YASKAWA

Plug-in cards

PCIe | YRCP32F0 | Manual

HB170 | PCIe | YRCP32F0 | en | 25-10

Plug-in card PCI Express - YRCP-MP4P

YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Germany
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
Email: info@yaskawa.eu
Internet: www.yaskawa.eu.com

YRCP32F0_000_PCIe_YRCP-MP4P,2,EN - © 2025

Table of contents

1 General

1.1 About this manual

Objective and contents

The manual describes the PCIe plug-in card YRCP32F0.

- It describes the structure, configuration and application.
- The manual is targeted at users with good basic knowledge in automation technology.
- The manual does not replace sufficient basic knowledge of automation technology or sufficient familiarity with the specific product.
- The manual consists of chapters. Each chapter describes a completed topic.
- For guidance, the manual provides:
  - An overall table of contents at the beginning of the manual
  - References with pages numbers

Validity of the documentation

Type	Order no.	as of version:	
YRCP-MP4P	YRCP32F0	PCIe HW: 1	PCIe FW: V2024.0

Documentation

In the context of the use of the pertinent Yaskawa product, the manual is to be made accessible to the pertinent qualified personnel in:

- Project engineering
- Installation department
- Commissioning
- Operation

Icons and headings

Important passages in the text are highlighted by following icons and headings:

DANGER

- Immediate danger to life and limb of personnel and others.
- Non-compliance will cause death or serious injury.

CAUTION

- Hazardous situation to life and limb of personnel and others. Non-compliance may cause slight injuries.
- This symbol is also used as warning of damages to property.

NOTICE

- Designates a possibly harmful situation.
- Non-compliance can damage the product or something in its environment.

Supplementary information and useful tips.

1.2 Copyright © YASKAWA Europe GmbH

Download Center

By entering the product order number in the *'Download Center'* at www.yaskawa.eu.com, the pertinent manuals, data sheets, declarations of conformity, certificates and other helpful information for your product can be found.

Trademarks

All Microsoft Windows, Office and Server products mentioned are registered trademarks of Microsoft Inc., USA.

Linux is a registered trademark of Linus Torvalds.

PLCnext Technology is a registered trademark of Phoenix Contact.

EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

PROFINET is a registered trademark of PROFIBUS and PROFINET International (PI).

All other trademarks, logos and service or product marks specified herein are owned by their respective companies.

General terms of use

Every effort was made by Yaskawa to ensure that the information contained in this document was complete and correct at the time of publication. Nevertheless, the information contained therein is only owed by Yaskawa as it is available at Yaskawa. Correctness is not assured by Yaskawa, the right to change the information contained herein is always reserved by Yaskawa. There is no obligation to inform the customer of any changes. The customer is requested to actively keep this documentation up to date. The use of the products covered by these instructions, together with the associated documentation, is always at the customer's own risk, in accordance with the applicable guidelines and standards. This documentation describes the hardware and software components and functions of the product. It is possible that units are described which the customer does not have. The exact scope of delivery is described in the respective purchase contract.

Document support

Contact your local representative of YASKAWA Europe GmbH if you have errors or questions regarding the content of this document. You can reach YASKAWA Europe GmbH via the following contact:

Email: Documentation.HER@yaskawa.eu

Technical support

Contact your local representative of YASKAWA Europe GmbH if you encounter problems or have questions regarding the product. If such a location is not available, you can reach the Yaskawa customer service via the following contact:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany
Tel.: +49 6196 569 500 (hotline)
Email: support@yaskawa.eu

2 Hardware description

2.1 Properties

YRCP-MP4P

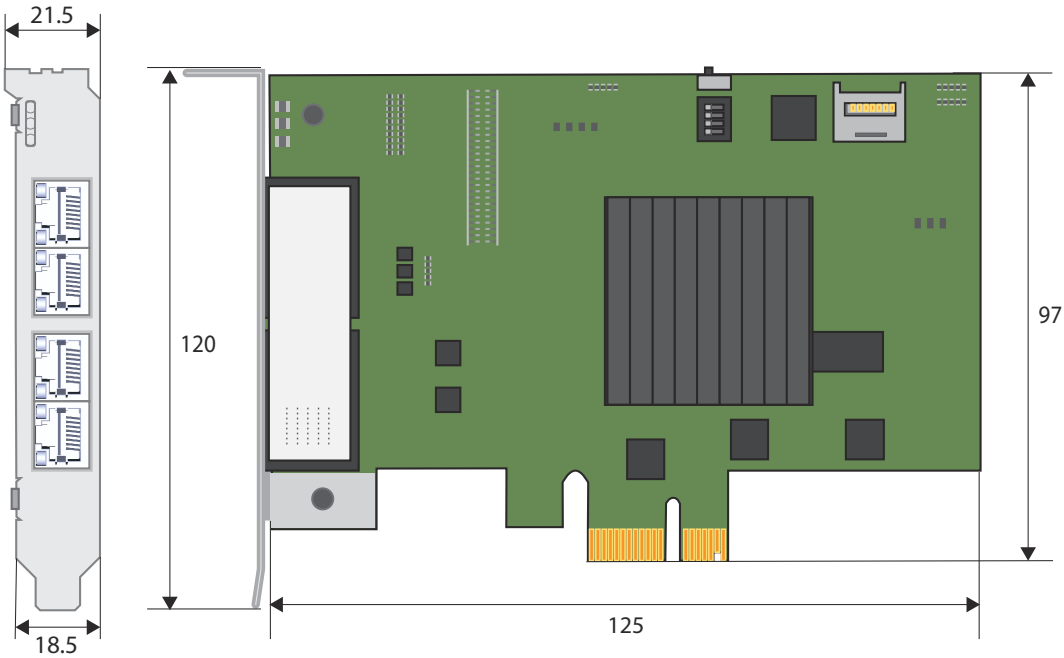
- The YRCP-MP4P is a PCIe x1 Gen1 plug-in card for installation in a robot controller with a PCI Express slot.
- The communications processor integrated on the PCIe plug-in card allows Ethernet-based connection to PROFINET and EtherCAT.
- PROFINET IO controller/device respectively EtherCAT SubDevice functionalities are supported.
- The PROFINET IO controller is configured by means of the programming tool 2CON from Yaskawa.
- When deployed in a Yaskawa robot controller, communication and data exchange with the plug-in card takes place via direct access to the memory area. This is assigned directly to the plug-in card by the operating system. An user API is used on the host side, which makes all the functionalities of the plug-in card available.

Ordering data

Typ	Order no.	Description
YRCP-MP4P	YRCP32F0	PCIe x1 Gen1 plug-in card

2.2 Dimensions

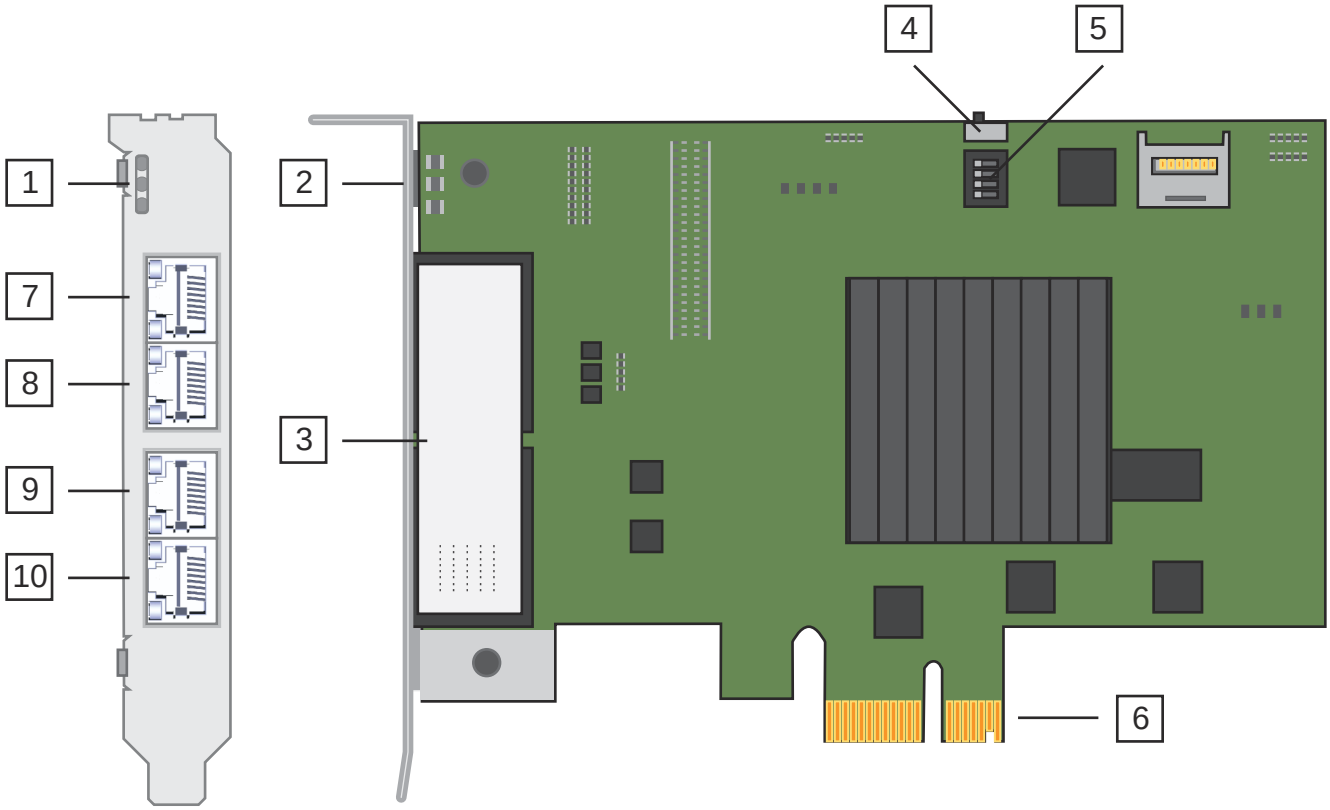
All dimensions are in mm.



2.3 Structure

2.3.1 YRCP-MP4P

Overview



1 LED bar
2 Slot bracket
3 Specific information
4 S1: Slide switch
5 S2: DIP switch
6 PCI Express interface

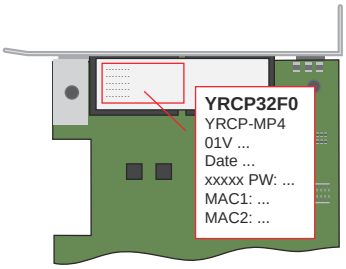
PROFINET activated (default)

7 X1: PROFINET device (internally switched with X2)
8 X2: PROFINET device (internally switched with X1)
9 X3: PROFINET IO controller / Ethernet port (internally switched with X4)
10 X4: PROFINET IO controller / Ethernet port (internally switched with X3)

EtherCAT activated

7 X1: EtherCAT port - SubDevice IN
8 X2: EtherCAT port - SubDevice OUT
9 X3: Ethernet port (internally switched with X4)
10 X4: Ethernet port (internally switched with X3)

Specific informations 3



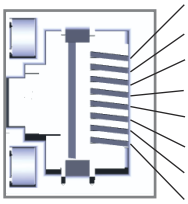
The following information is printed on the plug-in card:

- YRCP32F0 - Order number
- YRCP-MP4 - Type
- 01V - Hardware version
  - The example shows hardware version 1.
  - You can also find this in the WBM at *'Overview'...page 40*.
- Date
  - Date of production
- xxxxx - Serial number
- PW - Password
  - The password with the designation *'PW: '* is required for the initial login for the "Admin" user in *'Web-based management - WBM'...page 38*.
- MAC1/MAC2 - MAC addresses
  - *'MAC1'* for the interfaces X3/X4 (default: 192.168.1.1).
  - *'MAC2'* for the interfaces X1/X2 (default: 192.168.3.1).

It is advisable to write down the password before installing the plug-in card.

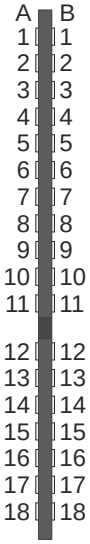
2.3.2 Interfaces

X1/X2 X3/X4



①	TD+	DA+
②	TD-	DA-
③	RD+	DB+
④	n.c.	n.c.
⑤	n.c.	n.c.
⑥	RD-	DB-
⑦	n.c.	n.c.
⑧	n.c.	n.c.

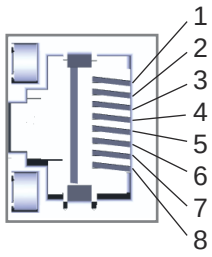
PCIe



A		B	
①	PRSNT1#	①	+12V
②	+12V	②	+12V
③	+12V	③	+12V
④	GND	④	GND
⑤	JTAG2	⑤	SMCLK
⑥	JTAG3	⑥	SMDAT
⑦	JTAG4	⑦	GND
⑧	JTAG5	⑧	+3.3V
⑨	+3.3V	⑨	JTAG1
⑩	+3.3V	⑩	+3.3Vaux
⑪	PERST#	⑪	WAKE#
⑫	GND	⑫	RSVD
⑬	REFCLK+	⑬	GND
⑭	REFCLK-	⑭	PETp0
⑮	GND	⑮	PETn0
⑯	PERp0	⑯	GND
⑰	PERn0	⑰	PRSNT2x
⑱	GND	⑱	GND

X1/X2/X3/X4 PROFINET

For configuration in a PROFINET IO controller, you can find the corresponding 'GSDML-V...-YASKAWA-YRCP-MP4P-....xml' in the 'Download Centre' at www.yaskawa.eu.com. Install these in your PROFINET configuration tool.



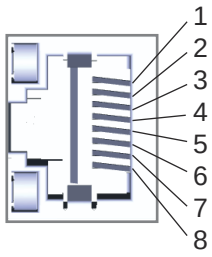
8pin RJ45 jack:

Pin	Signal	Description
1	DA+	Bidirectional pair A + (send data +)
2	DA-	Bidirectional pair A - (send data -)
3	DB+	Bidirectional pair B + (receive data +)
4	n.c.	reserved
5	n.c.	reserved
6	DB-	Bidirectional pair B - (receive data -)
7	n.c.	reserved
8	n.c.	reserved

- The plug-in card has an integrated Ethernet communication processor with PROFINET IO controller and PROFINET device.
- Use X1/X2 (default: 192.168.3.1, *'MAC2'*) to connect the plug-in card as a PROFINET device to a PROFINET IO controller.
- Use X3/X4 (default: 192.168.1.1, *'MAC1'*) to connect PROFINET devices to the PROFINET IO controller of the plug-in card.
- Via Ethernet you have access to *'Web-based management - WBM'...page 38* of the plug-in card by means of these interfaces.

X1/X2: EtherCAT port

For configuration in an EtherCAT MainDevice, you will find the corresponding 'ESI-V...-YASKAWA-YRCP-MP4P-....xml' in the 'Download Center' at www.yaskawa.eu.com. Install these in your EtherCAT configuration tool and activate the EtherCAT communication for X1/X2 by means of the user API for your host system.

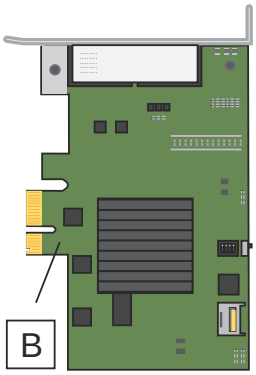


8pin RJ45 jack:

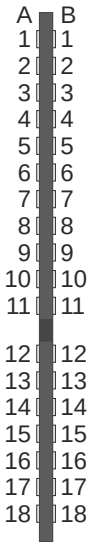
Pin	Signal	Description
1	TD+	Send data +
2	TD-	Send data -
3	RD+	Receive data +
4	n.c.	reserved
5	n.c.	reserved
6	RD-	Receive data -
7	n.c.	reserved
8	n.c.	reserved

- The plug-in card has an integrated Ethernet communication processors with EtherCAT SubDevice.
- The connection to a higher-level EtherCAT MainDevice takes place via X1: EtherCAT port - SubDevice IN station.
- The connection to subsequent EtherCAT SubDevice takes place via X2: EtherCAT port - SubDevice OUT station.
- EtherCAT uses Ethernet as transfer medium. Standard CAT5 cables are used. Here distances of about 100m between two stations are possible.
- An EtherCAT network always consists of an EtherCAT MainDevice and an various number of EtherCAT SubDevices (coupler).
- Each EtherCAT SubDevice has a RJ45 jack for the incoming EtherCAT cable from the direction of the MainDevice (here X1) and a RJ45 jack for connecting to the subsequent participant (here X2). With the respective last station the "OUT" jack remains free.

