u-OS devices

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

ID	Typ	SW Vers.
AC1	UC20-WL2000-AC	all V2.5.0
AC2	UC20-WL2000-AC-CAN	
M3	UC20-M3000	
M4	UC20-M4000	
GW	IOT-GW30	
GWEU	IOT-GW30-4G-EU	
GWNA	IOT-GW30-4G-NA	
IBOX	FP IOT MD01 LAN S2 00000 see ID“GW”	
IBOXEU	FP IOT MD01 4EU S2 00000 see ID „GWEU“	

u-OS products

This Security Data Sheet provides you with a condensed overview of the security functions of the devices (basic u-OS functionality without extentions). It is an addition to the product specific documentation

- u-control manual / u-control MX0000 manual
- Online documentation u-OS – IOT-GW30
- Quick references / quick start guide

Security intended use:
The u-OS based products are intended for use in industrial automation. A u-control station comprising a controller and connected u-remote I/O modules is intended for the control of systems or sub-systems. The u-OS products are often connected to a fieldbus system. The product can be connected to higher-level computer networks via Ethernet and communicate with the Internet via mobile communications. Communication via Ethernet or other bus systems is assumed to be secure; i.e. the customer is responsible for preventing unauthorized access to their devices, systems, machines, and networks by means of access restrictions (e.g., access control, locked control cabinet). Networks with different security levels should only be connected with appropriate security measures, such as routers with firewalls. Communication via the Internet using mobile communications should only take place using secure communication (e.g., VPN or TLS).
The u-OS products are based on the Weidmüller Linux operating system u-OS. Individual applications are implemented using installable apps (from the Weidmüller App Hub) or directly installable Docker containers. Operation is web-based and is carried out using a browser.
Special security measures must be implemented, which are described in detail in supplementary documentation. References can be found in the “General information” chapter.

The device is not intended for storing or processing personal data or for carrying out financial transactions.

The u-OS products comply with protection class IP20 (according to IEC 60529).Proper use also includes observing the documentation supplied. The products may only be used for the intended applications.

If the products are used in a manner other than that intended by the manufacturer, the protective function they provide may be impaired. All work must only be carried out by trained specialists who are familiar with the applicable regulations and standards for the area of application.

Note
Only for IOT-GW30-4G-EU and IOT-GW30-4G-NA:
Observe the country-specific radio approvals. Check whether the device has radio approval for your location.

License terms
Components of free software are integrated into the u-OS products. The license terms can be accessed in u-OS. Observe the license terms.

General information

Additional Security Documents

Comment	Reference
Weidmüller Industrial Security website with extensive information on legal requirements (e.g., RED-DA, Machinery Directive, Cyber Resilience Act, NIS2) and solutions with Weidmüller components and security services.	https://www.weidmueller.com/int/solutions/solutions/industrial_security/index.jsp
The Weidmüller “Industrial Product Security Guideline” recommends security measures at the system level.	https://www.weidmueller.com/int/solutions/solutions/industrial_security/index.jsp

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 implemented 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

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. IOT-GW30) in the search field.	https://support.weidmueller.com/support-center/

General information

How to find product information

Device type	**Physical/optic:** Type plate on device, Label on packaging **u-OS Welcome Screen** : Device information/ Product name **u-OS Data Hub**: u_os_adm/ manufacturer_product_type
Software version	**u-OS Welcome Screen** : Device information/ u-OS version **u-OS Data Hub**: u_os_adm/ software_version
Hardware version	**Physical/optic:** Type plate on device, Label on packaging **u-OS Data Hub**: u_os_adm/ hardware_version
MAC address	**Physical/optic:** Type plate on device
Serial number	**Physical/optic:** Type plate on device, Label on packaging **u-OS Welcome Screen** : Device information/ Serial number **u-OS Data Hub**: u_os_adm/ serial_number
Supported browsers	Mozilla Firefox 102 or higher Google Chrome 114 or higher Microsoft Edge 115 or higher
App software version	**u-OS Control Center:** Apps/ App manager

u-OS devices

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

Additional Security Documents

Comment	Reference
The Weidmüller "Industrial Product Security Guideline" recommends security measures at the system level.	https://www.weidmueller.com/int/solutions/solutions/industrial_security/index.jsp

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 implemented 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 contact

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. IOT-GW30) in the search field.	https://support.weidmueller.com/support-center/

Technical information

Interfaces

Type	No	Default	Can be changed	Comment
Ethernet AC1, AC2, M3, GW, GWEU, GWNA M4	2 4	Active Active	Yes Yes	Disable unused interfaces. To disable interfaces see „Disabling ethernet interfaces“.
RS485 GW, GWEU, GWNA	1	Active	No	Active, but not connected with a functionality. It can only used by a specific application.
RS232 GW, GWEU, GWNA	1	Active	No	Active, but not connected with a functionality. It can only used by a specific application.
CAN GW, GWEU, GWNA	1	Active	No	Active, but not connected with a functionality. It can only used by a specific application.
USB AC1, AC2 GW, GWEU, GWNA M3, M4 M3, M4	 1 (device) 1 (host) 1 (device) 2 (host)	 Active Active Active Active	 No No No No	
Radio 2G, 3G, 4G GWEU, GWNA	1	Active	Yes, via SIM card	No active access from outside. A connection can only be established from the device.
Digital Input GW, GWEU, GWNA	2	Active	No	Active, but not connected with a functionality. It can only used by a specific application.
Digital Output GW, GWEU, GWNA	1	Active	No	Active, but not connected with a functionality. It can only used by a specific application.
Right-sided modul extension AC1, AC2, M3, M4	1	Active	No	Right-sided IO extension via u-remote module bus (backplane).
Left-sided modul extension M3, M4	1	Active	No	Left-sided IO extension via u-control moduls. Currently deactivated.

