connecting the Microwall Gigabit to the network.

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

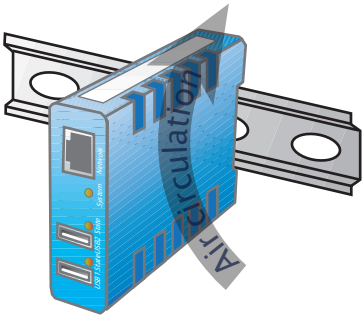
The complete Declarations of Conformity for the devices described in the manual can be found on the corresponding Internet page at the W&T homepage: http://www.wut.de.

2 Hardware, interfaces and displays

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

2.1 Hardware installation

The Microwall Gigabit is mechanically designed for mounting on a standard DIN rail. Here, as well as with possible alternative mounting types, the sketched air circulation must be ensured.



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

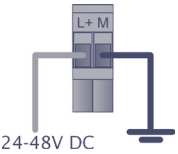
2.2.1 PoE supply

The Microwall Gigabit 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 Externe power supply

As an alternative to the PoE supply, the Microwall Gigabit can be supplied externally via the pluggable screw terminal 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

For the external supply of the Microwall Gigabit 55210 only a potential-free power supply unit may be used. 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 in accordance with EN60950-1 and must have the „LPS“ property.

2.3 Network interfaces

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

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

Commissioning with the factory settings as well as a possible supply via PoE are only possible via *Network 1* (yellow).

2.3.1 100/1000BaseT

Both LAN connections are made via shielded RJ45 sockets and max. 100m long, shielded patch cables. The autocrossing function allows both 1:1 wired and crossed patch cables to be used to connect the LAN device(s).

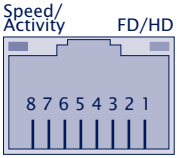
Both network connections are galvanically isolated from the supply voltage by at least 500Vrms.

Auto Negotiation: 100/1000BaseT, Full/Half Duplex
The network connections of the Microwall Gigabit both work in auto-negotiation mode. To avoid problems such as duplex mismatch, we recommend that connected devices or switches are also operated in auto-negotiation mode. Both the transmission speed and the duplex procedure are negotiated auto-

matically and set accordingly in the devices.

2.3.2 Link state

The link status for both network connections is indicated by two LEDs integrated into the RJ45 sockets.



- **Speed/Activity (green/orange)**
  Green = 1000MBit/s link
  Green blinking = 1000MBit/s link and Data traffic

  Orange = 100MBit/s Llnk
  Orange blinken = 100MBit/s link and Data traffic

- **FD/HD (yellow)**
  ON = Full-Duplex
  OFF = Half-Duplex

2.4 System and Error LED

2.4.1 System LED ⏻ (green)

ON: Indicates normal operational readiness.

Blinking: The Microwall Gigabit restarts 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.

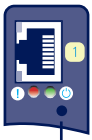
Slow blinking: The service button was pressed between 3.5s and 10s. The emergency access of the Microwall Gigabit is activated.

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

The emergency access opens a non-password-protected HTTPS access with the possibility to overwrite the current password. Therefore, start the emergency access only with caution and 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 Gigabit prepares a reset to the factory settings. If the service button is still pressed, a reset to the factory settings takes place after a total of 20s.

2.5 Service button



t

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

The service button triggers the following actions:

Reset/Restart
A short push of the button between 0.2 and 3.5s triggers a simple restart of the Microwall Gigabit.

Start Emergency Access
After pressing the button for more than 3.5s, the error LED starts flashing slowly. If the button is released during the slow flashing and before 10s have elapsed, the emergency access of the Microwall Gigabit is activated on both network connections via TCP port 446. Pressing it briefly again performs a reset and terminates the emergency access.

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

The emergency access opens a non-password-protected HTTPS access on TCP port 446 with the possibility to overwrite the current password. Start the emergency access only with caution and in a 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 setting after 20 seconds. If the service button is released while the service LED is flashing rapidly (time window 10-20s), the factory default reset is

aborted and the microwall continues with standard operation according to the current configuration.

By resetting to the factory settings, all settings made (filter rules, IP parameters, log files ...) are lost. The re-commissioning must be carried out as described in the chapter Commissioning.

3 Start-up

The Microwall can only be commissioned via the *Network 1* interface (yellow). In the first step, the IP address required for initial access is assigned to the Microwall Gigabit. During the subsequent first browser access, the other basic parameters required for operation, such as the system password, are then configured.

- Setting the IP address with the *WuTility* management tool
- Changing IP Parameters using Web-Based Management
- First access via browser

3.1 Initial assignment of IP parameters with WuTility

Starting with version 4.52, the Windows tool *WuTility* supports the inventory and management of the basic network parameters of the Microwall Gigabit. Older WuTility versions < 4.52 cannot be used.

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

When the Network 1 *interface is connected to the network, the initial website for assigning the system password can be accessed via the default IP address or the IP address assigned via WuTility. Therefore make sure that no unauthorized access to the Microwall Gigabit takes place during the period up to the password assignment on the initial website (e.g. by commissioning with a direct connection to the respective PC).*

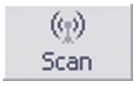
To assign the IP address, the PC and the Interface *Network 1* of the Microwall Gigabit must be located in the same physical network.

Installation with WuTility
The quickest way to install is to click the Install button on the start page of the product CD included in the scope of delivery.