PCI Express interface



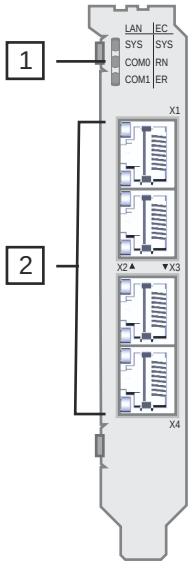
PCIe



The PCI Express interface is used to connect to a robot controller with a PCI Express slot. The interface has the following pin assignment:

Pin	Side A		Side B	
	Name	Description	Name	Description
1	PRSNT1#	Hot plug presence detect	+12	DC 12V power
2	+12	DC 12V power	+12	DC 12V power
3	+12	DC 12V power	+12V	DC 12V power
4	GND	Ground	GND	Ground
5	JTAG2	not used	SMCLK	not used
6	JTAG3	not used	SMDAT	not used
7	JTAG4	not used	GND	not used
8	JTAG5	not used	+3.3V	not used
9	+3.3V	not used	JTAG1	not used
10	+3.3V	DC 3.3V power	+3.3Vaux	DC 3.3V auxiliary power
11	PERST#	Fundamental reset	WAKE#	Signal for link activation
12	GND	Ground	RSVD	not used
13	REFCLK+	Reference clock input	GND	Ground
14	REFCLK-	(differential pair)	PETp0	Transmitter
15	GND	Ground	PETn0	(differential pair)
16	PERp0	Receiver (differential pair)	GND	Ground
17	PERn0	Receiver (differential pair)	PRSNT2x	Hot plug presence detect
18	GND	Ground	GND	Ground

2.3.3 LEDs



1 LED bar
2 LEDs RJ45 jacks

LED bar 1

Boot-up after PowerON

SYS green	COM0/RN green/red	COM1/ER green/red	Description
☐	green	☐	Application is loaded.
☐	green	green	Kernel could be copied successfully.
☐	red 2Hz	red	Error while copying the kernel.
green 2Hz	red 2Hz	red 2Hz	Application was stopped. Perform a power cycle.
green 2Hz	☐	☐	Firmware is loaded.
☐	red 0.5Hz	red 0.5Hz	Application could not be loaded. Perform a power cycle.
☐	red 2Hz	red 2Hz	Memory overflow flash memory.
green	☐	☐	Application was successfully loaded and initialized.
☐	green 2Hz	green 2Hz	Power cycle requirement according to *'Reset to factory settings type 1'...page 27*.
☐	green 2Hz	green 2Hz	Firmware update is in progress.
☐	red 2Hz	green	Invalid switch setting of DIP switch S2 *'Switches'...page 15*.

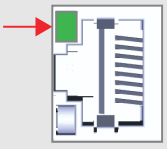
PROFINET operation 1

SYS green	COM0 green/red	COM1 green/red	Description
green 1Hz	X	X	Used for device identification.
PROFINET IO controller signals			
X	X	☐	■ The PROFINET IO controller has established an active communication connection to each configured PROFINET device. ■ The PROFINET IO controller is not configured.
X	X	red	■ Bus error, no link available. ■ Wrong transfer rate. ■ Full duplex transfer is not enabled.
X	X	red 1Hz	■ Link status is available, there is no communication connection to at least one PROFINET device.
PROFINET device signals			
X	☐	X	■ The PROFINET device has established an active communication connection to the PROFINET IO controller.
X	red	X	■ Bus error, no link available. ■ No communication connection to the PROFINET IO controller.
X	red 1Hz	X	■ Link status is available, there is no communication connection to the PROFINET IO controller.
not relevant: X			

EtherCAT operation 1

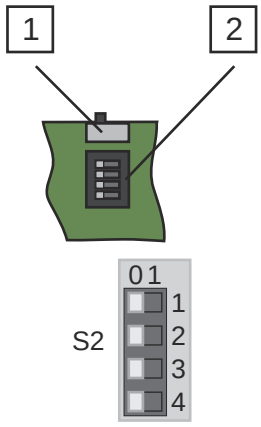
SYS green	RN green/red	ER green/red	Description
X	green 2.5Hz	X	EtherCAT SubDevice is in the PreOp state.
X	green 0.2/1s	X	EtherCAT SubDevice is in the SafeOp state.
X	green	X	EtherCAT SubDevice is in the Op state.
X		X	EtherCAT SubDevice is in the Init state or is not configured.
X	X		EtherCAT SubDevice does not report any errors.
X	X	red 2.5Hz	EtherCAT SubDevice reports incorrect configuration.
X	X	red 0.2/1s	EtherCAT SubDevice reports local error and switches to SafeOp state.
X	X	red 2x2.5Hz/1s	EtherCAT SubDevice reports a watchdog timeout, e.g. Sync manager timeout.
not relevant: X			

LEDs RJ45 jacks 2 Only the green LED (at the top) is used. The LED at the bottom has no function.

LED	Color	Function
	green	The according RJ45 jack is physically connected to the Ethernet.
	green flickers	The LED flickers when there is data traffic.

2.3.4 Switches

S1: Slide switch
S2: DIP switch



S1: Slide switch 1

The slide switch S1 is used internally and is not relevant for customer applications. Leave it in the sliding left position as shown.

S2: DIP switch 2

Only one switch may be in the "ON" position at any time. Here you can trigger the following actions:

Switch	Action
S2-1	0 (OFF): Reserved - default setting
S2-2	0 (OFF): Reserved - default setting
S2-3	■ 0 (OFF): After PowerON the plug-in card starts in *Standard Mode* - default setting. ■ 1 (ON): After PowerON, the plug-in card starts in *'Safe Mode'...page 29*. – Communication exclusively via *'Web-based management - WBM'...page 38*. – No communication via PROFINET respectively EtherCAT.
S2-4	■ 0 (OFF): The plug-in card starts after PowerON - default setting. ■ 1 (ON): After PowerON, the plug-in card performs *'Reset to factory settings type 1'...page 27*.

2.4 Approvals, directives, standards

Conformity and approval		
Conformity		
CE	2014/30/EU	EMC Directive
Approval		
UL	UL 61010-2-201	
KC	KSC C IEC 61131-2	
UKCA	2016 No. 1091	The Electromagnetic Compatibility Regulations 2016
	2012 No. 3032	The Restriction of the use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulation 2012
Others		
RoHS	2011/65/EU	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
ChinaRoHS	SJ/T 11363-2006	Use of Certain Hazardous Substances
WEEE	2012/19/EU	Take-back of electrical and electronic equipment in the EU

Protection of persons and device protection		
Type of protection	-	IP00
Electrical isolation		
to the field bus	-	electrically isolated
to the process level	-	electrically isolated
Insulation resistance	EN 61010-2-201	-
Insulation voltage		
RJ45 jack X1, X2, X3, X4	-	DC 1000V (tested for 60s)
Protective measures	-	-

Environmental conditions according to EN 61131-2		
Climatic		
Storage / transport	EN 60068-2-14	-40…+85°C
Operation	EN 61131-2	0…+60°C
Air humidity	EN 60068-2-30	RH1 (without condensation, rel. humidity 10…95%)
Pollution	EN 61131-2	Degree of pollution 2
Installation altitude max.	-	2000m
Mechanical		
Oscillation	EN 60068-2-6	1g, 9...150Hz
Shock	EN 60068-2-27	15g, 11ms

Mounting conditions		
Mounting place	-	PCI Express slot in robot controller

EMC	Standard		Comment
Emitted interference	EN 61000-6-4		Class A (Industrial area)
Noise immunity	EN 61000-6-2		Industrial area
Zone B		EN 61000-4-2	ESD 8kV at air discharge (degree of severity 3) 4kV at contact discharge (degree of severity 2)
		EN 61000-4-3	HF irradiation (casing) 80…1000MHz, 10V/m, 80% AM (1kHz) 1.4...6.0GHz, 3V/m, 80% AM (1kHz)
		EN 61000-4-6	HF conducted 150kHz…80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-4	Burst
		EN 61000-4-5	Surge[1]

1) Due to the high-energetic single pulses with Surge an appropriate external protective circuit with lightning protection elements like conductors for lightning and over-voltage is necessary.

2.5 Use in difficult operating conditions

Without additional protective measures, the products must not be used in locations with difficult operating conditions; e.g. due to:

- *dust generation*
- *chemically active substances (corrosive vapors or gases)*
- *strong electric or magnetic fields*

2.6 Technical data

Order no.	YRCP32F0
Type	YRCP-MP4P
Module ID	-
Power supply via PCIe	
Voltage	+3.3 V DC ±5 %
Voltage	+12.0 V DC ±5 %
Typical current consumption	
3V3@25°C	0.7 A
3V3@60°C	1.3 A
12V@25°C	10 mA
Maximum current consumption	

Technical data

Order no.	YRCP32F0
3V3@25°C	1.3 A
3V3@60°C	2.3 A
12V@25°C	20 mA
Hardware	
CPU	TRITON (ARM Cortex-A17)
CPU cores	3
Frequency	1.26 GHz
RAM	512 MB
eMMC	8 GB
Operating controls	LEDs, DIP switch (S2)
Integrated SliceBus supply	-
Connectors	
Serial Com (Sub-D)	-
SliceBus	-
Number of RJ45 interfaces	4
Operating system	
Operating system	Linux mit RT Kernel
Overlay filesystem on internal eMMC	✓
Overlay filesystem on internal eMMC, Capacity	1500 MB
Overlay filesystem on external SD card	-
Overlay filesystem on external SD card, Capacity	-
Firewall	✓
SSH/SFTP	-
Synchronization via Ethernet (NTP)	✓
DNS	✓
Web-based Management (WBM)	✓
PROFINET System	
VendorID	0x0111
DeviceID	0x047C
Specification	Version 2.4
PROFINET-capable ports	X1/X2 Device, X3/X4 Controller
Controller	✓
- Max. number of devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Max. number of I/O data (incl. IOxS)	8192 Byte
- Cycle time	1 ms .. 512 ms
- System Redundancy	-
- Fast Startup	✓
- Fast Startup, Max. number of devices	32

Order no.	YRCP32F0
- Topology	✓
Device	✓
Device I/O Data	2 Byte / 2 Byte 512 Byte / 512 Byte 4 Byte / 4 Byte 8 Byte / 8 Byte 16 Byte / 16 Byte 32 Byte / 32 Byte 64 Byte / 64 Byte 128 Byte / 128 Byte 256 Byte / 256 Byte 436 Byte / 436 Byte
- Cycle time	1 ms .. 512 ms
- MRP Client supported	✓
EtherCAT SubDevice	
I/O PDO mapping	2 Byte / 2 Byte 512 Byte / 512 Byte 4 Byte / 4 Byte 8 Byte / 8 Byte 16 Byte / 16 Byte 32 Byte / 32 Byte 64 Byte / 64 Byte 128 Byte / 128 Byte 256 Byte / 256 Byte 436 Byte / 436 Byte
Update time	1 ms .. 512 ms
EoE support	-
CoE support	✓
FoE support	-
Distributed Clock support	-
Housing	
Material	Stainless steel
Mounting	Plug-in card
Mechanical data	
Dimensions (WxHxD)	21.6 mm x 120.8 mm x 138.4 mm
Net weight	105 g
Weight including accessories	105 g
Gross weight	180 g
Environmental conditions	

Technical data

Order no.	YRCP32F0
Operating temperature	0 °C to 60 °C
Storage temperature	-40 °C to 85 °C
Certifications	
UL certification	yes
KC certification	yes
UKCA certification	yes
ChinaRoHS certification	yes

3 Deployment

3.1 Safety instructions

DANGER

Safety instructions

Observe the following safety instructions! Disregarding these safety regulations may result in death, serious personal injury or damage to equipment.

- Personal and property protection are only guaranteed if the device is used in accordance with its intended use.
- Observe the safety regulations of electrical engineering and the employer's liability insurance association!
- Only perform work on the device when the power is switched off!
- The device may only be installed by qualified personnel in accordance with the specifications in the corresponding documentation.
- Electrical work may only be performed by qualified electricians.
- The device may only be commissioned by a person responsible for the safety of the system. Only this person may connect the supply voltage.
- Observe the necessary precautions when handling electrostatically sensitive components (EN 61340-5-1, IEC 61340-5-1)!
- Repairs to the device must only be performed by the manufacturer.
- Keep the operating instructions!
- The operator of the device or plant is subject to the legal obligations regarding safety at work. The Machinery Directive must therefore be taken into account.

CAUTION

When working with and on electrostatic sensitive modules, make sure that personnel and equipment are adequately grounded.

NOTICE

Device failure due to operation outside the permissible ambient temperature range

Operating the plug-in card outside the permissible ambient temperature range may lead to malfunctions or even device failure. *'Approvals, directives, standards'...page 16*

- Make sure that the permissible ambient temperature of the plug-in card is observed during operation.

NOTICE

Device failure due to operation above the permissible specifications for vibration and shock

Operating the plug-in card above the permissible vibration and shock specifications may result in malfunctions or even device failure. *'Approvals, directives, standards'...page 16*

- Make sure that the permissible specifications for vibration and shock are observed during operation of the plug-in card.

Intended use

- It is the customer's responsibility to comply with all pertinent standards, codes, or regulations applicable to the use of the product, including those that apply when the Yaskawa product is used in combination with other products.
- The customer must confirm that the Yaskawa product is suitable for the customer's plant, machinery and equipment.
- If the Yaskawa product is used in a manner not specified by this manual, the protection provided by the Yaskawa product may be impaired and the use may result in material or immaterial damage.
- Contact Yaskawa to determine whether use is permitted in the following applications. If the use in the respective application is permissible, the Yaskawa product is to be used by considering additional risk assessments and specifications, and safety measures are to be provided to minimise the dangers in the event of a fault. Special caution is required and protective measures must be taken in the case of:
  - Outdoor use, use with possible chemical contamination or electrical interference, or use under conditions or in environments which are not described in product catalogs or manuals
  - Nuclear control systems, combustion systems, railway systems, aviation systems, automotive systems, medical devices, amusement machines and equipment that is specifically regulated by industry or government
  - Systems, machines and devices that can pose a risk to life or property
  - Systems that require a high degree of reliability, such as gas, water or electricity supply systems or systems that operate 24 hours a day
  - Other systems that require a similarly high level of security
- Never use the Yaskawa product in an application where failure of the product could cause serious danger to life, limb, health or property without first ensuring that the system is designed to provide the required level of safety with risk warnings and redundancy to avoid the realisation of such dangers and that the Yaskawa product is properly designed and installed.
- The connection examples and other application examples described in the product catalogs and manuals of Yaskawa are for reference purposes. Check the functionality and safety of the devices and systems actually to be used before using the Yaskawa product.
- To avoid accidental harm to third parties, read and understand all prohibitions on use and precautions, and operate the Yaskawa product correctly.

Field of application

WARNING

Danger by non intended use!

Any other use beyond the intended use and/or other use of this product can lead to dangerous situations and is prohibited.

The YRCP-MP4P is constructed and produced for:

- industrial use.
- general control and automation tasks.
- industrial network communication, machine and process control.
- the connection to PROFINET and EtherCAT (optional).
- the installation in a robot controller.
- operation within the environmental conditions specified in the technical data.

DANGER

This device is not certified for applications:

- in explosive environments (EX-zone)

Disclaimer

(1) The contractual and legal liability of Yaskawa and the legal representatives and vicarious agents of Yaskawa for compensation and reimbursement of expenses in relation to the content of this documentation is excluded or limited as follows:

a) For slightly negligent breaches of *Essential Contractual Duties* arising from the contractual obligation, for Yaskawa the amount of liability is limited to the foreseeable damage typical for the contract. *'Essential Contractual Duties'* are those duties that characterise the performance of the contract and on which the Yaskawa customer may reasonably rely.

(b) In each case, Yaskawa is not liable for (i) the slightly negligent breach of duties arising from the duties that are not *Essential Contractual Duties*, as well as (ii) force majeure, i.e. external events that have no operational connection and cannot be averted even by exercising the utmost care that can reasonably be expected.

(2) The aforementioned limitation of liability does not apply (i) in cases of mandatory statutory liability (in particular under the product liability law), (ii) if and to the extent that Yaskawa has assumed a guarantee or same as guaranteed procurement risk according to § 276 BGB, (iii) for culpably caused injuries to life, limb and/or health, also by representatives or vicarious agents, as well as (iv) in case of delay in the event of a fixed completion date.

(3) A reversal of the burden of proof is not associated with the provisions above.

