

Data sheet:

## Microwall IO



Article no.: 55212

**EUR 558.00**

\*Net price for commercial users









### Secure communication for machines and systems

The Microwall IO routes these device islands securely and easily into the company intranet. Simple and intuitive filter rules protect sensitive island communication from harmful events in the intranet and from undesired access. Remote maintenance and remote access to the devices in the island network plus management of the Microwall VPN can be accomplished over a WireGuard VPN tunnel both as VPN server and VPN client.

The digital in- and outputs allow you to integrate remote maintenance and firewall-specific Microwall IO actions into automation and process environments. A PLC output or simple button/switch can for example provide VPN access, control certain firewall rules or check on the status of network interfaces. The outputs enable external visualization of messages and events such as an activated VPN access.

**More info:** More about how the firewalls work can be found [here](#).

## Properties

### Interfaces:

- **2x Ethernet 100/1000BaseT**
  - Autosensing/Auto-MDIX
  - High data throughput
  - max. 900 mbps in router mode, max. 300 mbps VPN
- **2 switching inputs + 2 switching outputs**
  - 24V inputs + outputs
  - Outputs drive up to 500mA

### Connectivity:

- **2 digital inputs + 2 digital 24V outputs**
  - Inputs control VPN, firewall rules and network interfaces
  - Outputs report for example VPN connections
- **Mode: Standard router**
  - Integration into the routing concept of the intranet
  - Static NAT can be used for 1:1 mapping of intranet IPs on island hosts.
- **Mode: NAT router**
  - Integration of the islands via a single Intranet IP
- **WireGuard VPN Server**
  - Secure VPN connection to the island for Windows, Linux, Android, MacOS, IOS clients, Microwalls
  - Access control of VPN clients using dedicated firewall
  - Optional control of the tunnel using digital inputs
  - Digital outputs indicate the VPN status
- **WireGuard VPN client**
  - VPN connection to your manufacture/service network
  - Optional control of the tunnel using digital inputs
  - Digital outputs indicate the VPN status
- **WireGuard VPN Box-to-Box**
  - VPN tunnel between two Microwalls
  - Secure connection of island networks using the intra/internet

### Management & Security:

- **Secure firmware concept with Secure Boot**
  - No uploading of manipulated firmware or third-party firmware

- **Configuration via HTTPS-Only Mode**
  - Supports individual certificates
  - Fast startup using WuTility or DHCP
  - Required password without default login
- **Port management for all local services**
  - All service/management services can be configured/deactivated
- **Consistent whitelist-based firewall concept**
  - Filter rules based on IPv4 addresses and TCP/UDP port numbers
  - Rule sets can be controlled using digital inputs
  - Dedicated firewall for incoming VPN connections
- **Logging**
  - Identification of undesired communication attempts
- **Network management systems**
  - Optional support for SNMPv2c/3 (read)

#### Power supply:

- **External power**
  - Screw terminals, 24V-48V DC
- **Power-over-Ethernet (PoE)**

#### Standards & more

- **Conforms to standards both in office and industrial environments:**
  - High noise resistance for industrial environments
  - Low noise emission for residential and business areas
- **5 year guarantee**

♥ Wish for something!  
Your suggestions for improvement and additions

---

## Run modes

The Microwall IO casts sensitive components or sub-networks into a separate island network and isolates the latter from the higher level company intranet. For remote maintenance, remote support, etc. a WireGuard VPN server is available which provides selected VPN clients with secure and dedicated firewall-protected access to the island components.

All connections between the networks must be given express permission via rules based on source/destination IP and the TCP/UDP port numbers used. Communication with undocumented and/or undesired services is prohibited and harmful events such as overload kept from the island.

#### Filter rules and VPN management

The firewall rules and VPN management are administered simply and clearly using the Microwall IO web pages and are uniformly whitelist-based. This blocks any communication which is not expressly permitted in the form of a rule.

#### Digital in- and outputs for control and reporting

The digital inputs enable event-based activation of VPN access or switching rule groups for the firewall. Then for example when there are equipment faults the operator or equipment controller itself can open the VPN connection to the manufacturer through a switching contact.