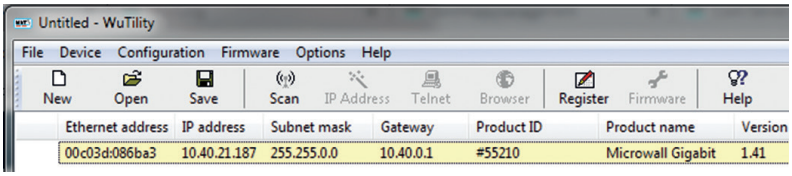
Then start WuTility via

Start → Programs → Wutility Version 4 → WuTility

Start of the allocation dialog
Make sure that the Interface *Network 1* of the Microwall Gigabit and the computer used are connected to the same physical network. At startup, *WuTility* automatically searches the local network for connected W&T network devices and creates an inventory list. This search process can be repeated manually as often as desired by pressing the *Scan* button:

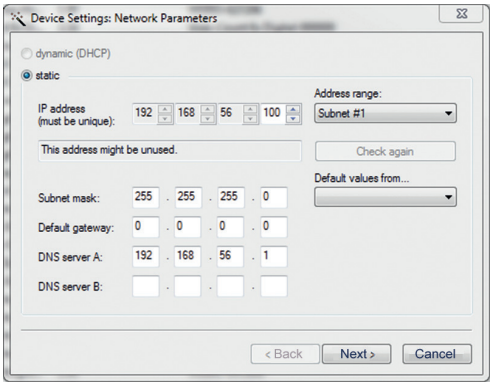


Within the inventory list you can identify the desired Microwall Gigabit by its MAC address. The factory default IP address is 190.107.233.110.



Select the desired Microwall Gigabit and press the *IP address* button:

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



By pressing the button Next, the network parameters of the Microwall Gigabit are stored non-volatile.

The IP assignment with WuTility can be repeated until the Microwall Gigabit has received a system password via the initial website. Afterwards, the IP parameters can only be changed via the standard web-based management.

The additional parameters required for the initial commissioning are carried out via an initial website with the help of a browser. Information on this can be found in the chapter *Initial Website of start-up*.

3.2 Start-up via the default IP address

The default IP address of the interface *Network 1* is 190.107.233.110 when delivered and after a reset to the factory settings.

When the Network 1 interface is connected to the network, the initial website for assigning the system password can be accessed via the default IP address or the IP address assigned via WuTility. Therefore make sure that no unauthorized access to the Microwall Gigabit takes place during the period up to the password assignment on the initial website (e.g. by commissioning with a direct connection to the respective PC).

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

On the computer side, one of the following two prerequisites must be fulfilled:

- The IP address of the computer used is in the subnet range 190.107.233.0 or is temporarily changed to a suitable value. You need administrator rights to change the IP address of the computer. Clarify such a change in advance with the responsible network administrator.

- The computer used temporarily receives a fixed route which redirects the IP address 190.107.233.110 to the local network. Administrator rights are required to set up such a route. The command line syntax for creating a fixed route under Windows is as follows:

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

The further parameters required for the initial commissioning are then carried out via an initial website with the help of a

browser. Information on this can be found in the chapter *Initial Website of start-up*.

3.2 Initial website of start-up

The initial website is only available during initial operation and after a reset to factory settings. It primarily serves to configure the password for further full access to the web-based management of the microwall. At the same time it is possible to determine the IP basic parameters of the two network interfaces and the operating mode.

Network connections between the two networks of the microwall are not yet allowed to assign the parameters available here. Communication releases must be explicitly released later in the form of whitelist rules for the selected operating mode.

When the Network 1 *interface (yellow) is connected to the network, the initial website for assigning the system password can be reached via the default IP address or the IP address assigned via WuTility. Therefore make sure that no unauthorized access to the Microwall Gigabit takes place during the period up to the password assignment on the initial website (e.g. by commissioning with a direct connection to the respective PC).*

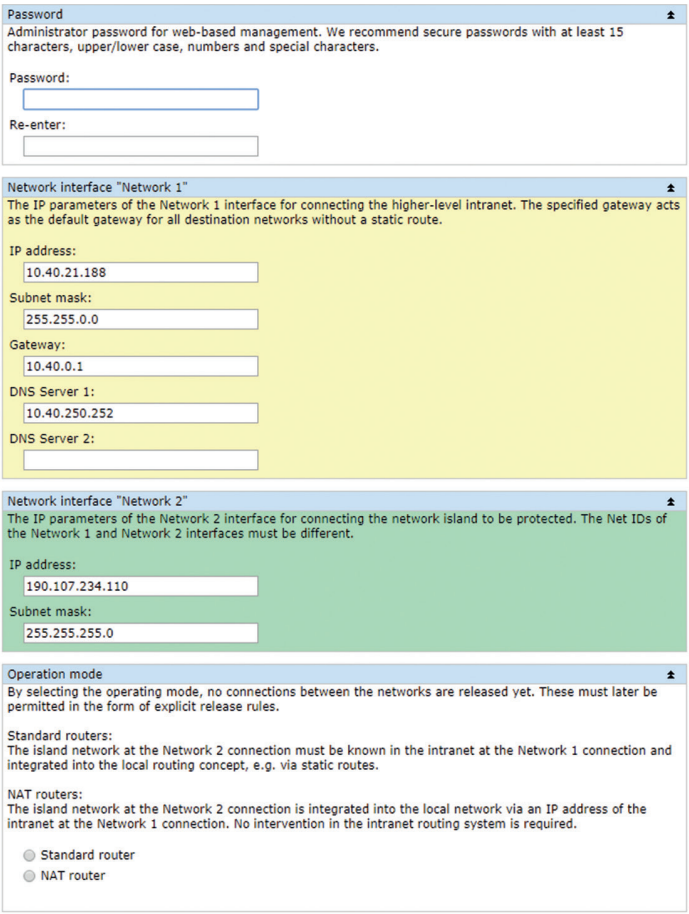
If the IP address was assigned using the WuTility tool, select the desired Microwall Gigabit and click the *Browser* button:

If the access is to take place via the default IP address of the Microwall Gigabit, start a browser on the PC prepared from the 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 from the browser used must be ignored and/or acknowledged during initial commissioning. After commissioning, the default certificate can be replaced by your own individual certificate via Web-based management.

All settings made here can be changed later using the Standard Web-Based Management.



Password (mandatory)
Enter the password for access to the Web Base Management of the Microwall Gigabit. We recommend passwords with a minimum length of 15 characters, consisting of upper and lower case letters, numbers and special characters. The maximum password length is 51 characters.

Operation without a password is not possible.

There is no default or master password. A lost password can only be reset with physical access to the device and the emergency access, which can be activated via the service button, or with a reset to the factory settings.

Network 1 (yellow)
If the browser access was done via the default IP of the Microwall Gigabit, now enter the values valid for your application here.

