Weidmüller

Industrial Security Router – 4TX & 4GT models

Firmware 2.1.1 or higher

IE-SR-4TX   IE-SR-4TX-LTE/4G-EU   IE-SR-4TX-LTE/4G-USEMEA

IE-SR-4GT   IE-SR-4GT-LTE /4G-EU   IE-SR-4GT-LTE /4G-USEMEA   IE-SR-4GT-M IE-SR-4GT-LTE/4G-USEMEA-M

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 is intended for the realization of communication networks within an industrial environment. It is intended to be used in a restricted access location (e.g. locked cabinet) with no direct internet connection.

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.

Weidmüller

Industrial Security Router – 4TX & 4GT models

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

General information

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/

Additional Security Documents

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

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

Industrial Security Router – 4TX & 4GT models

Technical information

Interfaces

Type	No	Default	Can be changed	Comment
Ethernet	4 (3 LAN + 1 WAN)	Active	Yes (LAN ports)	Disable any unused LAN port
Serial RS485	1	Not operative	No	Planned for future
Mobile	1 (4G models)	Disabled by default	Yes	If not used, don't enable it
Reset button	1	Active	No	Pressing only possible with a small object (not possible with fingers). If pressed in a specific sequence, the router gets the factory default programming
USB 2.0	1 (Only 4GT models)	Active	Yes	The USB port can be used to upload configuration files or firmware updates. This function can be partially or completely disabled

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 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)
Firewall	Disabled	Yes	Whitelisting firewall in the router. All communication that does not match to a rule top-bottom principle will be dropped. No rule ("Allow all" by default). Change the firewall settings by adding the list of communication that flows via the router. When all the required traffic is whitelisted, delete the rule "Allow all" to ensure that other traffic will be blocked

Component access functions

Function	Default	Can be changed	Comment
Login & Password	Active	Yes	Default credentials: Login: admin, Password: Detmold Strongly recommended to change to a strong and individual password!
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	Active	Yes	Not secure web access. Not recommended, disable function
SNMP (V1,V2c, V3)	Disabled	Yes	Recommended SNMP V3 if required because SNMP V2c is not secure

Industrial Security Router – 4TX & 4GT models

Technical information

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 servce 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.
Logging	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
Syslog	Disabled	Yes	Send logging information to an external Syslog server

Services and Ports

Function	Port	Protocol	Default	Can be changed	Comment
HTTP	80	TCP	OPEN	No	HTTP On Port 80 can be 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	Port is open when DHCP server is active
Remote Syslog	514	UDP/TCP	CLOSED	Yes	
SNMP	161	UDP	CLOSED	Yes	Only open when SNMP traps are activated
NTP server	123	UDP	CLOSED	Yes	NTP server/relay 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 setting
IPSec	500	UDP	CLOSED	Yes	IPSec Port
IPSec	4500	UDP	CLOSED	Yes	IPSec Port
OpenVPN	1194	UDP	CLOSED	Yes	OpenVPN Port

Industrial Security Router – 4TX & 4GT models

Technical information

Additional Support Center information

Headline	Comment	Reference
General	Further product-specific information and help can be found in the Weidmüller Support Center. Use the product type (e.g. IE-SR-4TX) in the search field.	https://support.weidmueller.com/support-center/