Security Datasheet

Industrial Security Router – 4TX & 4GT Models

Firmware 2.2.2 or higher

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
D-32758 Detmold
Germany
Fon: +49 5231 14-0
Fax: +49 5231 14-292083
www.weidmueller.com

Industrial Security Router – 4TX & 4GT Models

This Security Data Sheet provides you with a condensed overview of the security functions of the devices. It is an addition to the product specific

- Hardware Installation Guide
- User manual

Security intended use:

The device has been specifically developed to ensure IT security for machines and equipment, enable secure remote maintenance over the Internet and facilitate communication between networks within industrial environments.

The Industrial Firewall supports the following application scenarios:

- Remote maintenance
- NAT router
- Cellular router
- Machine firewall

The device may only be mounted, installed and operated within the limits of the stated specifications. Operation in any environment not described in this manual is prohibited.

In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

Cellular Communication and Cybersecurity:

Mandatory requirement
When operating over cellular or any wide-area connection (including Internet uplink via Ethernet), you must use an additional secure communication mechanism, e.g.:

- VPN via Weidmueller u-link
- OpenVPN or IPsec tunnels configured on the device
- Mutual TLS/HTTPS directly between endpoints, independent of the Weidmueller device

Note on user data
The device's own web interfaces (e.g. configuration GUI) are offered only via HTTPS with a valid certificate. However, the operator is responsible for protecting the confidentiality and integrity of transit traffic (e.g. from connected machines or sensors).

Further recommendations:

- Use a private APN (Access Point Name) to keep the device off the public Internet.
- Implement traffic filtering and IP whitelisting on the private APN to block unauthorized access and DoS attacks.
- If SMS services are used, protect them via the private APN as well.

Protection of sensitive data:

The device may store sensitive items such as:

- Cryptographic keys
- Passwords and certificates
- Security-related configuration parameters

At present, no secure storage per EN 18031-1 § 6.4 is implemented; data is not protected against modification or theft. Therefore, follow the guideline:

1. **Physical security**:

   Only create, store and use sensitive data when the device is in a physically protected environment (locked cabinet, access control, CCTV).

2. **Loss or theft**:

   Treat all keys, certificates and passwords as compromised and revoke or replace them immediately.

3. **Configure on-site:**

   Load configuration data only at the final installation site. Never pre-load during storage or transport. For remote communication (especially HTTPS), replace the factory certificate with an organisation-specific trusted certificate.

4. **Tamper-evident seal:**

   Each device ships with a seal. Inspect it on first start-up and at regular intervals.

Improper use:

Any operation other than, or extending beyond, the use described above constitutes improper use.

The device must not be used:

- To control vehicles.
- In applications that require additional approvals beyond the manufacturer's declaration (e.g. hazardous areas, medical technology).
- For payment-processing services.
- By private individuals.

Do not commission the device if it has suffered transport damage or if the specifications cannot be met. Take it out of service immediately if conditions change.

Weidmueller assumes no responsibility or liability for personal injury or property damage resulting directly or indirectly from improper use.
If the device shows obvious damage (e.g. due to incorrect storage or mishandling), shut it down at once and protect it against unintentional start-up.

Weidmüller PSIRT (Product Security Response Team)

Comment	Link
Weidmueller has established a PSIRT and provides information on product-specific security vulnerabilities and their elimination on the Weidmüller website "Security Advisory Board“	https://support.weidmueller.com/support-center/popular-resources/security-advisory-board
Weidmueller publishes security vulnerabilities of its products at VDE @CERT.	https://cert.vde.com/en/

Weidmüller security activities

Weidmüller has already implement a certified Secure Product Development Process according to IEC62443-4-1.