The specification of DNS servers is only necessary if the time server(s) for the NTP client of the Microwall Gigabit are configured in the form of a host name.

Network 2 (green)
Enter the IP address and subnet mask for the *Network 2* interface of the Microwall Gigabit. The Net-IDs of *Network 1* and *Network 2* must be different.

If there are additional routers in remote networks in Network 2, these can later be configured in the network settings of Web-Based Management in the form of static routes.

Operation mode (mandatory)
Select the desired operating mode of the Microwall Gigabit. Further information can be found in the chapter *Operating Modes and Rule Configuration*.

With a click on Apply, entered parameters are saved and you are automatically redirected to the standard configuration pages of the microwall.

4 Web-Based-Management

The configuration of the Microwall Gigabit is only possible encrypted via HTTPS. The WBM (Web-Based-Management) works session-oriented, but any changes made are immediately saved and valid with the Apply button.

- Navigation within the WBM

4.1 Start and navigation concept of the WBM

To access the WBM of the Microwall Gigabit you need a current Internet browser. Session cookies and Javascript must be activated.

Access to the web pages is only possible encrypted via HTTPS. The standard port 443 is preconfigured at the factory.

Start your Internet browser and enter the IP address of the Microwall Gigabit and, if necessary, the port number to be used in the address line.

https://[IP address]:[Portno.]

4.1.1 Navigation conzept of the Microwall Gigabit

The WBM of the Microwall Gigabit works session-oriented via a password-protected login. Operation without a password is not possible. It must be assigned during initial start-up.

After login, any changes made are immediately accepted and saved non-volatile by pressing the *Apply* button on the respective page. If the transfer of the parameters requires a restart of the microwall, a corresponding message is displayed after pressing the *Apply* button.

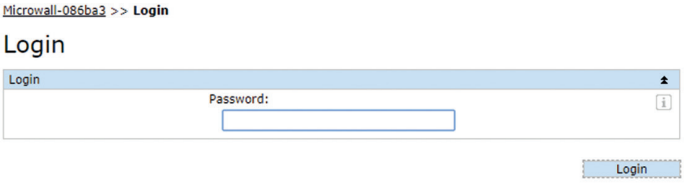
You can end a configuration session at any time by clicking the *Logout* button below the navigation tree.

4.2 Login/Logout

Settings on the Microwall Gigabit are made within password protected configuration sessions. These are exclusive, i.e. only one session can be active at a time.

The start page of the Microwall only offers the possibility to enter a password for login and to switch the interface language between German and English via the flag symbols under the menu tree.

4.2.1 Login



Enter the password of the microwall and click the *Login* button. After successful login, the extended navigation tree with all configuration options is available.

To protect against brute force attacks, the password input is protected with an escalating timeout. After each incorrect entry of the password, the new entry is only possible after a timeout that doubles with each attempt.

4.2.2 Logout

To end a configuration session, click the Logout button below the navigation tree.

4.3 Help and description texts

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

This manual contains detailed information on the operating modes and enable rules in the chapter *Operating Modes and Rule Configuration*

5 Operation modes and rule configuration

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

5.1 Functionality of the Microwall Gigabit

The Microwall Gigabit is designed as an IPv4 router with integrated whitelist firewall. It outsources network components in need of protection to a subnetwork (*Network 2*, green) and only permits communication connections to and from the higher-level network (*Network 1*, yellow) that have been explicitly approved via filter rules.

The two operating modes NAT router and standard router described below each have their own rule lists based on source/destination address, source/destination port and protocol.

5.2 Operating modes & changeover

5.2.1 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 via a public IP address.

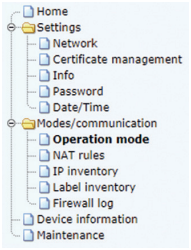
The IP addresses of the island hosts are replaced on the intranet page by the IP address of the microwall Gigabit and are therefore never visible on the intranet. The island IP range can therefore be freely selected. Several islands, each with identical IP ranges, can also be connected to the company intranet at the same time in this way. An intervention in its routing concept is not necessary.

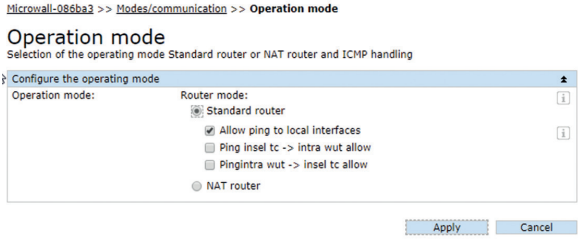
5.2.2 Mode Standard router

In standard router mode, the Gigabit microwall separates the island network at *Network 2* port (green) from the corporate intranet at *Network 1* port (yellow). However, the island network becomes an official subnet of the intranet infrastructure. The island will often be a border network in which the microwall gigabit is the only router and can therefore be entered as the standard gateway on the island hosts. On the intranet side, however, there are often other routers (e.g. WAN/DSL connection), so that the path to the island network must be made known here in the form of static routes on the participating hosts.

5.2.3 Switching the operating modes

Switching between the NAT router and standard router operating modes is done via the Operating mode link in the Web Management menu tree.





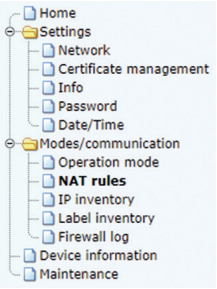
In addition to the operating mode, the handling and forwarding of ICMP requests/replies (ping) is also defined here.

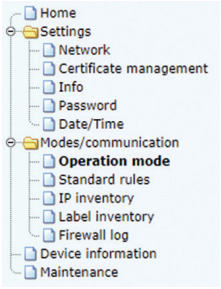
The Microwall Gigabit has two independent rule lists for each operating mode. Access is only possible to the rule list belonging to the currently active operating mode.

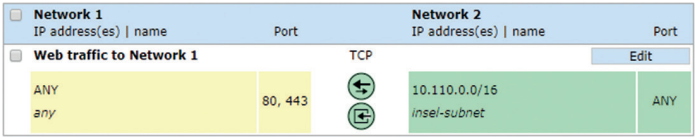
When switching the operating mode, it can be decided whether the rules of the previous mode should be deleted or saved.