Handling of electrostatic sensitive modules

The modules are equipped with highly integrated components in MOS technology. These components are highly sensitive to over-voltages that occur, e.g. with electrostatic discharge. The following symbol is used to identify these hazardous modules:

The symbol is located on modules, module racks or on packaging and thus indicates electrostatic sensitive modules. Electrostatic sensitive modules can be destroyed by energies and voltages that are far below the limits of human perception. If a person who is not electrically discharged handles electrostatic sensitive modules, voltages can occur and damage components and thus impair the functionality of the modules or render the modules unusable. Modules damaged in this way are in most cases not immediately recognized as faulty. The error can only appear after a long period of operation. Components damaged by static discharge can show temporary faults when exposed to temperature changes, vibrations or load changes. Only the consistent use of protective devices and responsible observance of the handling rules can effectively prevent malfunctions and failures on electrostatic sensitive modules.

Shipping of modules

Please always use the original packaging for shipping.

3.2 Mounting

The plug-in card must be installed in a robot controller with a PCI Express slot. The mounting procedure can be found in the corresponding robot controller manual.

3.3 Device replacement and repair

Device replacement

When replacing a device, all communication settings must be made again. Information on the demounting procedure can be found in the corresponding robot controller manual.

Device repairs and defects

Repairs may only be carried out by Yaskawa.

- Always contact your national representative of Yaskawa before returning the product.
- Return defective products to the national representative of Yaskawa for repair or to obtain a replacement device.
- Always use the original packaging when returning the product.

Disposal

National rules and regulations apply to the disposal of the device!

3.4 Industrial security in information technology

Latest version

This chapter can also be found as a guide *'Industrial IT Security'* in the *'Download Center'* of www.yaskawa.eu.com

Hazards

The topic of data security and access protection has become increasingly important in the industrial environment. The increased networking of entire industrial systems to the network levels within the company together with the functions of remote maintenance have all served to increase vulnerability. Hazards can arise from:

- Internal manipulation such as technical errors, operating and program errors and deliberate program or data manipulation.
- External manipulation such as software viruses, worms and trojans.
- Human carelessness such as password phishing.

Precautions

The most important precautions to prevent manipulation and loss of data security in the industrial environment are:

- Encrypting the data traffic by means of certificates.
- Filtering and inspection of the traffic by means of VPN - "Virtual Private Networks".
- Identification of the user by "Authentication" via save channels.
- Segmenting in protected automation cells, so that only devices in the same group can exchange data.
- Deactivation of unnecessary hardware and software.

Further Information

You can find more information about the measures on the following websites:

- Federal Office for Information Technology ➦ *www.bsi.bund.de*
- Cybersecurity & Infrastructure Security Agency ➦ *us-cert.cisa.gov*
- VDI / VDE Society for Measurement and Automation Technology ➦ *www.vdi.de*

3.4.1 Protection of hardware and applications

Precautions

- Do not integrate any components or systems into public networks.
  - Use VPN "Virtual Private Networks" for use in public networks. This allows you to control and filter the data traffic accordingly.
- Always keep your system up-to-date.
  - Always use the latest firmware version for all devices.
  - Update your user software regularly.
- Protect your systems with a firewall.
  - The firewall protects your infrastructure internally and externally.
  - This allows you to segment your network and isolate entire areas.
- Secure access to your plants via user accounts. *'User Authentication'...page 61*
  - If possible, use a central user management system.
  - Create a user account for each user for whom authorization is essential.
  - Always keep user accounts up-to-date and deactivate unused user accounts.
- Secure access to your plants via secure passwords.
  - Change the password of a standard login after the first start.
  - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
  - Change the passwords according to the rules and guidelines that apply to your application.
- Consider possible defence strategies when planning and securing the system.
  - The isolation of components alone is not sufficient for comprehensive protection. An overall concept is to be drawn up here, which also provides defensive measures in the event of a cyber attack.
  - Periodically carry out threat assessments. Among others, a comparison is made here between the protective measures taken and those required.
- Use secure access paths such as HTTPS or VPN for remote access to your plant.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.

3.4.2 Protection of PC-based software

Precautions

Since PC-based software is used for programming, configuration and monitoring, it can also be used to manipulate entire systems or individual components. Particular caution is required here!

- Use user accounts on your PC systems.
  - If possible, use a central user management system.
  - Create a user account for each user for whom authorization is essential.
  - Always keep user accounts up-to-date and deactivate unused user accounts.
- Protect your PC systems with secure passwords.
  - Change the password of a standard login after the first start.
  - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
  - Change the passwords according to the rules and guidelines that apply to your application.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.
- Protect your PC systems by security software.
  - Install virus scanners on your PC systems to identify viruses, trojans and other malware.
  - Install software that can detect phishing attacks and actively prevent them.
- Always keep your software up-to-date.
  - Update your operating system regularly.
  - Update your software regularly.
- Make regular backups and store the media at a safe place.
- Regularly restart your PC systems. Only boot from storage media that are protected against manipulation.
- Use encryption systems on your storage media.
- Perform security assessments regularly to reduce the risk of manipulation.
- Use only data and software from approved sources.
- Uninstall software which is not used.
- Disable unused services.
- Activate a password-protected screen lock on your PC systems.
- Always lock your PC systems as soon as you leave your PC workstation.
- Do not click any links that come from unknown sources. If necessary ask, e.g. on e-mails.
- Use secure access paths such as HTTPS or VPN for remote access to your PC system.

3.5 Licensing information for open source software

- The plug-in card works with a Linux operating system.
- You can access license information for the individual Linux packages in Web-based management (WBM) via the *'Legal Information '* button. *'Web-based management - WBM'...page 38*
- Every open source software that is used in the product is subject to the respective license conditions, which are not affected by the Yaskawa software license conditions (**S**oftware **L**icense **T**erms - SLT) for the product.
- The licensee can change the respective open source software in accordance with the applicable license terms.

Notes on OpenSSL

- *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (➥ http://www.openssl.org/).*
- *This product includes cryptographic software written by Eric Young (➥ eay@cryptsoft.com).*

3.6 Reset to factory settings type 1

Please note that Reset to factory settings type 1 resets all settings of the plug-in card to their default values. This also applies to all settings made via the WBM.

After resetting to factory settings type 1, the plug-in card has the following communication settings:

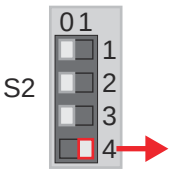
- Communication via PROFINET is activated.
  - X1/X2 (default: 192.168.3.1, *'MAC2'*): PROFINET device
  - X3/X4 (default: 192.168.1.1, *'MAC1'*): PROFINET IO controller
- Communication via EtherCAT is deactivated.
- *'Web-based management - WBM'...page 38* can be reached via:
  - X1/X2 (default: 192.168.3.1, *'MAC2'*)
  - X3/X4 (default: 192.168.1.1, *'MAC1'*)

With DIP switch S2

DIP switch S2 *'Switches'...page 15* can be used to *Reset to factory settings type 1* according to the following procedure.

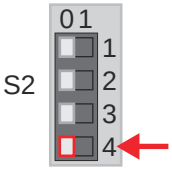
1. Switch off the power supply of the plug-in card.

> **CAUTION**
>
> When switching off the power supply of the plug-in card, the higher-level system must also be switched off. Please observe the procedures and safety instructions in the associated documentation!



2. Set the DIP switch S2-4 to position 1 (ON).
3. Switch on the power supply of the plug-in card again.
   ➡ The plug-in card is reset to its default settings.
4. As soon as the LEDs show the following behavior, switch off the power supply to the plug-in card:

SYS	COM0	COM1	Description
☐	◪ green 2Hz	◪ green 2Hz	Power cycle requirement.



5. Set DIP switch S2-4 to position 0 (OFF).
6. Switch on the power supply of the plug-in card again.
   ➡ The plug-in card now works with the standard settings.

With WBM

Via the toolbar of *'Cockpit'...page 41*, you can *Reset to factory settings type 1* according to the following procedure.

1. Click in the Toolbar at .
   ➡ The plug-in card is reset to its default settings.
2. As soon as the LEDs show the following behavior, switch off the power supply to the plug-in card:

SYS	COM0	COM1	Description
☐	◪ green 2Hz	◪ green 2Hz	Power cycle requirement.

3. Switch on the power supply of the plug-in card again.
   ➡ The plug-in card now works with the standard settings.

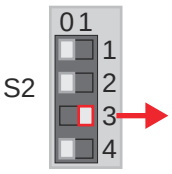
3.7 Firmware update

You can only run a firmware update of the plug-in card via 'Web-based management - WBM'...page 38.

'Firmware Update'...page 64

3.8 Safe Mode

Start-Up in *Safe Mode*

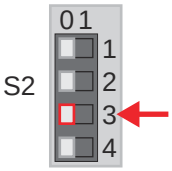


By means of the DIP switch S2 *'Switches'...page 15* you can start your plug-in card in *Safe Mode*. In safe mode, the plug-in card starts with the following behavior:

- Communication via PROFINET is deactivated.
- Communication via EtherCAT is deactivated.
- You can only communicate with the plug-in card via *'Web-based management - WBM'...page 38*. Access is only possible via the default IP addresses.
  - X1/X2 (default: 192.168.3.1, *'MAC2'*)
  - X3/X4 (default: 192.168.1.1, *'MAC1'*)
- The current firmware version remains unchanged.

1. Switch off the power supply of the plug-in card.
2. Set DIP switch S2-3 to position 1 (ON).
3. Switch on the power supply of the plug-in card again.
   ➡ The plug-in card starts in *Safe Mode*.

Start-up in *Standard Mode*



1. Switch off the power supply of the plug-in card.
2. Set DIP switch S2-3 to position 0 (OFF).
3. Switch on the power supply of the plug-in card again.
   ➡ The plug-in card starts in *Standard Mode*.

4 Deployment with PROFINET

4.1 Deployment as PROFINET IO controller

PLCnext Technology

- The plug-in card is based on PLCnext Technology ® from Phoenix Contact.
- The plug-in card works with a Linux operating system.
- The integrated PROFINET IO controller can only be configured with 2CON.

Firewall

- *On delivery the firewall at the plug-in card is disabled!*
- *Security recommendation: Enable the firewall!*
- *In the WBM, you can enable the firewall at 'Security → Firewall'.*
  'Firewall'...page 56
- *Please note that you only have access to the firewall settings as an administrator!*

4.1.1 Install 2CON

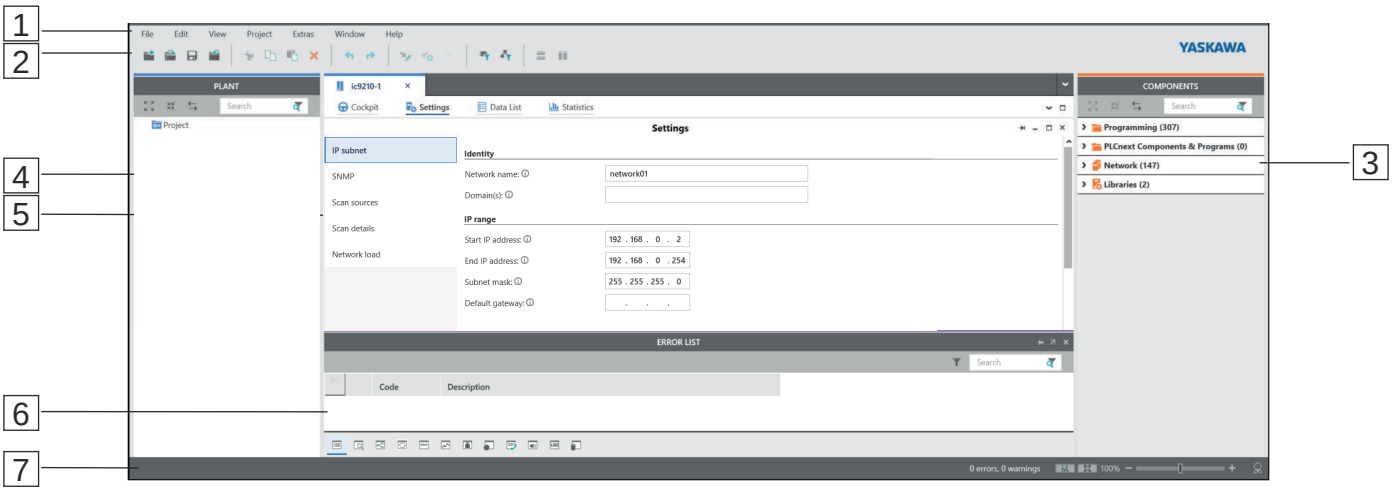
Installation

To use the PROFINET IO controller the software 2CON is required.

1. Download the software 2CON to your PC. You can find this at www.yaskawa.eu.com in the *'Download center'*.
2. Unzip the file in your working directory and start the installation by double-clicking on the exe file.
3. Follow the instructions of the installation wizard.
   ➡ The installation is started.
4. When prompted, restart your system.
   ➡ The installation is finished. You can start 2CON now.

4.1.2 2CON user interface

Overview



1 Menu bar
2 Toolbar
3 *'Components'* area
4 *'Plant'* area
5 Editor area
6 Cross-functional area
7 Status bar

Menu bar

The menu bar provides access to a number of project-related commands that do not explicitly relate to a specific engineering task.

Toolbar

The menu bar provides access to a number of project-related commands that do not explicitly relate to a specific engineering task. In addition, the various areas and editors have their own specific toolbars.

***'Components'* area**

The *'Components'* area contains all components available for the project. The components can be divided into the following types based on their function:

- Develop program code (data types, programs, functions and function blocks).
- Show or add all devices available for the *'Plant'* area.
- Insert libraries such as firmware libraries, IEC user libraries, etc.

***'Plant'* area**

In the *'Plant'* area, you map all the physical and logical components of your application as a hierarchical tree structure.

Editor area

- Double-clicking on a node in the *'Plant'* area or on an element in the *'Components'* area opens the associated editor group in the editor area.
- Editor groups are always shown in the center of the user interface.
- Each editor group contains several editors, which can be opened and closed using buttons in the editor group.
- You can identify the corresponding editor based on the color representation of the editor group:
  - Blue: Editor from the area *'Plant'*.
  - Orange: Editor from the area *'Components'*.

Cross-functional area

The cross-functional area contains functions that extend across your entire project.

- All errors, warnings and messages of the current project are shown here.
- Items that you have recently deleted from the *'Plant'* or *'Components'* areas are moved to the recycle bin. If necessary, you can restore deleted items.

You can find more information on this in the corresponding online help of 2CON.

Status bar

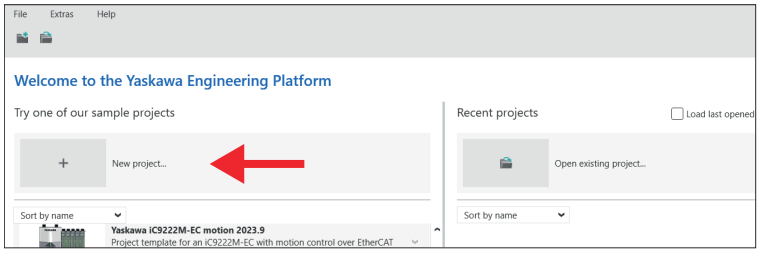
Detected errors and warnings are shown here. In addition, you have a zoom function here for graphical applications.

4.1.3 Configuration

4.1.3.1 Create a new project

Proceeding

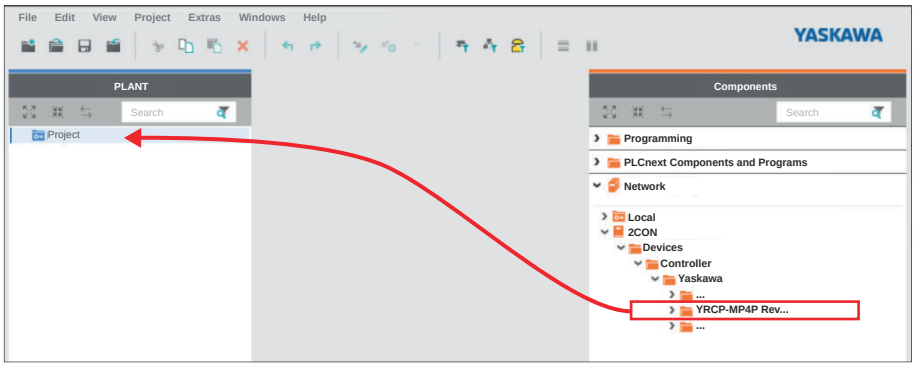
1. Start 2CON.