Weidmüller will offer "Secure by Design" products in accordance with IEC62443-4-2. If required, please contact our sales staff

How to find product information

Device type	**Physical/optic:** Type plate on device, Label on packaging **Web interface**:„Device type“ in „System State“ page
Software version	**Physical/optic:** no **Web interface**:„Firmware Version“ in „System State“ page
Hardware version	**Physical/optic:** Type plate on device, Label on packaging
MAC address	**Physical/optic:** Type plate on device, Label on packaging **Web interface**: „MAC Address“ in „System State“ page
Serial number	**Physical/optic:** Type plate on device, Label on packaging **Web interface**:„Serial No“ in „System State“ page

Overview of Available Network Interfaces

Network Interface	Role	Factory default behavior	Packet forwarding
WAN/ETH1	Single port	Separate; not connected to LAN 1-3 (ETH 2-4 for 4GT models). DHCP client. No IP forwarding in commissioning mode.	No
LAN1-LAN3/ETH2-ETH4	Internal switch group	Wired as an internal Layer-2 switch. Forwards all traffic in factory state. Optional packet filtering.	Yes

Important notes

- LAN1-LAN3 (ETH2-4 for 4GT models) behave as an unmanaged Layer-2 switch with no isolation between ports in factory default.
- For 4GT models, port isolation for ETH2-4 is possible using extended operating mode.
- WAN (ETH1 for 4GT models) is completely physically and logically isolated from LAN1-LAN3 (ETH2-ETH4 for 4GT models), allowing a secure initial setup (Commissioning Mode).
- Routing and firewall functions that are in place with factory default settings do not change the behavior.
- All Ethernet ports are physically accessible; secure or document them as part of your risk analysis.

Hardware Interface	Default	Can be changed	Comment
Serial RS485	Not operative	No	Planned for future
Mobile	Disabled	Yes	If not used, do not enable it

Protection of hardware interfaces:

The device offers several physical interfaces that have no built-in authentication or access control and therefore present potential attack vectors. Secure them during installation and commissioning.

Hardware Interface	Default	Can be changed	Risk	Possible consequences
USB Ports	Active	Yes	Connection of unauthorized devices (keylogger, malware)	Malware injection, data exfiltration
Reset Button	Active	No	Reset to insecure settings	Loss of secure configuration, removal of access control
Serial & Digital I/Os	Disabled	No	Direct access to control signals	Manipulation of control logic
Smart-card slot	Active	No	Access to cryptographic keys	Identity theft, misuse of authentication

Recommended safeguards

- Mount the device in a locked control or server cabinet accessible only to authorised personnel.
- Use mechanical port blockers or locks to protect unused connectors.

Network access functions

Function	Default	Can be changed	Comment
Port usage	Active	Yes	Disable unused LAN Ports
Virtual Private Network (VPN)	Disabled	Yes	Use a VPN to access your local network remotely. OpenVPN, IPSec and u-link are supported.
NAT masquerading	Disabled	Yes	Hide local IP addresses. Use NAT masquerading when the router is directly connected to a public network (e.g. via 4G)

Default packet filter rules:

The device includes a packet-filter engine supporting Layer-2 (Ethernet/MAC) and Layer-3 (IP) rules for granular traffic control.

Filter type	Operating Mode (Default)	Description
Layer-2 filter	Allow all traffic	No MAC-Level restrictions
Layer-3 filter	Block all traffic	In Factory Default mode all packets are dropped (Drop-All). An explicit operating mode must be selected before normal use.

Supported functions:

- **Layer-2:** MAC-address filtering (e.g. allow only specific sources)
- **Layer-3:** IP addresses, subnets, protocols and ports (TCP/UDP) with separate rules for ingress and egress

Two base modes are available to choose from at the initial configuration:

- **Whitelist mode ("Block All"):** Only explicitly allowed packets are passed.
- **Blacklist mode ("Allow All"):** All traffic allowed; specific rules can block packets.

Component access functions

Function	Default	Can be changed	Comment
Login & Password	Active	Yes	Default credentials: Login: admin, Password: Detmold Setting a new password is required after starting the device with factory defaults.
User Management	Active	Yes	Two users created by default (admin and guest) but only admin user is active. Administrators can create additional users and define their privilege roles. Recommended to define additional user based on the security concept of least privilege.
Web via HTTPS	Active	Yes	Secure web access. Recommended for web access.
Web via HTTP	Disabled	Yes	Not secure web access that is not recommended. Accessing the device via HTTP will result in a redirect to HTTPS.
SNMP (v3)	Disabled	Yes	Only enable if SNMP functionality is needed.