5.3 Rule Overviews & Labels

Depending on the selected operating mode, the NAT Rules or Standard Rules link in the menu tree leads to the page with an overview of all created rules.







Each rule is displayed in its own overview block. This contains information about the source/destination host(s) and source/destination ports used. The direction of the rule from the connection setup point of view is represented by the large arrow of symbols and . The symbol indicates that each connection creates an entry in the log of the Microwall Gigabit according to the rule definition.

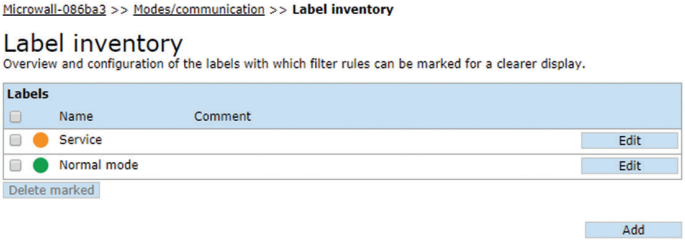
5.3.1 Label

If one or more labels are assigned to a rule during creation, they can be used as display filters in the rule overview.

If no label is activated in the filtering, all rules are displayed. As soon as one or more labels are activated, the rules overview only shows rules that contain at least one of these labels.

5.3.2 Create and manage labels

In addition to the two factory labels normal operation and maintenance, you can create your own labels via the link Label Inventory in the menu tree.



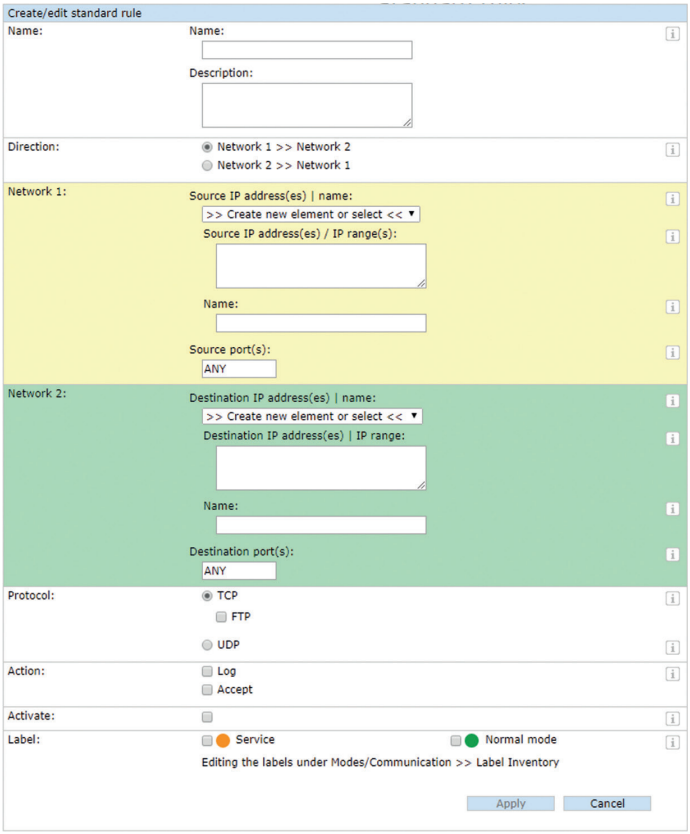
Click the Add button and assign a name, an optional description and any color.t

5.4 Create firewall rules

The creation of firewall rules for communication is largely identical for the following operating modes and connection directions:

- Mode Standard router both directions
- Mode NAT router direction *Network 2* (green) to *Network 1* (yellow)

Depending on the selected operating mode, a click on NAT router or Standard router in the menu tree starts the rule dialog.



Name

The specified individual name (mandatory field) identifies the rule in the rule overview. The optional *Description* serves exclusively for information in this dialog.

Direction

Definition of the direction for the rule from the point of view of the connection setup with TCP. With UDP, the initial UDP datagram determines the direction.

Network 1 (yellow) & Network 2 (green)

The *Destination IP address(es) | Source IP address(es)* can either be selected from the inventory lists via the select box or entered directly numerically. If a numeric value is specified, the destination/source is automatically transferred to the IP inventory with the name specified under Name.

Permissible numeric specifications of the addresses:

- *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 concatenations of IP ranges within an 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

Bei der Angabe des/der Ziel-Port(s) sind folgende Eingaben zulässig:

- *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 that „8000, 10-1000“, for example, is an invalid input.

Protocol

Specifies whether the rule applies to *TCP* or *UDP*.

The *FTP* TCP option must be enabled when formulating the rule for FTP connections. Parallel TCP connections negotiated in the protocol history are automatically allowed and blocked.

UDP is a connectionless protocol which, however, often works according to a request reply principle (e.g. DNS). In these cases the option *Allow reply in reverse direction* must be activated. The microwall automatically accepts an incoming reply datagram within a timeout.

Action

Accept allows the data traffic defined by the rule.

Log creates an entry in the log file of the microwall for each connection setup according to the rule.

Activate

Activates the rule immediately after pressing the *Apply* button.