2. Click on *'New project...'*.

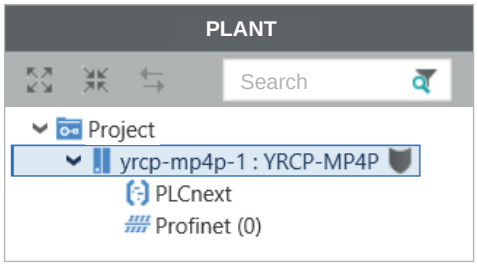
   ➡ An empty project template opens.

3. In *'Components'* area navigate via *'Network'* to the YRCP-MP4P... plug-in card, which corresponds to the hardware respectively firmware version. *'Specific informations* 3 *'...page 10*



4. Drag the selection to *'Project'* in the *'Plant'* area.

   ➡ The selected plug-in card is added to the project.



5. Open *'File → Save Project As'*, assign a meaningful name to your project and close the dialog with [Save].

   ➡ The project for the plug-in card is saved.

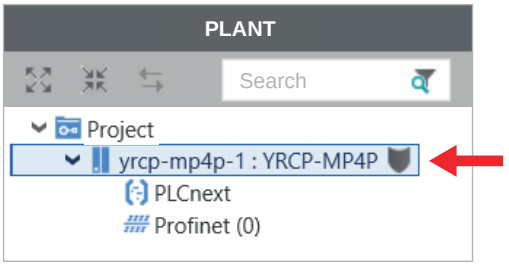
4.1.3.2 Online access to the plug-in card

IP address parameters for communication

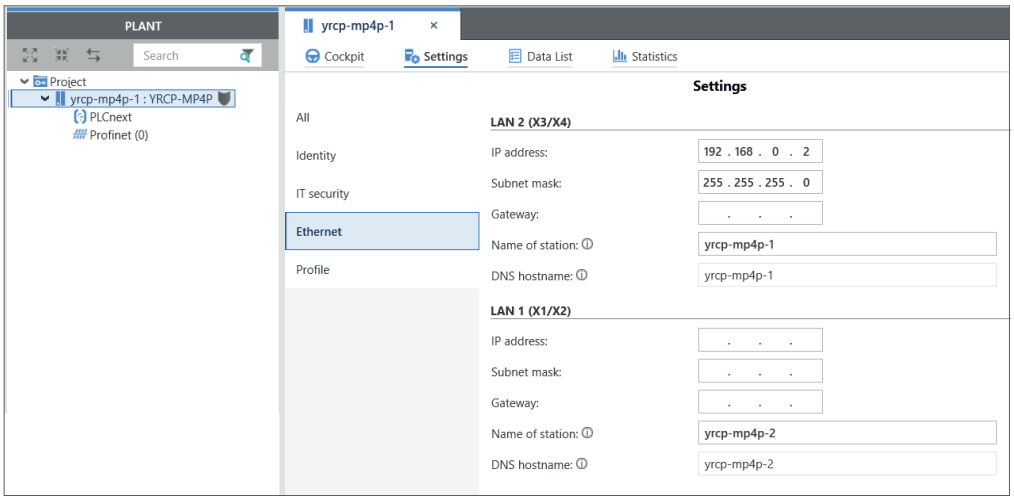
On delivery, the plug-in card has the following access parameters for online access:

- X1/X2 (default: 192.168.3.1, *'MAC2'*): PROFINET device
- X3/X4 (default: 192.168.1.1, *'MAC1'*): PROFINET IO controller
- X1/X2/X3/X4: Access to *'Web-based management - WBM'...page 38*
- Subnet mask: 255.255.255.0
- Gateway: -

For online access from 2CON, you can adjust the IP address parameters using the following procedure:



1. In the *'Plant'* area, double-click the plug-in card node.
   ➡ The plug-in card editor group opens.
2. Select the *'Settings'* editor.
3. Select the *'Ethernet'* view.

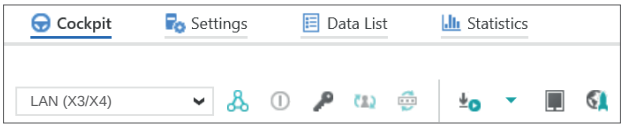


4. At *'LAN ...'*, enter the IP address parameters for the connection via the corresponding Ethernet port (X...).
   ➡ When establishing an Ethernet connection to the plug-in card, the IP address parameters specified here are used by 2CON for the corresponding interface.

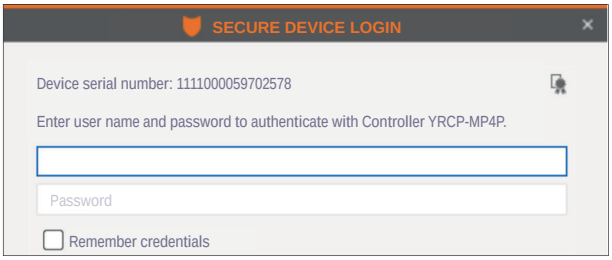
Connecting to the plug-in card

Connect for example port X3 or X4 to the Ethernet interface of your PC. Please note that for communication via 2CON the network card of the PC and the Ethernet interface of the plug-in card are in the same IP circle. If necessary, contact your network administrator.

1. In the editor group of the plug-in card, select the editor *'Cockpit'*.
2. Set the interface *'LAN (X3/X4)'* and click on .



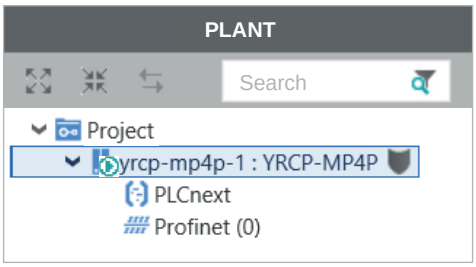
➡ A connection between 2CON and your plug-in card is established, by means of the IP address parameters, and the login dialog for authentication is opened.



3. Enter your login details and click on .

- *By default user authentication is enabled. On delivery, the "Admin" user is already created with administrator rights.*
- *Please note that by disabling the user authentication you endanger the security of your system against unauthorized access!*
- *The administrator password, labelled 'PW:', is located on the plug-in card.* *'Specific informations 3'...page 10*
- *Only use the administrator password for the initial login to the WBM.*
- *After you have successfully logged in, you should change the administrator password for security reasons.*

➡ Now you can access your plug-in card. An existing connection is shown in the *'Plant'* area at the node of the plug-in card by .

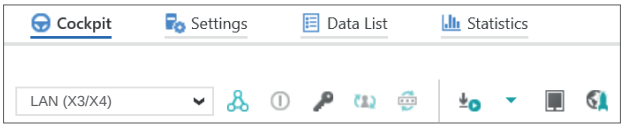


4.1.3.3 Assigning new IP address parameters

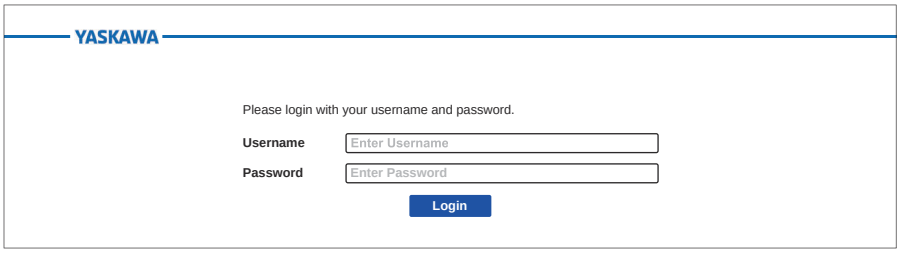
Assignment via WBM

As soon as you are online connected to the plug-in card, you can assign new IP address parameters to it via WBM (Web-based management).

1. To access WBM, click in the *'Cockpit'* editor at .



➡ The WBM login page opens.



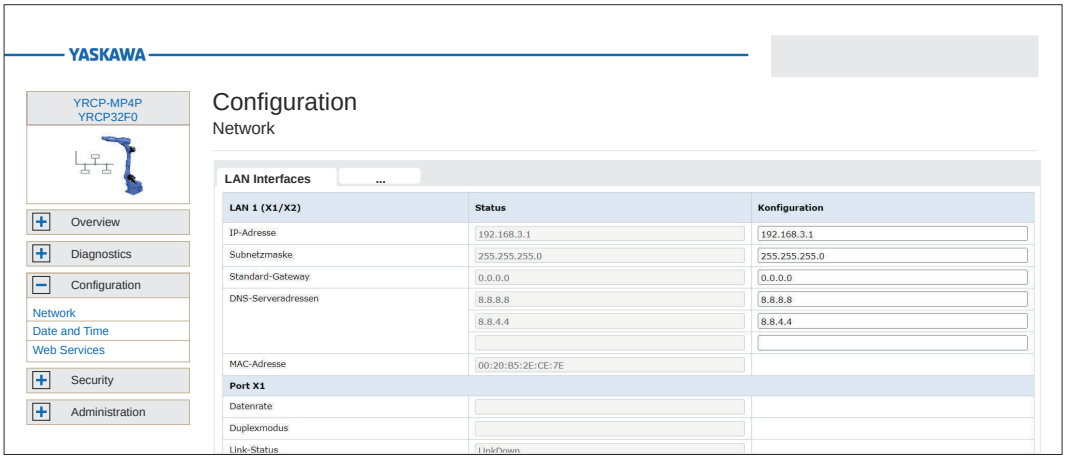
2. Enter your login details and click on [Login].

- *By default user authentication is enabled. On delivery, the "Admin" user is already created with administrator rights.*
- *Please note that by disabling the user authentication you endanger the security of your system against unauthorized access!*
- *The administrator password, labelled 'PW:', is located on the plug-in card. 'Specific informations 3'...page 10*
- *Only use the administrator password for the initial login to the WBM.*
- *After you have successfully logged in, you should change the administrator password for security reasons.*

➡ You now have access to the WBM of the plug-in card with the access rights assigned to you.

3. Navigate to Network in the Configuration area.

➡ Here you can change the current IP address parameters in the *'Configuration'* column.



4. Enter your new IP address parameters in the *'Configuration'* column.

CAUTION

When assigning the IP address parameters, please note that the number ranges of the IP addresses of X1/X2 and X3/X4 must not overlap if they exist!

5. Click on [Apply and Reboot].

➡ The settings are accepted, transferred to the plug-in card and the plug-in card is automatically restarted for activation.

The plug-in card can now only be reached via the new IP address parameters. Please note that these new data are currently not automatically transferred in the settings of 2CON. You have to manually adjust these in the settings there.

Further information on configuring the PROFINET IO controller and integrating it into your PROFINET network can be found in the online help of 2CON.

4.2 Deployment as PROFINET device

Overview

- The *PROFINET device* functionality allows data to be exchanged with a higher-level PROFINET IO controller.
- The PROFINET device is to be connected to a PROFINET IO controller as an IO device via X1/X2 (default: 192.168.3.1, *'MAC2'*).
- For configuration in a PROFINET IO controller, you can find the corresponding *'GSDML-V...-YASKAWA-YRCP-MP4P-....xml'* in the *'Download Center'* of www.yaskawa.eu.com.
- To communicate via PROFINET, you have to assign a name to your PROFINET device. This is done via the engineering tool of the higher-level PROFINET IO controller.

For more information, please refer to the manual of your higher-level PROFINET IO controller.

5 Deployment with EtherCAT

5.1 Designations

MainDevice (MDevice)

The MDevice is the central control unit under EtherCAT. It assumes the role of the higher-level device that coordinates the communication process and sends commands to the connected SubDevices.

SubordinateDevice (SubDevice)

The SubDevice is a lower-level device under EtherCAT. This receives the instructions from the MDevice and reacts accordingly. YRCP32F0 is a SubDevice.

5.2 Deployment as EtherCAT SubDevice

Overview

- For configuration in an EtherCAT MainDevice, you will find the corresponding *'ESI-V...-YASKAWA-YRCP-MP4P-....xml'* in the *'Download Center'* at www.yaskawa.eu.com. Install these in your EtherCAT configuration tool.
- By means of the user API activate EtherCAT communication in your robot controller for X1/X2.
- The connection to a higher-level EtherCAT MainDevice takes place via X1: EtherCAT port - SubDevice IN.
- The connection to a subsequent EtherCAT SubDevice takes place via X2: EtherCAT port - SubDevice OUT.
- Set the required PDO sizes. Only the PDO sizes listed in the *'Technical data'...page 17* are supported.

For more information, please refer to the manual of your higher-level EtherCAT MainDevice.

6 Web-based management - WBM

6.1 Overview and first steps

Accessing WBM

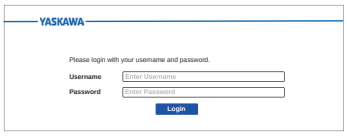
- The plug-in card has a web-based management (WBM). In the WBM you can access static and dynamic information and change certain settings. You may access WBM via the Ethernet interfaces of the plug-in card.
- You may only access WBM if the plug-in card has a valid IP address.
- In the delivery state, the plug-in card has the IP addresses:
  - X1/X2 (default: 192.168.3.1, *'MAC2'*)
  - X3/X4 (default: 192.168.1.1, *'MAC1'*)

1. For the initial commissioning, establish a secure connection between the configuration PC and plug-in card, such as a point-to-point connection via Ethernet.
2. You can use the 2CON search to determine the IP address of the corresponding Ethernet interface.

   To do this, navigate to *'PROFINET'* at 2CON in the *'Plant'* area and select *'Online devices'*.
3. Open the web browser on your configuration PC.
4. Enter the URL in the address field such as https://192.168.1.1

   ➡ For secure communication the web server uses a self-signed TLS certificate that is automatically generated by the plug-in card during the commissioning. Due to the system, you will receive a security message regarding the certificate, as it has not yet been installed on the configuration PC. After logging in, you can install the corresponding certificate of the plug-in card at configuration PC as a trusted certificate (see below). This authenticates the plug-in card to the web browser on the configuration PC.
5. Take note of the security message and only continue if there is a secure connection between configuration PC and plug-in card and no third parties can access it!

   ➡ The WBM login page opens.



6. Enter your login details and click on [Login].

   - *By default user authentication is enabled. On delivery, the "Admin" user is already created with administrator rights.*
   - *Please note that by disabling the user authentication you endanger the security of your system against unauthorized access!*
   - *The administrator password, labelled 'PW:', is located on the plug-in card. 'Specific informations 3'...page 10*
   - *Only use the administrator password for the initial login to the WBM.*
   - *After you have successfully logged in, you should change the administrator password for security reasons.*

   ➡ You now have access to the WBM of the plug-in card with the access rights assigned to you.

Install certificate

First access via TLS certificate

- *During commissioning, the plug-in card generates a TLS certificate during the start-up.*
- *The certificate is used for all Ethernet interfaces of the plug-in card and contains all IP addresses.*
- *When resetting to factory settings, a new certificate is automatically generated.*

To secure communication, the same security certificate should be installed in the configuration PC and on the plug-in card. Otherwise, you will get a warning message. Transfer the generated certificate to your configuration PC with the following proceeding:

1. After logging into the WBM, you can view or respectively adjust the contents of the automatically generated certificate via *'Configuration → Web Services'* and re-generate it with [Re-generate HTTPS certificate]. *'Web Services'...page 50*

   As soon as you change one of the IP addresses of the plug-in card, you must regenerate the certificate via [Re-generate HTTPS certificate].

2. Navigate to the certificates via *'Security → Certificate Authentication'*.
3. Switch to the tab Identity Store.

   ➡ Here you have access to the generated certificate.

4. Load the requested HTTPS certificate onto your configuration PC with . Here you can also transfer your own existing HTTPS certificate to the plug-in card. *'Certificate Authentication'...page 53*
5. Install the certificate according to your operating system as a trusted root certification authority. For this, please contact your system administrator.

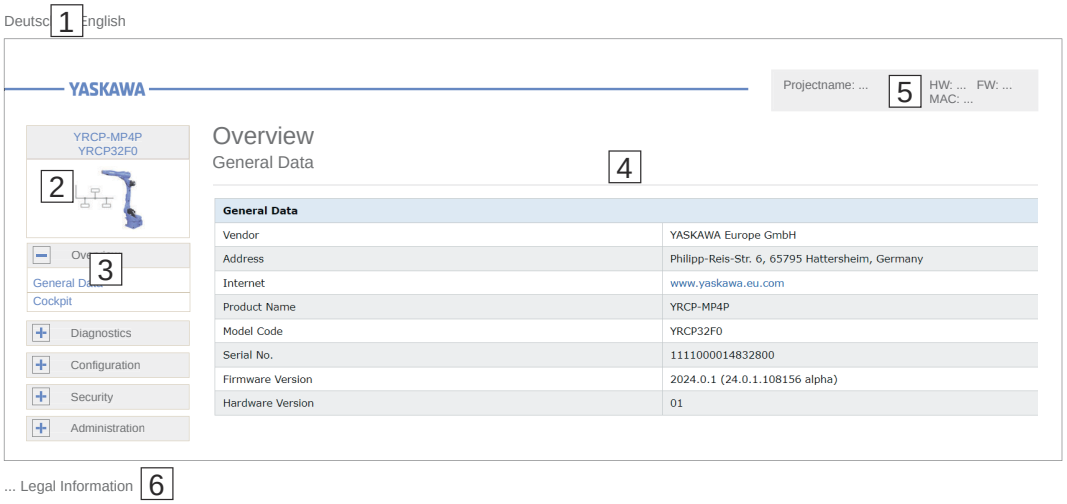
   ➡ After installation, communication between the configuration PC and plug-in card takes place as a *'secure connection'*.