#### Use as NAT or standard router

Similar to a traditional DSL internet connection, the entire island network is incorporated into the network there via just a single IP address of the intranet. No intervention into the routing concept of the intranet is necessary. Operation of multiple island networks having the same IP ranges is also possible in this mode. Machine and equipment builders can then also operate internal networks using a uniform series IP configuration - no cumbersome adjustments to the customer infrastructure necessary.

In Standard Router mode the island network is incorporated into the routing concept of the intranet by means of static routing for example. Static NAT can also be used for 1:1 mapping of intranet addresses to fixed IPs in the island network. These island hosts thereby become quasi-local components of the intranet while still enjoying the protection of appropriate firewall rules.

#### WireGuard VPN

As a VPN solution for remote access to the island network the Microwall IO uses the WireGuard platform. Compared with other VPN solutions this offers advantages such as high data throughput and ease of management with the same high level of security and stability. Details and current information about WireGuard can be found at <https://www.wireguard.com>. The Microwall IO can provide a VPN client or VPN server terminal point on your intranet connection. Depending on the application external WireGuard clients can dial in to the island or the Microwall connects like a VPN client - for example to your service network.

---

## Technical data

#### Connections and displays:

Network: 2x 100/1000BaseT Autosensing/Auto-MDIX  
RJ45  
IPv6 on request

Digital outputs:	2 x Digital Out 6V-30V, 500mA Short-circuit-protected
Digital inputs:	2 x Digital In max. input voltage +/-30V protected against reverse connection within this range Switching threshold 8V +/- 1.5V "On" current = 2.2 mA
Data throughput:	Router mode (unidirectional TCP): max. 900MBit/s VPN tunnel (unidirectional TCP): max. 300MBit/s
Galvanic isolation:	Network connections min. 1500 V
Power supply:	Power-over-Ethernet (PoE) or DC 24V .. 48V (+/-10%) and
Connections:	1 x 6 position screw terminal, plug-in, I/Os, RM 3.5mm 1 x 2 position screw terminal, plug-in, ext. power, RM 5.08mm 2 x RJ45 for network
Current consumption:	PoE Class 2 (3.84 W to 6.49 W) or for external supply: typ. 160mA @24V DC max. 200mA @24VDC
Indicators:	2x LED System and Services 4x LED I/O Status

#### Housing and other data:

Housing:	Plastic compact housing for top-hat rail mount 105x45x75mm (l x w x h)
Enclosure rating:	IP20
Weight:	ca. 180g
Ambient temperature:	Storage: -40..+85°C Operating 0..+50°C (no stack mounting)
Permissible relative humidity:	5..95% RH, non-condensing
Scope of delivery:	1x Microwall IO 1x Quick Guide


#### Accessories

\*Net unit price for commercial users


#### Power supplies

Plug-in power supply, 24V / 500mA DC with Euro plug	11021	21.00€	
Plug-in Power Supply, 24V / 750mA DC with Euro, US and UK plug	11026	38.00€	
Power supply for DIN rail, 24V / 630mA DC (merchandise, 2-year manufacturer's guarantee)	11080	33.00€	

#### Mechanical Accessories

Wall mount housing, enclosure rating IP66 / IP67	11120	54.00€	
Mounting bracket for wall mounting	58812	11.20€	
19" DIN rail	58813	21.00€	

#### Supplementary network products

Ethernet Switch Industry, 4 Port	55604	218.00€	
----------------------------------	-------	---------	---

#### Software

WuTility	00104	free	
----------	-------	------	---

\* Our offering is intended only for commercial users. We will be happy to refer private end customers to trading partners through whom our products can be purchased.



We are available to you in person:

Wiesemann & Theis  
GmbH  
Porschestr. 12  
42279 Wuppertal  
Phone: +49 202/2680-110 (Mon.-Fri. 8 a.m. to 5 p.m.)  
Fax: +49 202/2680-265  
info@wut.de

none of our statements should be applied without verification. Please let us know of any errors or misunderstandings you find so that we can become aware of and eliminate them.

[Data Privacy](#)