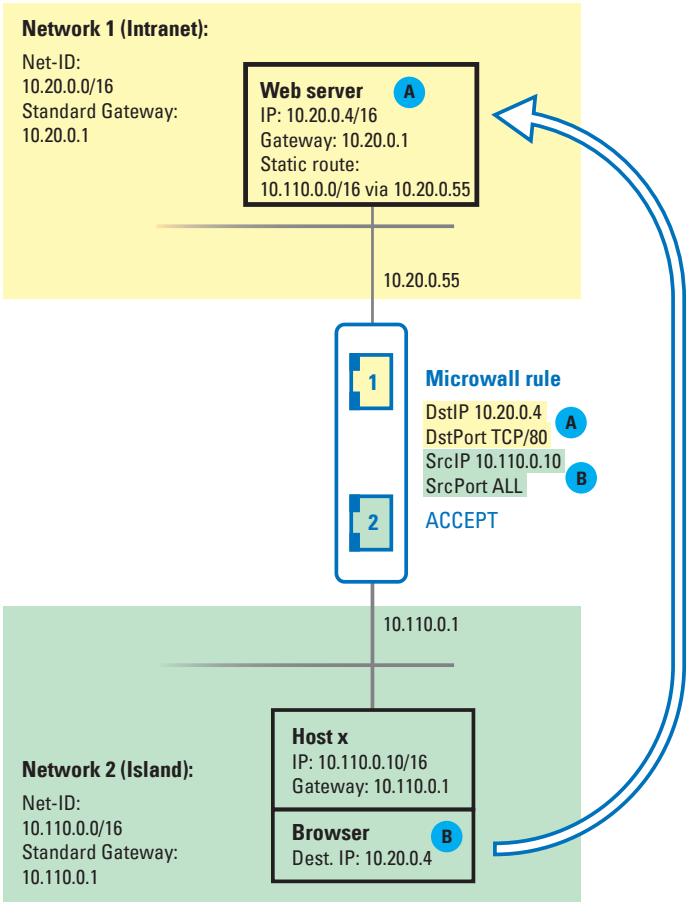
If this option is not set, pressing the *Apply* button creates the rule but does not apply it; data traffic according to the rule is not possible. The rule can be activated later in the rule overview.

Label

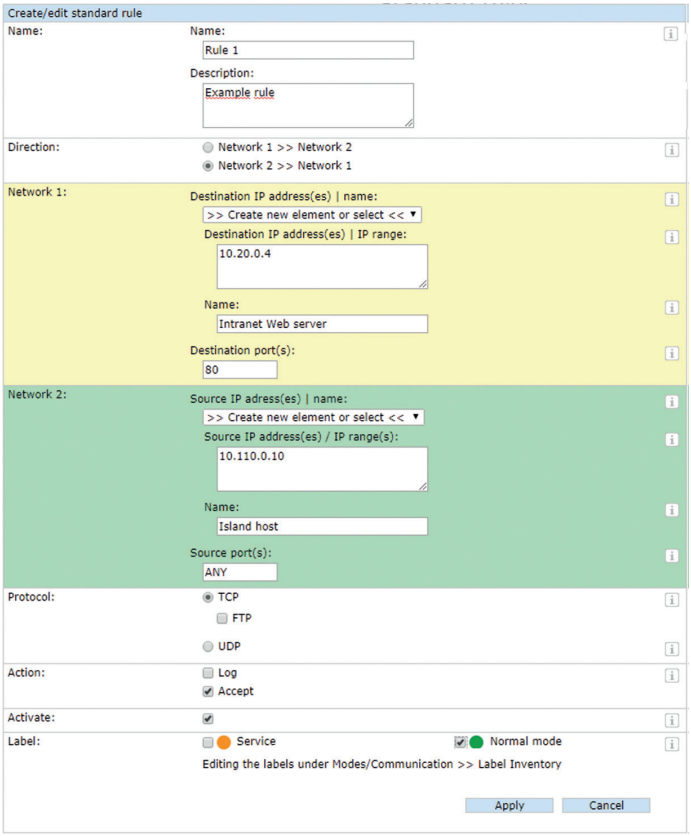
One or more labels can be assigned to the rule for a clearer display or display filtering in the rule overview. The labels *Normal mode* and *Service* are pre-installed ex works. Via the link *Label inventory* in the menu tree further labels can be created.

5.4.1 Firewall rule example

Island host (B) 10.110.0.10/16 on *Network 2* port should access the Intranet Web server (A) 10.20.0.4/16 via browser, TCP/80 on *Network 1* port. The Microwall Gigabit itself is integrated with the IPs 10.110.0.1 and 10.20.0.55 into the networks. The rule should be marked with the label *Normal mode* in the rule overview.



The rule dialog to be filled in for this example:

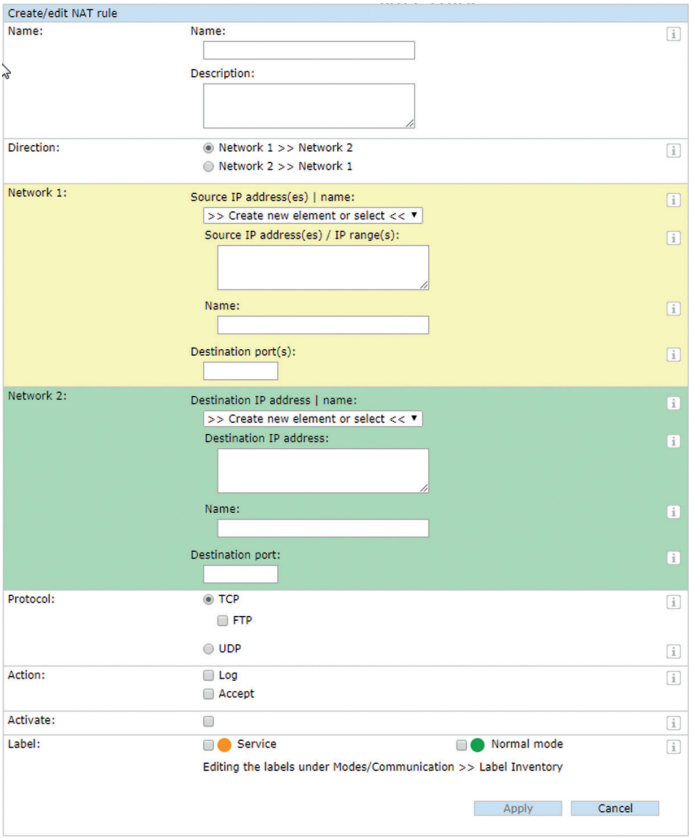


5.5 Creating Firewall NAT Rules

The creation of firewall NAT rules for communication is possible for the following operating mode and connection direction:

- Mode NAT router direction *Network 1* (yellow) to *Network 2* (green)

A click on *NAT router* in the menu tree starts the rule dialog.



Name

The specified individual *Name* (mandatory field) identifies the rule in the rule overview. The optional *Description* serves exclusively for information in this dialog.

Direction

Firewall NAT rules can only be created in NAT router mode for the direction from *Network 1* (yellow) to *Network 2* (green). For TCP, the direction is defined by the connection setup and for UDP by the initial UDP datagram.