Network access functions

Function	Default	Can be changed	Comment
DHCP Client	Deactive	Yes	Static IP configuration is recommended.
Network load limiter	Active	No	Rate limiting for prevention of DoS attacks.
Firewall for mobile radio GWEU, GWNA, IBOXEU	Active	No	The firewall prevents active access from outside via mobile radio (3G/4G/LTE).
NTP Client	Active	Yes	A valid time is important for e.g. certificate verification. Choose a valid NTP server.

Component access functions

Function	Default	Can be changed	Comment
Login & password	Active	Yes	Default credentials: No. When starting for the first time, the user must enter a user name and password. The first user is automatically logged in as admin. Minimum password length is 6 character. Strongly recommended to change to a strong and individual password! Password policy: Minimum password length is 6 character. Note: Extened functionality is planed for future versions
Identitiy & access	Active	Yes	Identity and access management (Users & Roles) can be configured in the u-OS Control Center -> Identity & access. Multiple Users and Roles can be configured. Different permissions can be assigned to Roles. Clients can be created for using APIs e.g. u-OS Data Hub. OAuth 2.0 client credentials flow is used (Identity & access -> Clients). Unauthorized access can be configed for APIs e.g. u-OS Data Hub or Apps (Identity & access -> Access -> Unauthenticated access). This is not recommended in production. Note: Extened functionality is planed for future versions
HTTPS	Active	Yes	Secure web access. Recommended for web access.
HTTP	Deactive	Yes	Not secure web access. Not recommended, disable function.
SSH	Deactive	Yes	SSH access. Not recommended in production.

Software and Data

Function	Default	Can be changed	Comment
Backup & restore	On demand		Local Backup & Restore of Apps, data and settings via web browser is supported. The Backup is encrypted.
Firmware update	On demand		Firmware updates, APP offline installations and other SWUs are signed. Signiture is checked in installation process. Local firmware update via Web browser is supported (Welcome screen / u-OS control center / Software & updates / Update & installation). Remote firmware update be performed via hawkBit. For hawkBit configuration navigate to Welcome screen / u-OS Control Center / Software & updates / hawkBit
Logging	Yes	No	u-OS system log can be opened in the u-OS Control Center. The log is not persistent.

Software and Data

Function	Default	Can be changed	Comment
App and service installation	On demand		The u-OS operating system allows the system to be individually expanded using Apps, Docker containers or native services. Best security practices • Make sure that you only download updates from trustworthy sources (e.g. Weidmüller APPHUB or Weidmüller Support Center) • Check cyclically for new updates for the devices you are using. • Install software updates and security fixes as quickly as possible. • Bring the machine or system into a safe state before the update. • Test the new software before installing it on a large scale. • Make sure that service personnel are present at the machine or system during an automatic update so that they can react in the event of a security incident. • Create and update your security risk analysis.

Services and Ports

Note:

- Additional ports may be available through installed Apps, Docker containers or services.

Function	Port	Protocol	Default	Can be changed	Comment
HTTP all	80	TCP	Deactive	Yes	Web access unsecure
HTTPS all	443	TCP	Active	Yes	Web access secure
SSH all	22	TCP	Deactive	Yes	Secure Shell Protocol
Codemeter all	22350	TCP	Active	No	Licence management
LLMNR all	5355	TCP/UDP	Active	No	Link-Local Multicast Name Resolution
mDNS all	5353	UDP	Active	No	Multicast DNS
DHCP all	67	UDP	Active	No	Dynamic Host Configuration Protocol
avahi-daemon all	Dynamic (32768 - 61000)	UDP	Active	No	Multicast DNS Queries
SFTP all	22	SSH	Deactive	Yes	SSH File Transfer Protocol
TLS versions supported all					Supported version 1.2 and 1.3

Disabling ethernet interfaces

Note:

- Disabling of interfaces should only be performed by trained personnel and administrators.

Before disabling or enabling an interface, the following conditions must be met:

- SSH access must be enabled.
- An administrator must be connected to the device terminal.

Explanation

- Auto-connect: Prevents an interface from automatically establishing a connection when a cable is plugged in.
- Disconnect: Terminates the current active connection of the interface.

Disabling an interface
Disable auto-connect:

- sudo nmcli connection modify "<eth0|eth1|eth-x4|eth-x5|eth-x6|eth-x7>" connection.autoconnect no

Disconnect the interface:

- sudo nmcli device disconnect <eth0|eth1|eth-x4|eth-x5|eth-x6|eth-x7>

Enabling an interface
Enable auto-connect:

- sudo nmcli connection modify "<eth0|eth1|eth-x4|eth-x5|eth-x6|eth-x7>" connection.autoconnect yes

Connect the interface:

- sudo nmcli device connect <eth0|eth1|eth-x4|eth-x5|eth-x6|eth-x7>

Important: Always ensure that at least **one interface remains enabled**, otherwise you may lose access to the device. The interface names can be seen on the user interface as described in our handbook.