CAUTION

If the communication between configuration PC and plug-in card is declared as an *'insecure connection'* during operation, either the certificate has changed, e.g. due to an IP address change, or your system has been compromised by third parties! Always make sure that either the current certificate of the plug-in card or, if available, an associated higher-level certificate is installed on the configuration PC!

Structural design

The WBM is divided into the following areas:

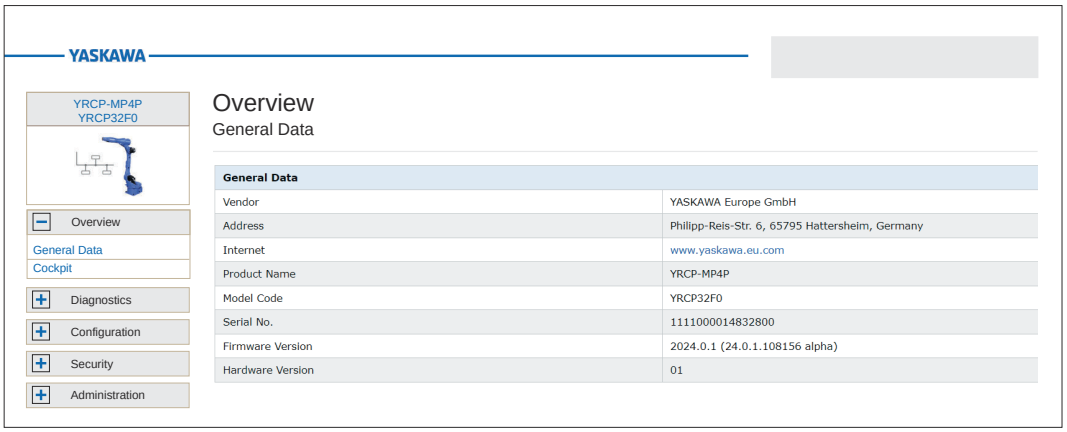


1 Language switching between *'German'* and *'English'*.
2 Symbol image of the robot controller with type and order designation.
3 Menu column for navigation.
4 Area for information output and input dialogs
5 Shows project name (if exists), current hardware/firmware version and MAC address of the plug-in card.
6 Access to the Yaskawa software license conditions (**S**oftware **L**icense **T**erms - SLT) and the license information for the individual Linux packages.

6.2 Overview

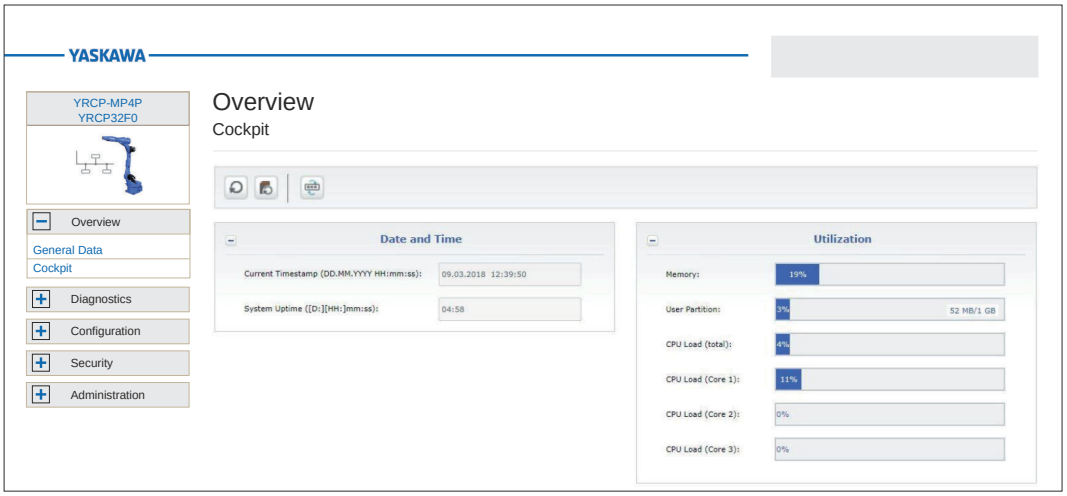
6.2.1 General Data

Here you will find general details about the plug-in card, e.g. hardware and firmware versions, order number as well as vendor information.



6.2.2 Cockpit

Here you will find the Cockpit toolbar and information about the time, status and utilization of the plug-in card.



Cockpit toolbar

The toolbar provides access to the following functions:

- : Reboot - Restars the plug-in card. The operation corresponds to a power off/on process. The plug-in card restarts with the last saved settings.
- : Reset - Executes *'Reset to factory settings type 1'...page 27* on the plug-in card. Here, all communication settings are reset to default settings.
- : Change Password - This allows you to change the password of the current user account for online access to the plug-in card.

> *Please note that Reset to factory settings type 1 resets all settings of the plug-in card to their default values. This also applies to all settings made via the WBM.*

Date and time

The current system time is shown via Current time stamp. System uptime shows the current runtime since PowerON. Date and time are set via *'Date and Time'...page 48*.

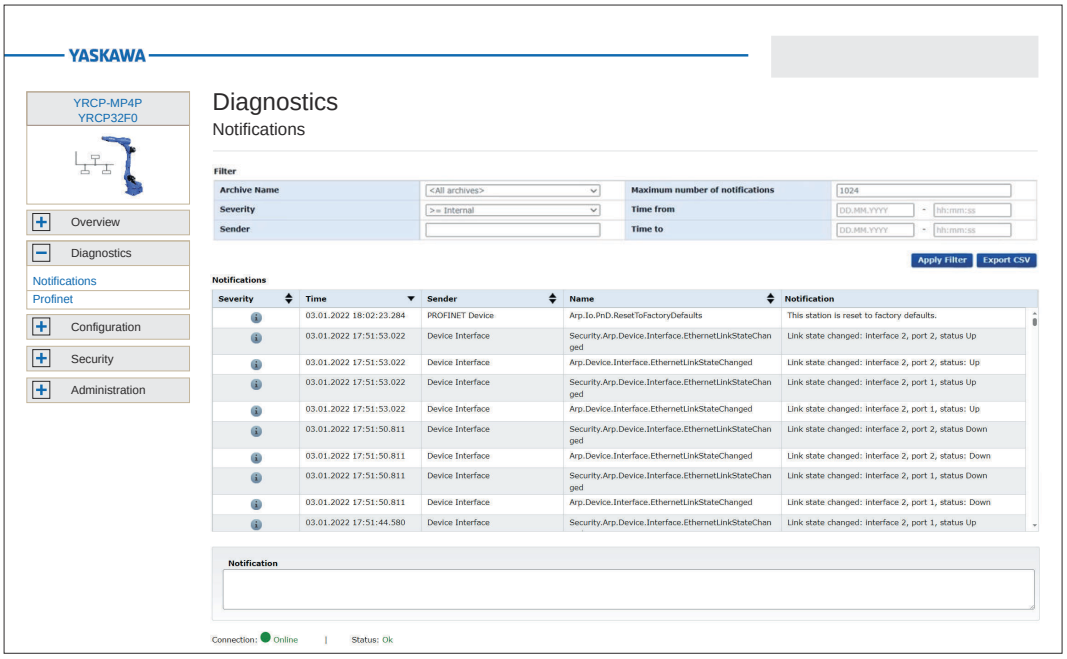
Utilization

CPU memory utilization and the CPU load are shown here.

6.3 Diagnostics

6.3.1 Notifications

Every user with access rights can view and download message entries here. The page contains buttons for filter functions and for the CSV export of the messages, as well as an overview table of all messages and a full text area of a selected message. This information is refreshed once a second.



Sort criteria for the message entries

By default, the message entries in the table are sorted in descending order based on the time stamp. To sort the notifications, click on the header of the corresponding table column. The arrows at the column headings have the following meaning:

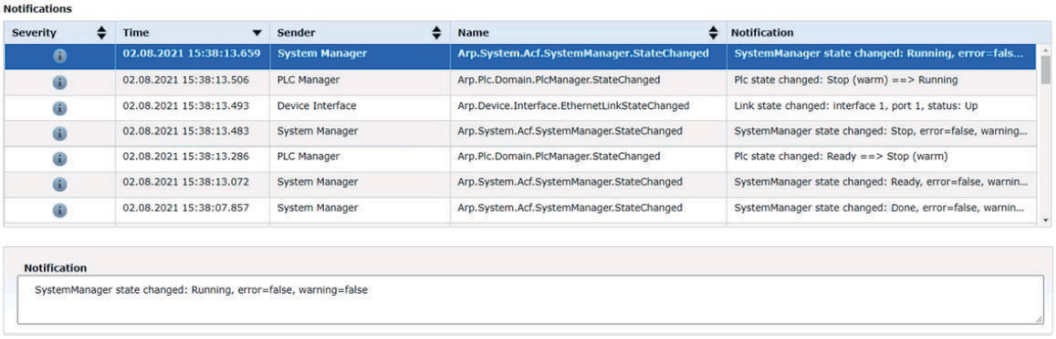
Double arrow ▲▼ - The table is not sorted by this column.

Up arrow ▲ - The table is sorted according to this column in ascending order.

Down arrow ▼ - The table is sorted according to this column in descending order.

Full text view

Below the table is the full text view of a selected message entry in the table. If no message is selected, the full text view remains empty.



Filter functions

Specify the filter settings. By clicking on [Apply Filter], the previously made filter settings are activated and the table with the message entries is refreshed accordingly.

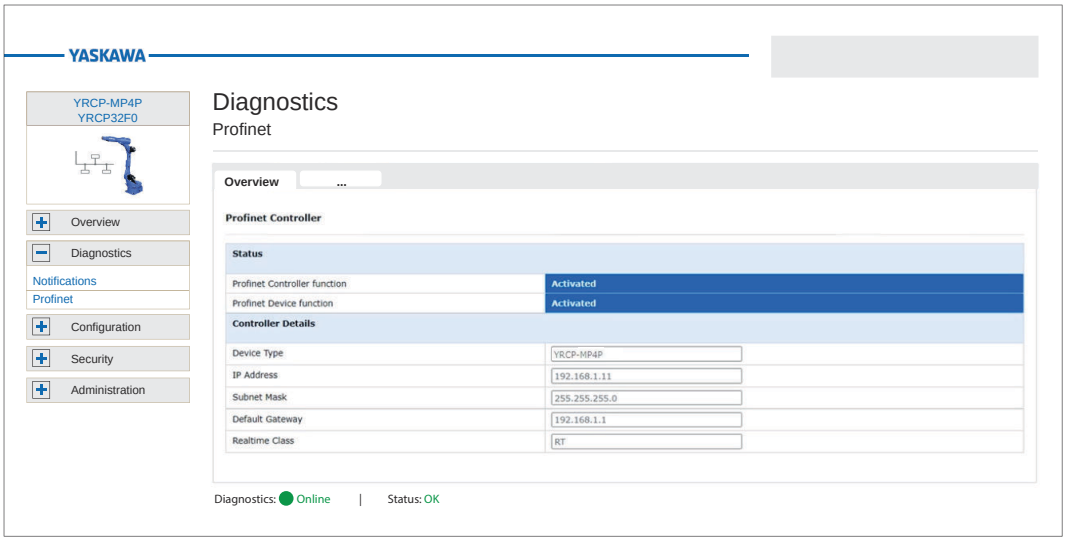
There are the following filter options:

- Archive name
  - Here you can filter the message entries by specifying an archive name.
- Severity
  - Here you can limit the message entries based on their severity.
  - The limitation is based on the following graduation for the minimum severity:
    Internal → *Information* → *Warning* → *Error* → *Critical Error* → *Fatal Error*
    For example with *Internal*, all degrees of severity are listed. With the setting *Error*, all *Error*, *Critical Error* and *Fatal Error* are listed.
- Sender
  - Here you can limit the message entries by entering or selecting a sender in the selection field.
  - The currently list of message entries is always decisive for the names in the selection field.
  - When entering a name or part of the name, click on [Apply Filter] to list messages from senders that match or partially match the name you are looking for.
- Maximum number of notifications
  - Here you can limit the number of message entries to be listed.
  - 1024 is set by default, a maximum of 4000 is allowed.
- Time from, Time to
  - Here you can limit the period of the message entries by entering the date and time.
  - Time from: Lists all message entries that are not older than the specified time.
  - Time to: Lists all message entries that are older than the specified time.
  - When filtering by time specification, a date must always be entered and a time can be added.

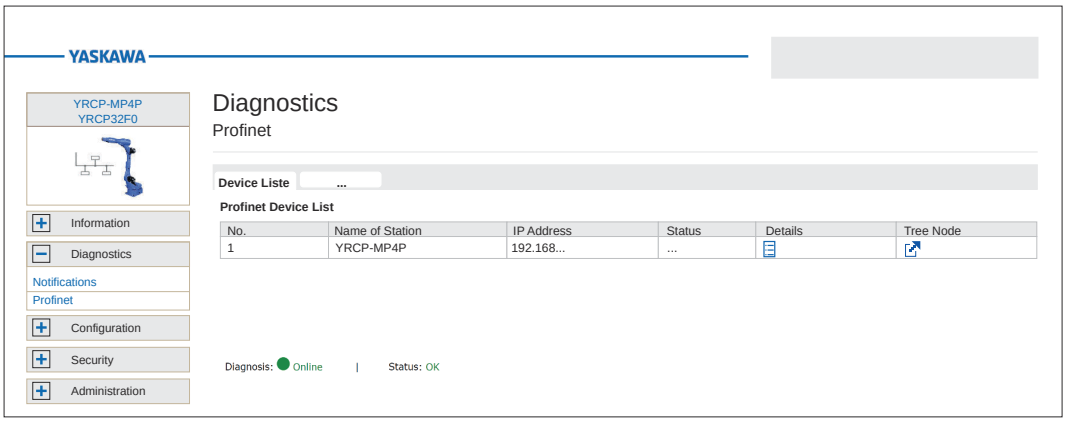
6.3.2 PROFINET

Tab: *'Overview'*

Here you will find information on the current PROFINET function of the controller and its IP settings.



Tab: *'Device List'*



Open the WBM of a PROFINET device

→ To access the WBM of a PROFINET device, click on the corresponding PROFINET device in the Device Name column.

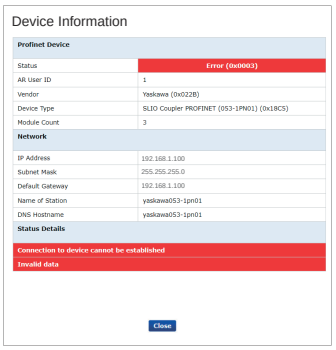
➡ The WBM of the PROFINET device opens in a new tab in the web browser.

Open Details

For the corresponding PROFINET device, you will find information on IP settings and diagnostics at Details. This information is refreshed once a second.

→ To show the Device Information of a PROFINET device click in Details column on .

➡ The Device Information view with the current information on IP settings and diagnostics is opened.