Network 1 (yellow)

The *Source IP address(es)* from the intranet on the *Network 1* connection can either be selected from the inventory list via the select box or entered directly numerically. If a numeric value is specified, the source or source area is automatically transferred to the IP inventory for *Network 1* with the name specified under Name.

Permissible numeric specifications of the source addresses:

- *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 of „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 concatenations of IP ranges within an 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.

The *Destination port(s)* is the port number to which the client initiates a connection in *Network 1*. The Microwall

Gigabit monitors incoming packets with this destination port and forwards them to the destination system defined in Network 2. The following entries are permitted when specifying the destination port(s):

- *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 that „8000, 10-1000“ is, for example, an invalid input.

Network 2 (green)

Here the destination system (destination IP and destination port) is specified at connection *Network 2*, to which the connections defined in area Network 1 are forwarded.

The destination IP address at connection *Network 2* can either be selected from the inventory list via the select box or entered directly numerically. If a numeric value is specified, the destination is automatically transferred to the IP inventory for Network 2 with the name specified under Name.

Permissible numeric specifications of the destination address:

- *Single IP address*
  IP address in dot notation (e.g. 10.20.0.4)

The following entry is permitted when specifying the destination port:

- *Single port number*
  e.g. 8000

Protocol

Specifies whether the rule applies to *TCP* or *UDP*.

The *FTP* TCP option must be enabled when formulating the rule for FTP connections. Parallel TCP connections negotiated in the protocol history are automatically allowed and blocked.

UDP is a connectionless protocol which, however, is frequently used by applications with a request reply principle (e.g. DNS). In these cases the option *Allow reply in reverse direction* must be activated. The microwall automatically accepts an incoming reply datagram within a timeout.

Action

Accept allows the data traffic defined by the rule.

Log creates an entry in the log file of the microwall for each connection setup according to the rule.

Activate

Activates the rule immediately after pressing the *Apply* button.

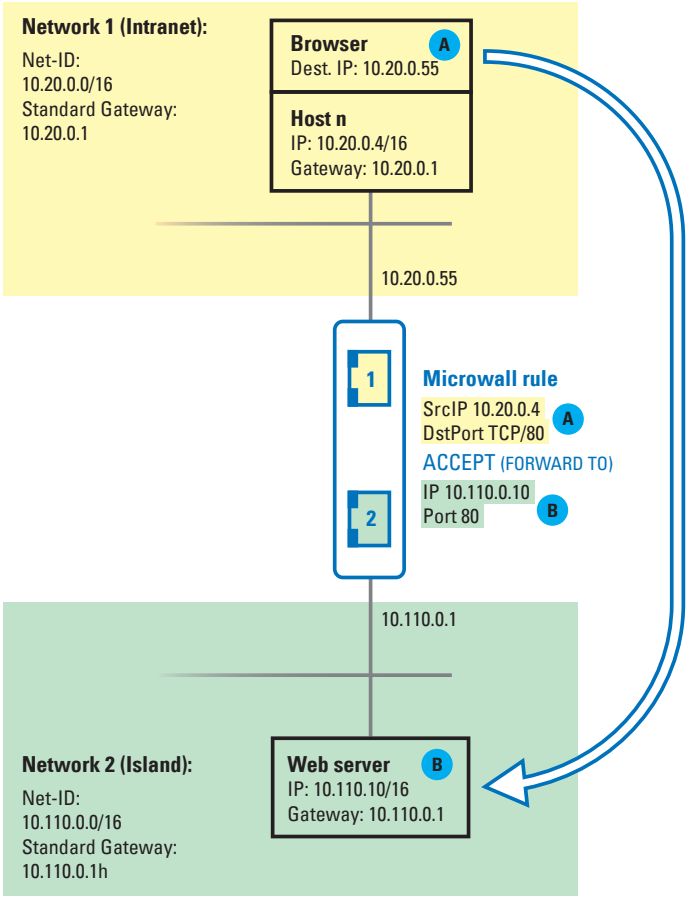
If the option is not set, pressing *Apply* creates the rule but does not apply it. Data traffic according to the rule is not possible. The rule can be activated later in the rule overview.

Label

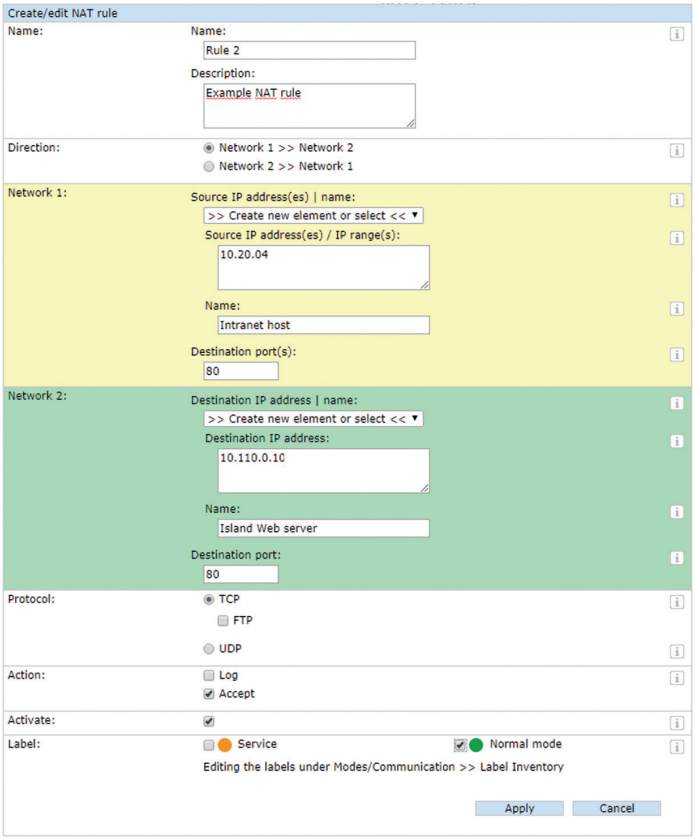
One or more labels can be assigned to the rule for a clearer display or display filtering in the rule overview. The labels *Normal mode* and *Service* are pre-installed ex works. Via the link *Label inventory* in the menu tree further labels can be created.