Software and data

Function	Default	Can be changed	Comment
Backup & Restore	On demand		The configuration of the router can be stored in a file; similarly, a configuration file can be uploaded on a router.
Firmware update	On demand		From the management of the router or from the u-link cloud service the user can easily upgrade its firmware (FW) whenever any new version is available. Latest FW version of every product will always be available at Weidmüller's online catalogue.
Eventlog	Active	No	The router will always store the main events in a log. This log can be displayed and downloaded from the Management System and can also be sent to a Syslog server.
Audit log	Active	No	Logs all the security related events of the router (e.g. Login attempts, Password changes, Configuration changes, Packet filter changes, Anomalies)
Syslog	Disabled	Yes	Send logging information to an external Syslog server.

Function	Port	Protocol	Default	Can be changed	Comment
HTTP	80	TCP	Closed	No	HTTP on Port 80 is disabled
HTTPS	443	TCP	Open	No	Cannot be changed
DNS	53	TCP	Closed	Yes	DNS Proxy Service is disabled by default and can be enabled if required
DNS	53	UDP	Open	No	DNS UDP client will always apear as open UDP port 53, DNS Proxy Service on UDP port 53
DHCP Client	68	UDP	-	No	DHCP UDP Client will always appear as open port, if DHCP IP acquisition is enabled on any network device
DHCP Server	67	UDP	Closed	Yes	Pot is open when DHCP server is active
Remote syslog	514	TCP/UDP	Closed	Yes	
SNMP	161	UDP	Closed	Yes	Only open when SNMP traps are activated
NTP Server	123	UDP	Closed	Yes	NTP server/relay are active
Remote capture	2002/2003	TCP/UDP	Closed	Yes	Enable this service to capture network traffic of any interface remotely, e.g., with Wireshark. The server is listening on port 2002 (TCP) or 2003 (UDP).
Modbus TCP Server	502	TCP	Closed	Yes	Can be turned on with ModbusTCP settings
IPSec	500	UDP	Closed	Yes	IPSec Port settings
IPSec	4500	UDP	Closed	Yes	IPSec Port settings
OpenVPN	1194	UDP	Closed	Yes	OpenVPN Port settings

Network Environment Services

This device supports numerous optional network services and special functions that are disabled by default. In their default configuration some of these services are not secure against attacks from the public Internet, including (but not limited to):

Function	Port	Protocol
USBIP Device Server	3240	TCP
GPSD-Services	2947	TCP
RIP v2	520	UDP
OSPF	89	IP Protocol
Modbus/TCP Server	502	TCP
SMS Communication interfaces	-	-
Virtual COM Port	3001 / 20000	TCP
Debugging & Diagnostic (RPCAP, SSH)	22	TCP

Purpose of these services
They are intended solely for controlled, trusted networks, typically:

- Behind an active, fully configured firewall
- Over a secure VPN (e.g. IPsec, OpenVPN, u-link)
- Inside completely isolated networks (e.g. test benches, commissioning environments)

Never enable these services directly on the public Internet. Doing so creates significant risks of unauthorised access, data leakage or remote control, violating EN 18031-1:2024.

If you must enable them, apply at least these counter-measures:

1. VPN or tunnelling – IPsec, OpenVPN or u-link
2. Access protection - strong authentication
3. Network segmentation - isolate weak services
4. Firewall restrictions - limit IP ranges and ports
5. Logging - activate audit and log functions
6. Restrict access - allow only authorised hosts

Configuration is performed via the web interface or APIs.

Additional Security Documents

Comment	Reference
Weidmüller Security Guideline	„Weidmüller Security Guideline“ at https://support.weidmueller.com/support-center