Open Tree Node

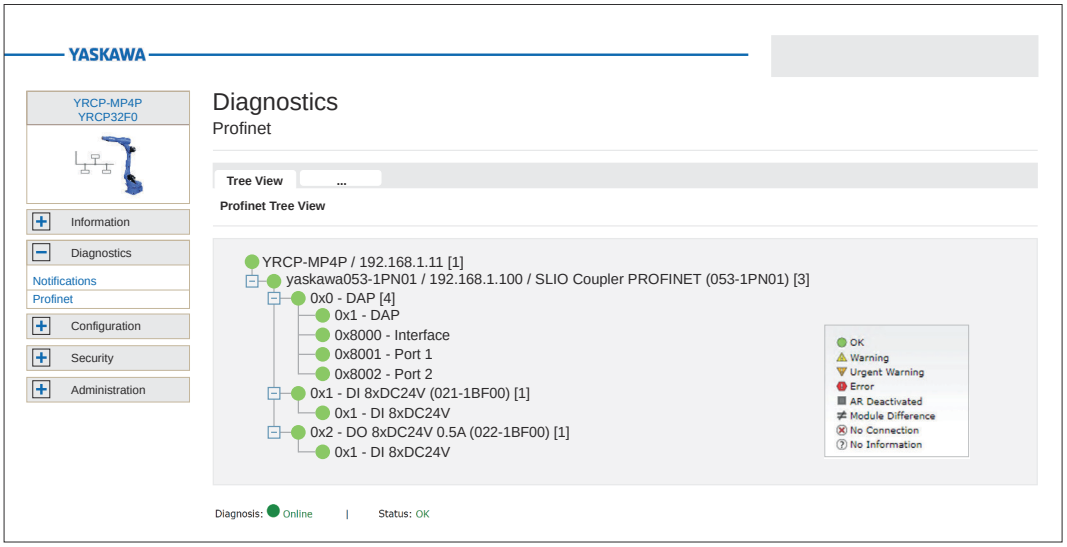
For the corresponding PROFINET device, you will find the associated view of the tree node at Tree Node. This information is refreshed once a second.

→ To show the tree node of a PROFINET device, in the Tree Node click on .

➡ The Tree View of the selected device is opened.

Tab: *'Tree View'*

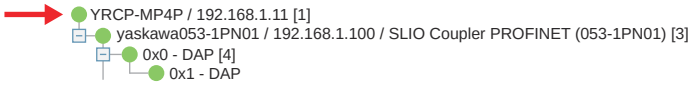
Here you have a tree view of all configured PROFINET devices. The overview contains the device names of the PROFINET devices, their current IP settings and the diagnostic status of the devices and modules. Via [+] and [-] you can open or close the next level of the Tree View.



Controller level

On the PROFINET controller level you will find the following information:

- Controller designation
- IP address of the controller
- Number of PROFINET devices



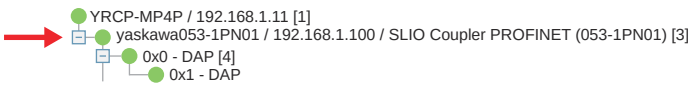
Station level

On station level you will find the following information about the PROFINET devices:

- Station name
- IP address of the station
- Station designation
- Number of connected modules

The following symbols inform about the diagnostic state of the PROFINET device:

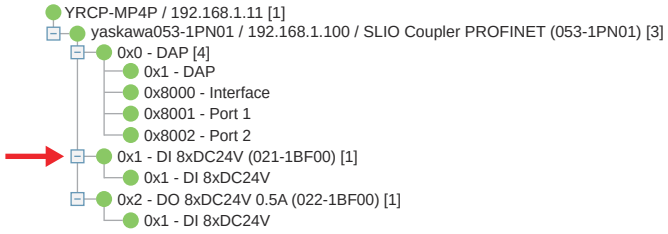
Symbol	Diagnostic status
	OK
	Warning
	Error



Module level

On module level you will find the following information:

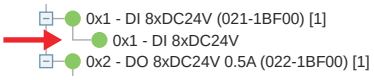
- Slot number
- Module designation
- Number of sub modules



Sub module level

On sub module level you will find the following information:

- Sub module number
- Sub module designation



6.3.2.1 PROFINET Diagnostics Code

Here you can get the status of a connection with an IO controller (Application Relation - AR) bit-coded.

Status AR

Bit	Description and action recommendation
0	Bit 0 is set when there is no connection. ■ The PROFINET IO controller could not establish a connection with the PROFINET device or the AR was deactivated. – Please check the Ethernet connection and the PROFINET device name with your 2CON configuration tool. – Also check whether the AR was deactivated in the device settings of PROFINET.
1	Bit 1 is set if the data is invalid. ■ The PROFINET device is connected to the PROFINET IO controller, but the process data were marked as invalid due to an error. The process data were not transferred to the process image. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
2	Bit 2 is set when a diagnostic message is pending. ■ The PROFINET device reports a diagnosis. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
3	Bit 3 is set if the module deviates from the configured module. ■ When the PROFINET connection was initialized, a discrepancy was found between the target and current configuration. – Please check the configuration of the PROFINET device. In the 2CON default setting, the connection remains established in the event of a configuration difference.
4	Bit 4 is set when the AR is disabled. ■ The PROFINET device is configured in the project, but the AR was disabled. – Check the PROFINET device settings and enable the AR.

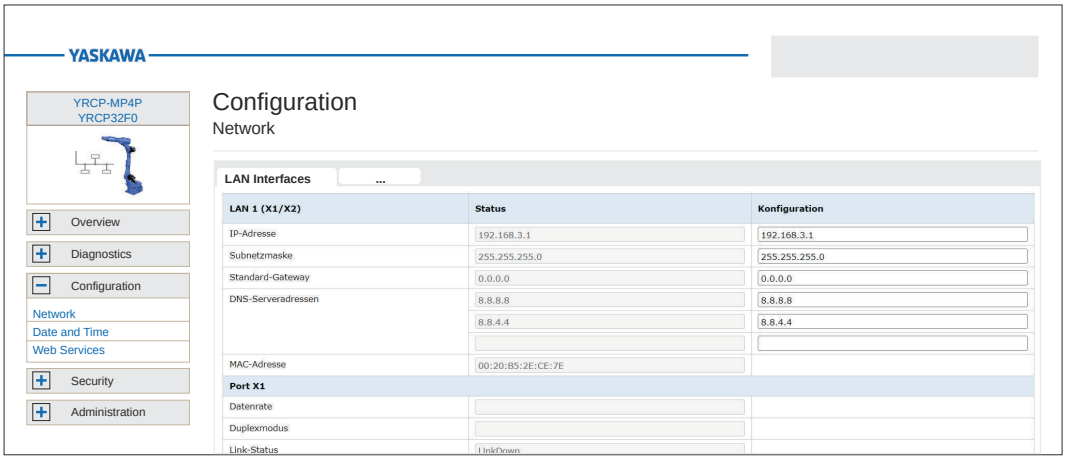
Bit	Description and action recommendation
5	Bit 5 is set if no neighbor information is available. ■ No neighbor information are available in the network used. – This is usually due to the use of components that are not at least compatible with PROFINET Conformance Class-B (CC-B). For a stable PROFINET network, you should only use CC-B or CC-C-compliant PROFINET devices.
6	Bit 6 is set if neighbor information are not uniform. ■ Neighbor information are available in the network used, but not clearly. This means that more than two PROFINET devices can be detected on a port by at least one switch. This is not permitted and may result in the automatic device change not working reliably. – This is usually due to the use of components that are not at least PROFINET Conformance Class-B (CC-B) compatible (e.g. unmanaged switches).
7	Bit 7 is set if the alias name of a device being searched for is already being used by an AR. ■ A DCP identification request (alias) was sent to the network. However, the alias of a device being searched for is already being used by an AR. – This information is only an indication that the control program is probably trying to establish a connection with a device, although a connection is still active.
8	Bit 8 is set when a maintenance request is pending. ■ The PROFINET device has transmitted a maintenance request (maintenance alarm). – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
9	Bit 9 is set when a high-priority maintenance demand is pending. ■ The PROFINET device has transmitted a high-priority maintenance request (maintenance alarm). – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
10	Bit 10 is set if a vendor- or channel-specific diagnosis is pending. ■ The PROFINET device has transmitted a vendor- or channel-specific diagnosis. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.

6.4 Configuration

6.4.1 Network

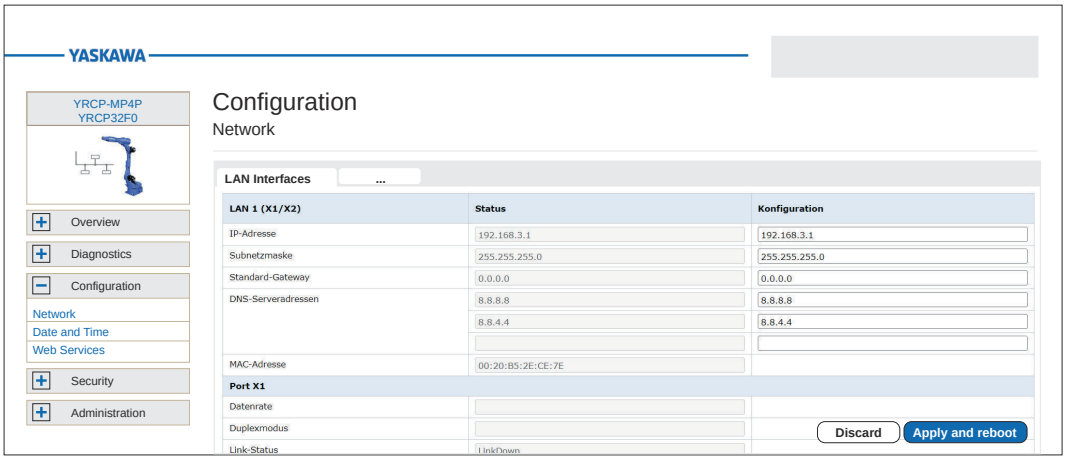
User with read permission

Here you can view the Ethernet settings of your plug-in card.



User with write permission

If you are logged in with administrator rights, you can view the Ethernet settings of your plug-in card here. You can also change the current network settings in the *'Configuration'* column.



To change the network settings, proceed as follows:

1. Enter your new settings in the *'Configuration'* column.
2. Click on [Apply and Reboot].

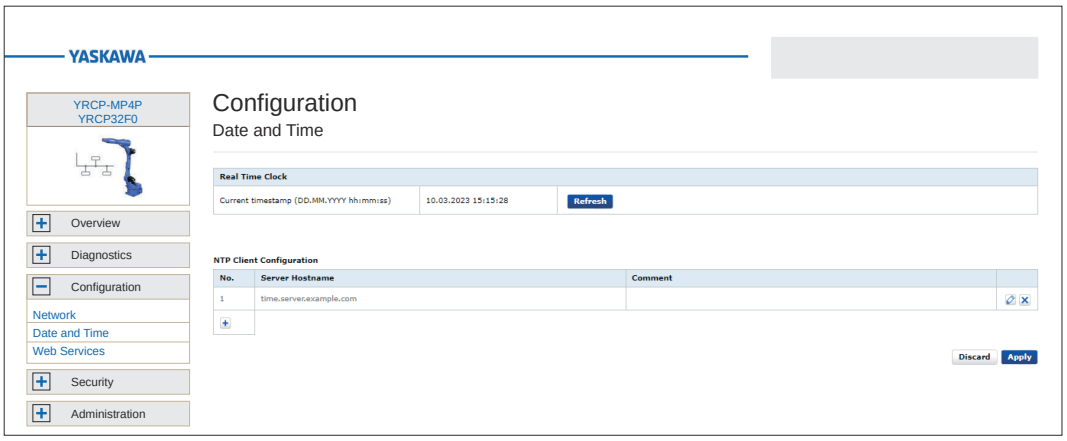
   ➡ The settings are adopted, transferred to the plug-in card and the plug-in card is automatically restarted for activation.

You can also configure the network settings via 2CON. For more details, please refer to the corresponding online help.

6.4.2 Date and Time

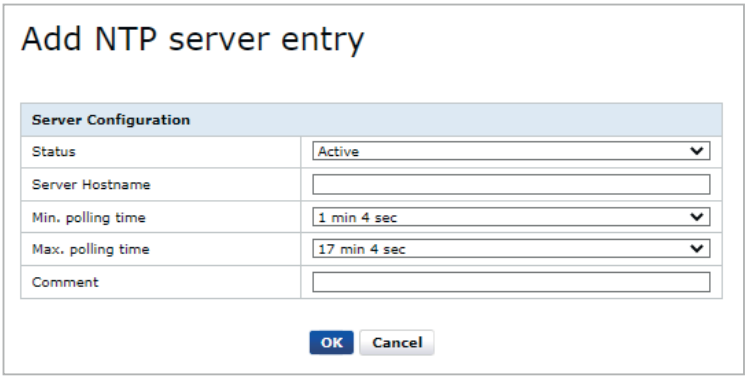
The Date and Time page provides access to the NTP client configuration. NTP stands for **N**etwork **T**ime **P**rotocol and is a standard described in RFC 958 for time synchronisation in end devices connected via a network or the Internet. NTP is based on the connection-less UDP protocol (port 123). For synchronisation, NTP relies on Coordinated Universal Time (UTC), which is obtained from the individual clients and servers in a hierarchical system.

The plug-in card uses UTC0 as the default setting, which corresponds to the coordinated world time UTC ±00:00.



Here you can configure the NTP client by adding new NTP server entries.

1. To do this, click below the table on +.
   ➡ The dialog for adding an NTP server opens.



2. Enter the according parameters.
   - Server Hostname
     - Enter the IP address at which the NTP server can be reached in the network.
   - Min. polling time and Max. polling time
     - Specify the range within which the time should be synchronized with the NTP server with the aim to achieve high accuracy with the lowest possible network load. The preset values are standard values.
   - Comment
     - Here you can assign an internal designation for the NTP server.
3. Click at [OK].
   ➡ The dialog is closed and the NTP server is listed in the table.
   You can remove entries with × and edit them with ✎ .
4. Click on [Apply].
   ➡ You will receive a message that applying the new NTP daemon configuration requires a restart of the NTP daemon and that this may lead to a real-time violation. With [OK], the NTP servers listed in the table are accepted for time-of-day synchronization and the NTP daemon is restarted.

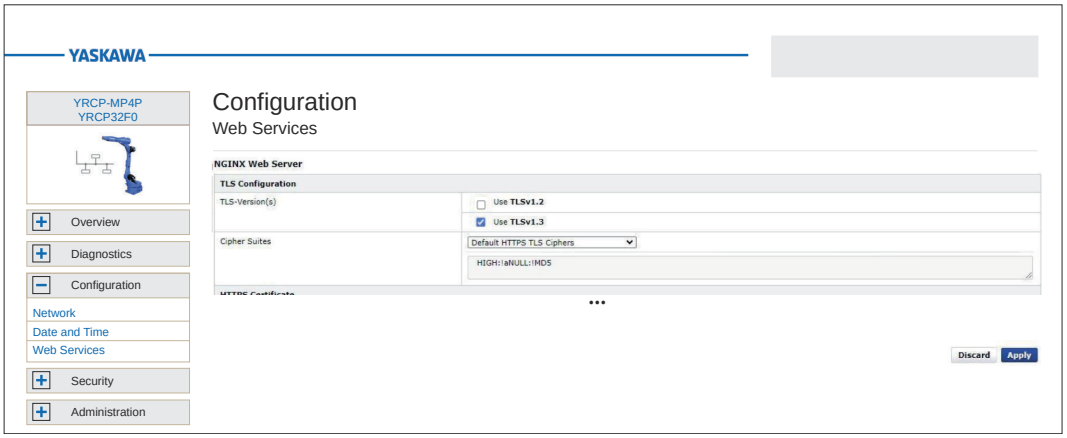
6.4.3 Web Services

The page provides access to the configuration of web services, e.g. HTTPS certificate, which is used for the NGINX web server.

The HTTPS certificate and the associated private key are located as files in the file system of the plug-in card and are listed as symbolic links on the web page. During a firmware update, the existing certificate and key files are moved to a backup directory and symbolic links are created that refer to this backup.

6.4.3.1 NGINX Web server

TLS configuration



TLS (**T**ransport **L**ayer **S**ecurity) is an encryption protocol for secure data transmission on the Internet between the user and the web page. The following procedure is used in the NGINX configuration:

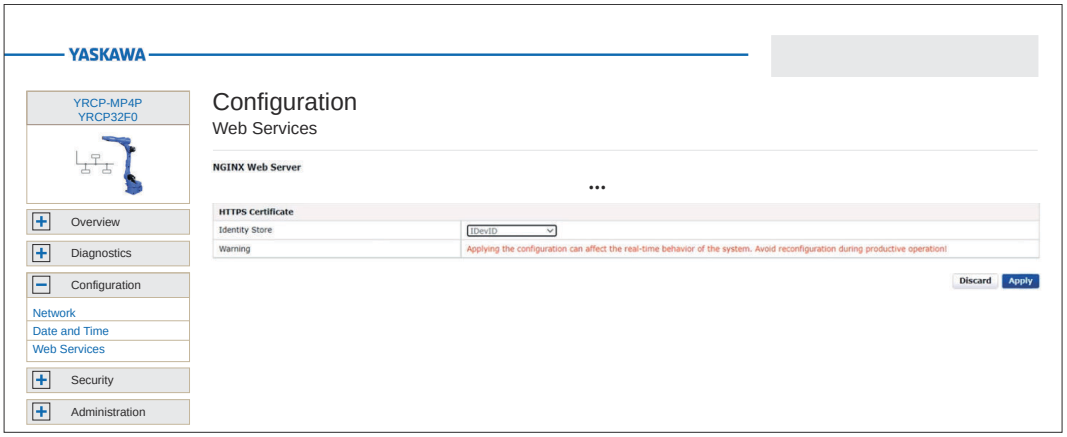
1. Activate *'TLSv1.3.'*. Always activate one and always the latest TLS version.
2. At *'Cipher suits'*, select a predefined cipher collection.
3. Click on [Apply].