5.5.1 Firewall NAT rule example

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 Gigabit itself is integrated with the IPs 10.110.0.1 and 10.20.0.55 into the networks. The intranet IP of the microwall Gigabit is used as the destination address in the browser, where it is then replaced by the island IP 10.110.0.10 as a rule.



The rule dialog to be filled in for this example:.



6 Security & maintenance

- Firmware updates
- Individual certificates
- Deactivation of unneeded services
- Emergency access via service button
- Reset to factory settings via service button

6.1 Firmware updates

The firmware of the Microwall Gigabit is constantly being further developed. For this reason, the following chapter describes how to upload the firmware.

The firmware can be updated either with the help of the management tool WuTility or via the web-based management of the Microwall Gigabit.er

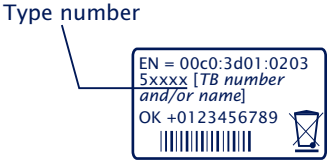
6.1.1 Where is the latest firmware available?

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 take it from the sticker on the narrow side of the housing, which also shows the Ethernet address.



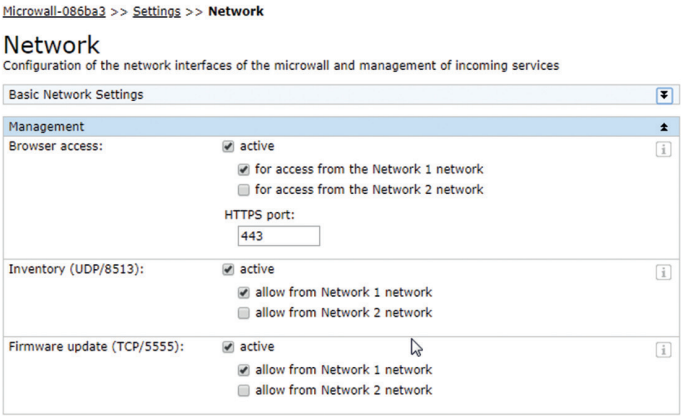
On the web data sheet of the Microwall Gigabit follow the link Firmware and start the download of the desired version. Before uploading into the microwall, the actual firmware file must be unpacked from the zip archive.

6.1.2 Firmware update with WuTility

For the firmware update with WuTility, this must be installed

on a Windows PC. Its IP settings must allow communication with the microwall and its current IP parameters.

Prerequisite for the firmware update 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 *Network 1* interface.



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

To transfer the new firmware to the Gigabit microwall, select the desired microwall in the WuTility inventory list and click the Firmware button.

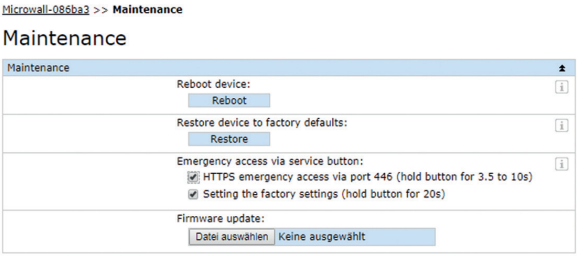
In the following dialog select the firmware file to be transferred (*.uhd) and press the Next button. After the successful transfer, the device automatically restarts and is then ready for operation again.

6.1.2 Firmware update per Web-Based-Management

In network environments that do not permit the use of WuTility or where the update service in the microwall has been

deactivated for security reasons, the firmware update can be performed from Web-based management.

Switch to the *Maintenance* page in the Microwall Gigabit menu tree.



Select the previously downloaded and unpacked firmware file (*.uhd) and press the *Apply* button. The update is started with confirmation of tChe confirmation prompt.

6.2 Individual Certificates

For security reasons, access to the Web-Based-Managemnet of the microwall is only possible encrypted via the HTTPS protocol.

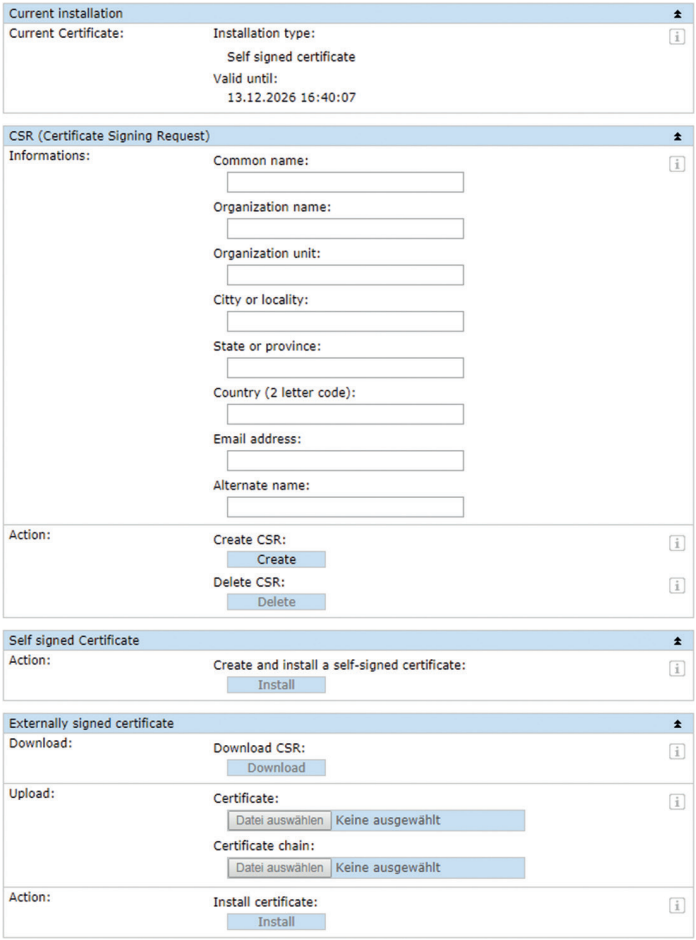
The factory preinstalled, self-signed certificate of the Microwall Gigabit generates security warnings for current browsers. These must be explicitly acknowledged and/or confirmed with suitable exception rules for WBM accesses.

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

The creation, signature and installation of your own certificate are divided into the following rough steps:

- Generation of a CSR (Certificate Signing Request) with associated private key in the Microwall Gigabit
- Download of the CSR and external signature to a certificate by a trustworthy certification authority.
- Upload and install the certificate into the Microwall Gigabi

Click on the link *Certificate Management* in the menu tree. In addition to information on the currently installed certificate, all functions for handling individual certificates are included here:



Creating a Certificate Signing Request (CSR)

Enter all required information in the CSR form. The only mandatory field is the *Common Name* under which the web pages of the Microwall Gigabit will be called later in the browser. Under *Alternative Names* you can enter additional names, IP addresses and wildcard names. The name entered in *Common Name* is automatically adopted in the *Alternative Names*.

By clicking on *Create*, the Microwall Gigabit generates an RSA key pair and creates a CSR from the public key and the information provided.

Installing a self-signed certificate

By clicking on *Install* under *Self Signed Certificate*, the CSR can be provided with a self signature. Browsers will report a security warning when they visit the web pages.

Externally signed certificate

The generated signing request can be downloaded from the Microwall Gigabit via the button Download for the purpose of an external signature. The download is in PEM format.

After the signature by the certification authority (CA), the certificate and any required certificate chain can be loaded into the Microwall Gigabit using the appropriate 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 Information, you can find the file information of the current certificate, the certificate chain, and the validity date.

6.3 Deactivation of unneeded services.

The Microwall Gigabit provides three incoming own services:

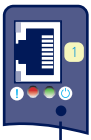
Port/Socket number	Application	System-password?-	Configurable/deactivate?
443 (TCP)	HTTPS management)	yes	yes/yes
8513 (UDP)	Inventory	no	no/yes
5555 (TCP)	Firmware update with WuTility	yes	no/yes
446 (TCP)	HTTPS Emergency access (only after activation via the service button)	no	no/yes

Configuration and activation/deactivation of these services can be 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 network environments with increased security requirements, it can be useful to deactivate all incoming services after the communication rules have been set up in operation. If changes are necessary at a later date, Web access can be reactivated at any time using the emergency access button. (see chapter Emergency access via service button).

6.4 Emergency access of the Microwall Gigabit

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



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

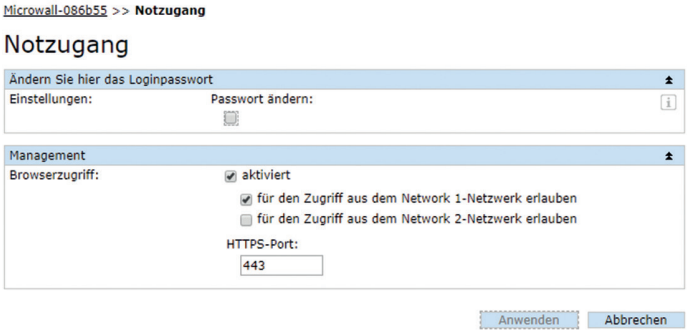
The router/firewall function remains fully active in this state.

Emergency access activates a non-password-protected web page on the microwall with the option of overwriting the current password. Therefore, take appropriate measures against unauthorized access in advance.

Emergency access call and function
Emergency access is via browser with HTTPS via TCP port 446:

https://[IP address|Host name]:446

Without a password request you will go to the following website:



Overwrite the current password
By activating the option *Change password*, you have the possibility to change the current password for the 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.

Activation of Standard Web-Based Management
Under Management, define on which port and under which port the web management of the Microwall Gigabit should be accessible.

End emergency access
Änderungen werden mit einem Klick auf *Anwenden* übernommen und die Microwall führt einen Neustart der betroffenen Dienste durch. Anschließend ist wieder der Zugriff auf das passwortgeschützte Standard Web-Interface über den konfigurierten TCP-Port möglich.

A click on *Cancel* discards any changes made and the microwall restarts the required services. Afterwards, access to the password-protected standard web interface is again possible via the configured TCP port.

6.5 Factory settings

A reset to the factory settings of the microwall can be performed via the recessed service button on the front panel.

Service button

Press the service button with a suitable pointed object (e.g. paper clip) and keep it pressed for at least 20s. After 3.5, the Error LED starts flashing slowly and after approx. 10 seconds it starts flashing rapidly. After a total of approx. 20s the reset to the factory setting is carried out. If the service button is released while the service LED is flashing rapidly in the 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 lights up permanently again. The Microwall Gigabit must now be put into operation again. Information on this can be found in the chapter Start-up.

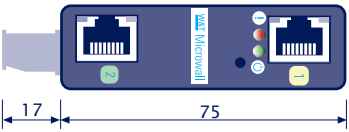
7 Appendix

- Technical data and dimensions
- Licenses

7.1 Technical data and dimensions

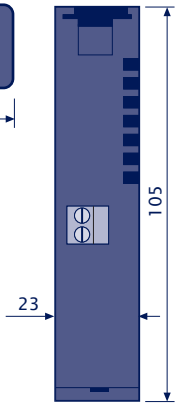
Power supply ... Power-over-Ethernet: External power supply, screw terminal	 37-57V DC from PSE DC 24-48V (+/-10%)
Current consumption ... Power-over-Ethernet: Ext. supply	 PoE Class 2 (3,84 W - 6,49W) typ. 150mA@24V DC max. 200mA@24V DC
Galvanic isolation	Network interfaces: min 500V
LAN-Port *Network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

Front view 55210



Measure in mm, +/-1mm

Bottom side 55210



7.2 Licenses

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

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

Preamble

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

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

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

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

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

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

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

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

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

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

Index

A
Auto Negotiation 16

C
Certificates 57

E
Emergency access 61

F
Firmware updates 54

H
Hardware installation 14

L
Licences 67
Link state 17
Login 33

N
NAT router 37

O
Operating modes 37

P
PoE 15

R
Reset 19
Rule overviews 39

S
Security 53
Service button 19
Standard router 37
System LED 18

T
Technical data 65

W
Web-Based-Management 31
WuTility 22