➥ TLS is used for authentication in the configuration.

Please note that reconfiguring the web service can affect the real-time behavior of your system. Avoid this during productive operation.

Selected HTTPS certificate

The HTTPS certificate is used to authenticate the plug-in card to the web server.

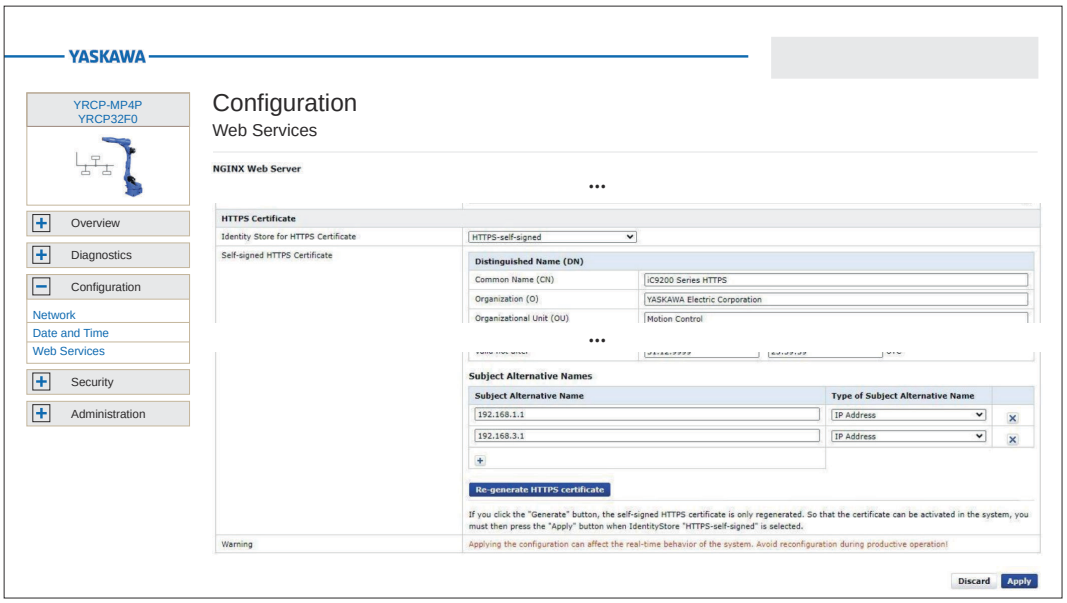


In the configuration table for the NGINX Web server you have the option of selecting the HTTPS certificate from one of the identity stores stored in the plug-in card.

1. Select the corresponding Identity store.
   ➡ The corresponding HTTPS certificate is selected.
2. Click on [Apply].
   ➡ The certificate is used for authentication in the configuration.

Please note that reconfiguring the web service can affect the real-time behavior of your system. Avoid this during productive operation.

Self-signed HTTPS certificate



In addition to the HTTPS certificates stored in the plug-in card, you also have the option of selecting a self-signed certificate created by the firmware.

1. To do this, select in the selection field *'HTTPS-self-signed'*.
   ➡ The configuration of the self-signed HTTPS certificate is listed in a table. You can adapt these accordingly and generate new certificate files with [Apply].
2. Enter the according parameters.
   - Distinguished name
     - Enter your company information here for identification.
   - Validity
     - Enter the date in the format DD.MM.YYYY and the time in hh:mm:ss.
     - If at *'Valid not before'* the input field is empty, the current date is used.
     - If at *'Valid not after'* the input field is empty, the date 31.12.9999 and time 23:59:59 are used.
   - Subject alternative names
     - The IP addresses from the network configuration of the plug-in card are suggested by default.
     - You have the option of expanding or adapting this or specifying a DNS name. Use ⊕ to add an entry. Use ⊗ to remove an entry.

   If the web server is to be accessible via different IP addresses without an error message, you have to specify all IP addresses as Subject alternative names of the type IP address. If the plug-in card can be reached via DNS name, you have also to specify this!
3. To apply the changes, click on [Re-generate HTTPS certificate].
   ➡ The certificate is regenerated. This overwrites an existing self-signed HTTPS certificate.
4. Click on [Apply].
   ➡ The certificate is used for authentication in the NGINX configuration.

Please note that reconfiguring the web service can affect the real-time behavior of your system. Avoid this during productive operation.

6.5 Security

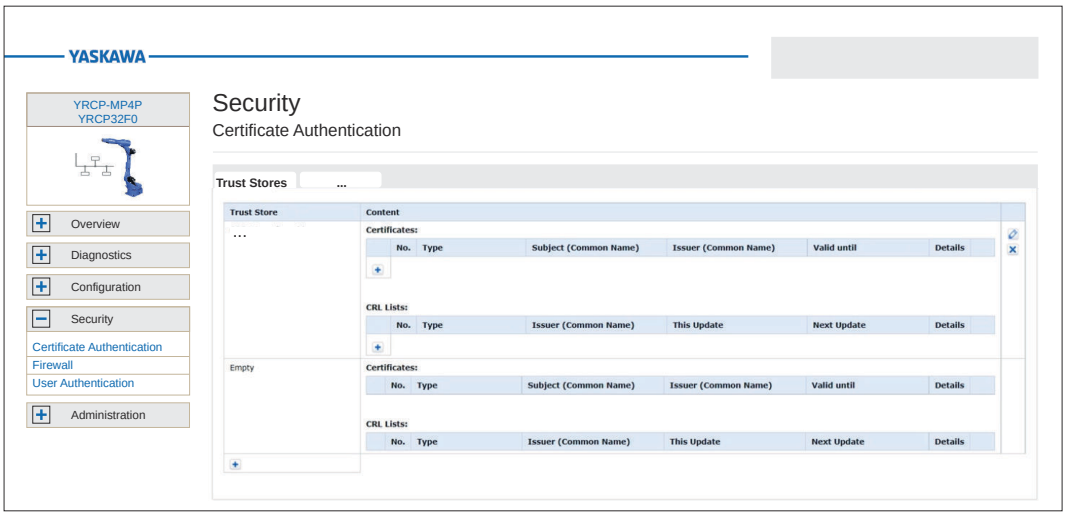
The safety-related settings for the plug-in card must be configured in the *'Security'* area of the WBM.

6.5.1 Certificate Authentication

At *'Certificate Authentication'* you can manage your certificates for secure communication with the plug-in card. *'Certificate Authentication'* is divided into the following tabs:

- Trust Stores
  - Trusted certificates and revocation lists of possible communication partners are stored here.
- Identity Stores
  - The personally created certificates are stored here.

> – *The name for each store can be used with the interfaces for TLS communication.*
> – *The names of the stores are case-sensitive.*



Tab: Trust Stores

Each Trust Store is defined in the WBM by two tables:

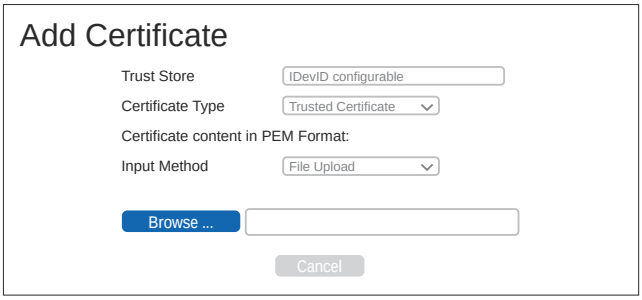
- Table *'Certificates'*
  - In this table you can manage trusted Certificates and issuer certificates.
- Table *'CRL lists'*
  - In this table you can manage the revocation lists for the corresponding Trust Store. By storing untrusted certificates and issuer certificates here.

Creating a Trust Store

1. To create a Trust Store, click the + button at the end of the table.
   ➡ The input dialog opens for entering a name for the Trust Store.
2. Enter a name.
3. Click on [Add].
   ➡ The dialog is closed and the new Trust Store is added.
   You can remove it again with × and rename it with ✎.

Adding a certificate

1. With ⊕ below the table *'Certificates'* you can add a certificate via the dialog.



➡ ■ Trust Store
  – Name of the Trust Store.
  ■ Certificate Type
  – Specify here whether the certificate is trusted or untrusted.
  ■ Certificate in PEM format
  – Certificate files can only be processed in PEM format.
  ■ Input Method
  – Here you can specify the format in which the certificate is to be added.
  – You can choose between text and file (PEM format).

2. To add a certificate in text format, select at *'Input Method'* the *'Text Content'* parameter, enter the text in the input field and click on [Add].

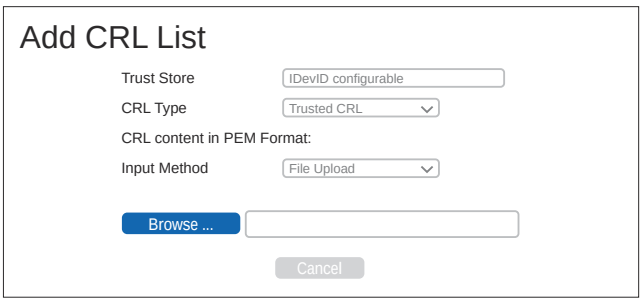
➡ The input dialog is closed and the certificate is added in text format.

3. To add a certificate as file, select at *'Input Method'* the *'File Upload'* parameter, navigate to your certificate in PEM format via [Browse...] and click [Add].

➡ The input dialog is closed and the certificate is added as PEM file.

Adding a revocation list

With ⊕ below the table *'CRL lists'* you can add a revocation list via the dialog.



➡ ■ Trust Store
  – Name of the Trust Store.
  ■ CRL Type
  – Specify here whether the revocation list is trusted or untrusted.
  ■ CRL content in PEM Format
  – Revocation list files can be processed in PEM format only.
  ■ Input Method
  – Here you can specify the format in which the revocation list is to be added.
  – You can choose between text and file (PEM format).

Deleting certificates and revocation lists

1. To delete a certificate or a revocation list, click on the ⊗ button for the relevant certificate or revocation list.
2. In the query dialog click on *'Remove'*.

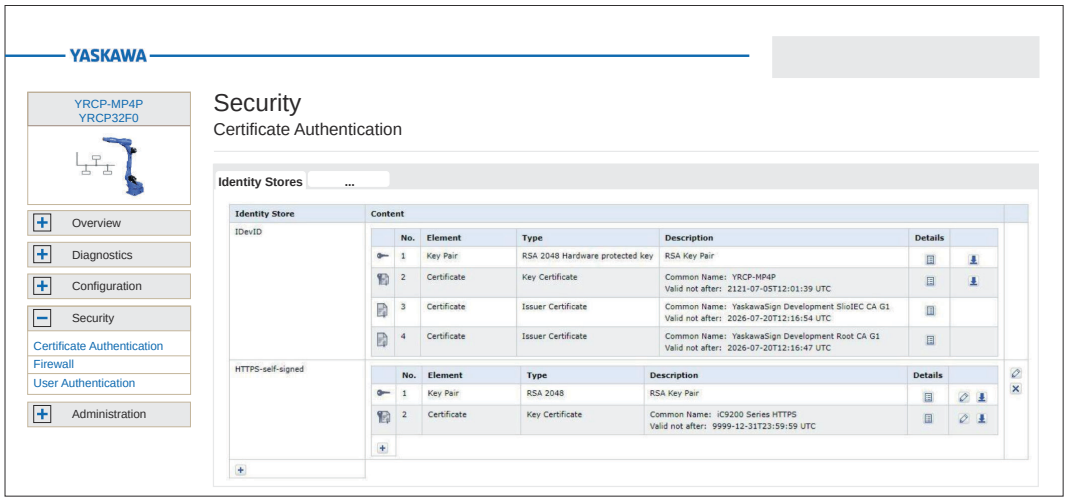
Detail view

The detail views provide detailed information on each certificate and each revocation list:

1. Click on to open the detail view.
   ➡ The detail view is opened.
2. This is closed again with [Close].

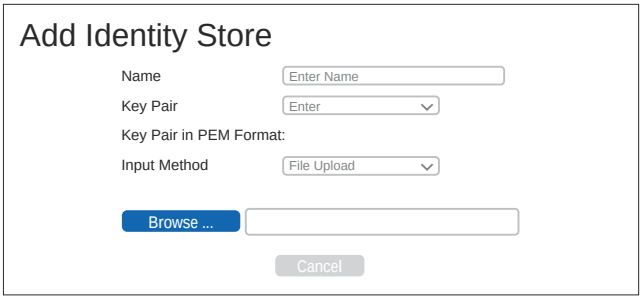
Tab: Identity Stores

- You can create and manage multiple identity stores in the *'Identity Stores'* tab.
- Each Identity Store usually contains an RSA key pair and the corresponding key certificate.
- Optionally, you can add further issuer certificates to an identity store.
- The IDevID identity store is part of the system and is supplied with the plug-in card.



Adding an Identity Store

1. With + below the table *'Identity Store'* you can add a Identity Store via the dialog.



   ➡
   - Name
     - Name for the Identity Store.
   - Key Pairs
     - Specify here how the key pair is to be added.
     - You can enter the key pair or let it be generated.
   - Key Pair in PEM Format
     - Key files can be processed in PEM format only.
   - Input Method
     - Here you can specify the format in which the key pair is to be added.
     - You can choose between text and file (PEM format).
2. To add a key pair in text format, select at *'Key Pairs'* the *'Enter'* parameter and at *'Input Method'* the *'Text Content'* parameter, enter the text in the input field and click on [Add].
   ➡ The input dialog is closed and the key pair is added in text format.

3. To add a key pair as file, select at *'Key Pairs'* the *'Enter'* parameter and at *'Input Method'* the *'File Upload'* parameter, navigate to your certificate in PEM format via [Browse...] and click [Add].

   ➡ The input dialog is closed and the key pair is added as PEM file.

4. To add a key pair generated by the plug-in card, select at *'Key Pairs'* the *'Generate'* parameter, select the encryption method at *'Key Type'* and click on [Add].

   ➡ The input dialog is closed and the key pair, automatically generated by the plug-in card, is added.

You can add, rename, define and remove key pairs or certificates by using the following buttons in the corresponding table entry:

- : New element - adds a new key pair or certificate.
- : Delete element - Deletes by clicking on *'Remove'* the selected key pair respectively certificate or, if selected, the Identity Store.
- : Details - Shows the detailed view of the corresponding element.
- : Download - You can download the public key content of a key pair as a PEM file.
  - If a key certificate is available, you can download it as a CRT file.
  - Save the file in a directory of your choice or open the file directly with a suitable tool.
- : Rename - depending on the position within a table, you can use this to rename the corresponding element.

6.5.2 Firewall

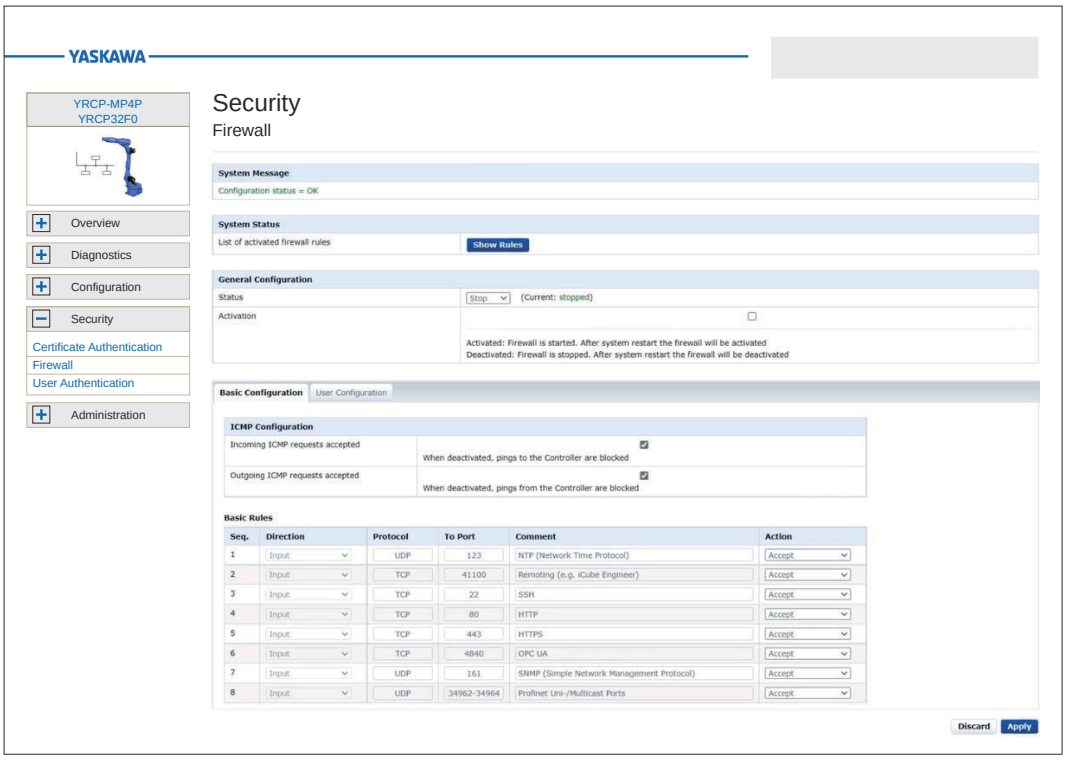
The plug-in card is delivered with a preset firewall. The Linux® firewall *'nftables'* is used here. As described below, you can create rules from predefined basic rules or create your own new ones.

- *On delivery, the firewall is disabled!*
- *Please note that you only have access to the firewall settings as an administrator!*

Accessing the firewall

1. Log in to the WBM as an administrator.
2. Navigate to *'Security → Firewall'*.

   ➡ The configuration page for the firewall is opened.



[Apply] and [Discard]

- The changed firewall settings are transferred to the plug-in card with the [Apply] button.
- With the [Discard] button the settings made are discarded after a security query and the WBM page is reloaded.

'System Message'

Messages regarding the transfer of firewall settings to the plug-in card are shown at *'System Message'*. The following system messages can occur:

- Configuration status = OK
  - The configured firewall settings were successfully transferred to the plug-in card.
- Warning
  - The plug-in card reports a warning, e.g. if one or more additional filter configurations in the system exist. The warning contains the names of all additionally loaded filter tables.
- Error
  - At least one firewall configuration is incorrect.

'System Status'

- When the firewall is enabled, you can use the [Show Rules] button to show an overview of all enabled firewall rules as a txt file.
- With [Save to File] you can save the file locally on your PC as a txt file.

'General Configuration'

At *'General Configuration'* you can see the current firewall status and set it temporarily or permanently.

Temporary enabling

1. Select at *'Status'* the entry *'Start'* or *'Restart'*.
2. Click on [Apply].
   ➡ The firewall is enabled. After restarting the plug-in card, the firewall is disabled again.

Temporary disabling

1. Select at *'Status'* the entry *'Stop'*.
2. Click on [Apply].
   ➡ The firewall is disabled. After restarting the plug-in card, the firewall is enabled again.

Permanent enabling

1. Activate the *'Activation'* selection field.
2. Click on [Apply].
   ➡ The firewall is enabled and remains enabled even after a restart.

Permanent disabling

1. Disable the *'Activation'* selection field.
2. Click on [Apply].
   ➡ The firewall is disabled and remains disabled even after a restart.

By disabling the firewall you endanger the security of your system, especially if it can be reached via the Internet! The firewall should only temporarily be disabled for testing purposes such as troubleshooting.

Configuration

The configuration of the firewall rules is divided into the following tabs:

- Basic Configuration
  - Here you will find predefined firewall rules which you can enable or disable.
- User Configuration
  - Here you can create, enable or disable your own firewall rules according to defined specifications.

There is a *'Action'* column in both tabs. The firewall settings are applied with the [Apply] button. There are the following setting options for the *'Action'* column:

- Accept
  - The corresponding connection and connection request is accepted.
  - The corresponding connection can be established.
- Drop
  - The corresponding connection is interrupted.
  - There is no answer to the corresponding request.
  - The corresponding package is discarded.
- Reject
  - The corresponding connection is rejected.
  - The sender receives a response to the corresponding request.
- Continue
  - The rule is not executed.
  - This can be used e.g., to skip a rule in the *'Basic Configuration'* and instead create a rule in the *'User Configuration'* and enable it there.

Tab: Basic Configuration

'ICMP Configurations'

- *'Incoming ICMP requests accepted'*
  - enabled: Incoming ICMP echo requests are accepted. The plug-in card can be reached with a ping request.
  - disabled: Incoming ICMP echo requests are blocked. The plug-in card can not be reached with a ping request.
- *'Outgoing ICMP requests accepted'*
  - enabled: Outgoing ICMP echo requests are accepted. Ping requests from the plug-in card are transmitted.
  - disabled: Outgoing ICMP echo requests are blocked. Ping requests from the plug-in card are blocked.

'Basic Rules'

- Here you will find predefined firewall rules for the corresponding incoming connections. You can control their use accordingly via *'Action'*.
- The settings are valid for all Ethernet interfaces. For individual customization, you can instead create a rule in the *'User Configuration'* and enable it there.

Blocking the WBM access

- *On the plug-in card the WBM is accessed via TCP port 443.*
- *By blocking this port with permanently enabled firewall, you have no more access to the WBM of the plug-in card even after a reboot.*
- *Resetting to the factory settings also resets the firewall to its default settings, among others. This way you get access to the WBM of the plug-in card again with the original access data.*

Tab: User Configuration

- In addition or as an alternative to the *'Basic Rules'*, you can define and enable your own user-specific firewall rules for different filter categories.
- You create firewall rules for the output in the *'Output Rules'* tab.
- You create firewall rules for the input in the *'Input Rules'* tab.
- With the order of firewall rules in the table, you define the priority for applying them.
- You can create new rules, delete rules or change the order of the rules by using the following buttons at the end of the table:
  - : New rule - adds a new firewall rule.
  - : Delete rule - deletes the selected firewall rule.
  - : Rule up - moves the rule up.
  - : Rule down - moves the rule down.
- The firewall settings are applied and enabled with the [Apply] button. An existing configuration will be overwritten.

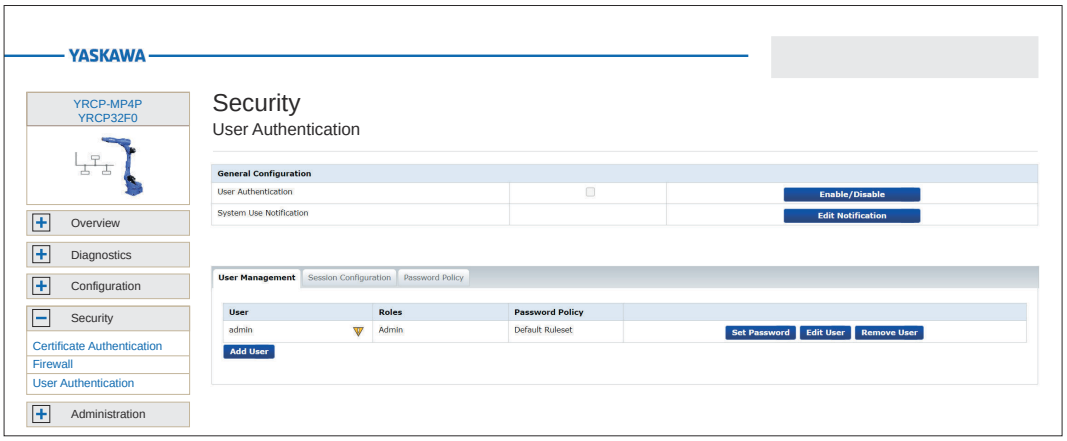
In addition to *'Action'*, there are the following parameters for specifying a firewall rule:

- *'Seq.'*
  - Numbers the order for the priority according to which the firewall rules are applied.
  - The rules are applied in ascending order from 1.
  - With and you can move the firewall rules accordingly.
- *'Interface'*
  - In the *'Input Rules'* tab you can select a single interface from a selection list for which the rule is to be applied.
  - You have no choice in the *'Output Rules'* tab. Here the rule applies to all interfaces.
- *'Protocol'*
  - Specify the protocol for which the rule is to be applied.
- *'From IP'*
  - Enter the IP address for connections that are received from this address.
- *'From Port'*
  - Enter the port for connections that are received via this port.
  - You can specify all ports, selected ports, or a range of values.
- *'To IP'*
  - Enter the IP address for connections that are sent to this address.
- *'To Port'*
  - Enter the port for connections that are sent via this port.
  - You can specify all ports, selected ports, or a range of values.
- *'Comment'*
  - Here you can comment your filter rule accordingly.

6.5.3 User Authentication

- At *'User Authentication'* you can enable or disable user authentication.
- If user authentication is enabled, you have access to definable components of the plug-in card and functions in 2CON exclusively by specifying user name and password.
- If user authentication is disabled, access takes place without a user query. The areas for the administrator remain password-protected.

- *By default user authentication is enabled. On delivery, the "Admin" user is already created with administrator rights.*
- *Please note that by disabling the user authentication you endanger the security of your system against unauthorized access!*
- *The administrator password, labelled 'PW:', is located on the plug-in card. 'Specific informations 3'...page 10*
- *Only use the administrator password for the initial login to the WBM.*
- *After you have successfully logged in, you should change the administrator password for security reasons.*



Enable/disable User Authentication

1. Click the [Enable/Disable] button next to User Authentication.
   ➡ The user authentication dialog is opened.
2. Here you can enable respectively disable the user authentication by selecting or deselecting the checkbox.
3. With [Save] the changes are applied and the dialog is closed.

Changing System Use Notification

Every time you log on to the plug-in card via WBM or 2CON, System Use Notification is shown. You can edit this text for customization. The displayed information is independent of the language used for the user interface. You should therefore take into account all required languages when editing.

1. To edit, click [Edit Notification] next to System Use Notification.
   ➡ The dialog window for editing the text is opened.
2. Adjust your text accordingly.
3. With [Save] the changes are applied and the dialog is closed.

User management

User authentication is used to manage the access data of all users who are authorised to access the plug-in card and to assign the required access authorizations to each user. The user data of the newly created users are stored internally in the plug-in card.

Adding a user

1. Click the [Add User] button.
   ➡ The dialog window for creating a new user is opened.
2. Enter user name and password.

   When assigning user names and passwords, note the length restriction of 127 bytes for passwords and 63 bytes for user names. The characters are encoded with UTF-8 and the number of bytes used depends on which characters are entered. For normal characters (letters a-z or digits 0-9) 1 byte per character is used. Up to 4 bytes per character are used for special characters and umlauts. The length limit therefore limits the number of bytes and not the number of characters.
3. With [Add] the new user is added to the list and the dialog is closed.

Removing a user

1. In the table behind the user entry that you want to remove, click on the [Remove User] button.
   ➡ A security query follows to remove the user entry.
2. With [Remove] the user entry is removed from the table and the dialog is closed.

Change password

1. Click the [Set Password] button in the table behind the user entry whose password you want to change.
   ➡ The dialog window for entering the password for the corresponding user entry is opened.
2. Enter your new password in the 2 input fields.
3. With [Save] the new password for the user entry is applied and the dialog is closed.

Modifying user roles

You can select one or more user roles with different permissions for each user entry. These permissions control access to:

- 2CON
- Web-based management - WBM

1. Click the [Edit User] button in the table behind the user entry whose role you want to change.
   ➡ The dialog window for assigning roles for the corresponding user entry opens.
2. Assign the corresponding roles to the user entry by selecting them.
3. With [Save] the selected roles for the user entry are applied and the dialog is closed.

User roles and their access rights

2CON	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engi-neer	Commis-sioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Cockpit output (e.g. utilization)	✓	✓	✓			✓	✓	✓	✓	✓	✓		
Plug-in card restart (reboot)	✓												
Plug-in card reset (default type 1)	✓												
Read plug-in card status	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Read device information	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Accessing WBM	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engi-neer	Commis-sioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Overview - General Data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Overview - Cockpit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - Notifications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - PROFINET (optional)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Configuration - Network	✓	✓	✓[1]			✓[1]	✓[1]	✓[1]					
Configuration - Date and Time	✓	✓	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]		
Configuration - Web Services	✓	✓											
Security - Certificate Authentication	✓	✓		✓									
Security - Firewall	✓	✓											
Security - User Authentication	✓	✓			✓								
Administration - Firmware Update	✓	✓											

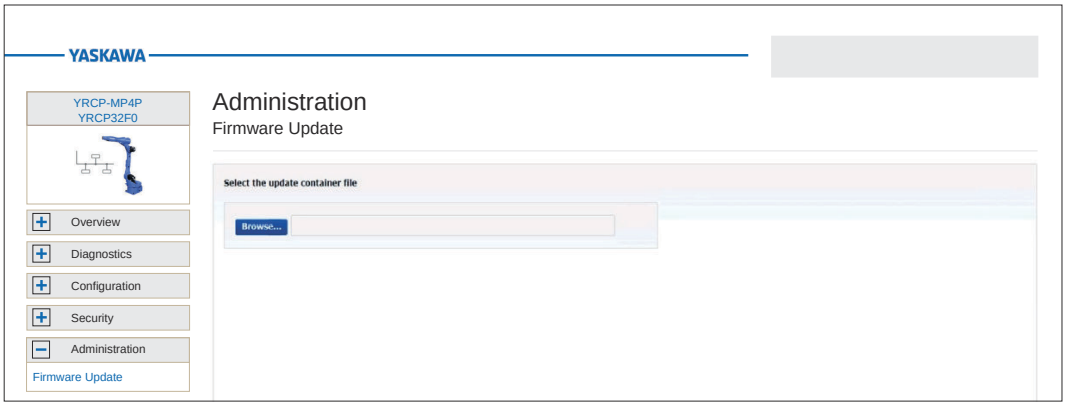
[1]) Read-only access

6.6 Administration

6.6.1 Firmware Update

Here you can execute a firmware update on your plug-in card.

Please note that you can only execute a firmware update with administrator rights!



Proceeding

CAUTION

When installing a new firmware you have to be extremely careful. Under certain circumstances you may destroy the plug-in card, for example if the voltage supply is interrupted during transfer or if the firmware file is defective. In this case, contact our support!

You can find the currently installed firmware version of your plug-in card in the WBM at *'Overview → General Data'*. Here you can also check whether the firmware update was successful. *'General Data'...page 40*

1. The latest firmware can be found in the *'Download Center'* of www.yaskawa.eu.com under the corresponding order number.

   Load the current firmware file into your working directory.

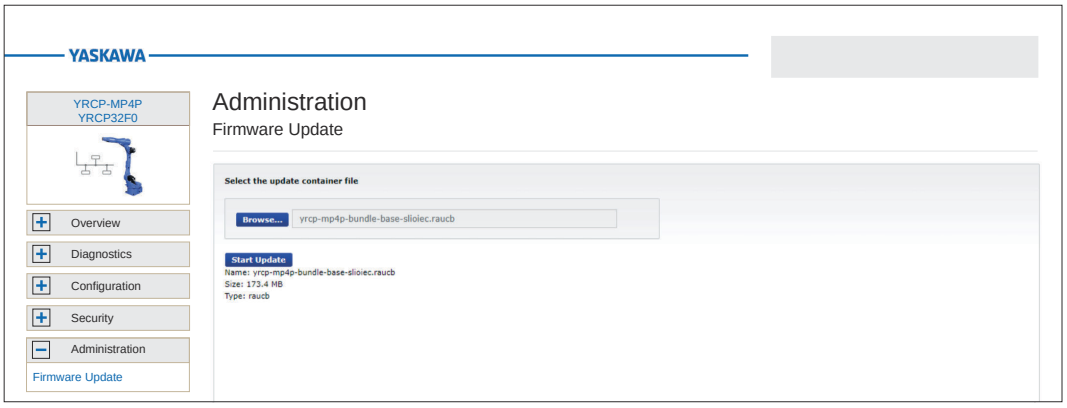
2. Unzip the zip file.

3. Go back to the WBM to *'Firmware Update'* and click on [Browse...].

   ➡ A file selection window is opened.

4. Navigate to the unzipped raucb file and click on [Open].

   ➡ The firmware file to be installed is loaded and shown in the WBM.



5. Click on [Start Update].
   ➡ The firmware file is transferred to the plug-in card and the firmware update is started. The status of the file transfer and the status of the update process are shown in the WBM as a progress bar.
6. The connection to the plug-in card is interrupted during the firmware update. After the start-up of the plug-in card you have to log on to the WBM of the plug-in card again. This will refresh the WBM pages.
7. To check the firmware update, in WBM, go to *'Overview → General Data'* page. *'General Data'...page 40*
   ➡ The new firmware version should be shown here. Otherwise start the update again. If the update does not work, please contact our support.