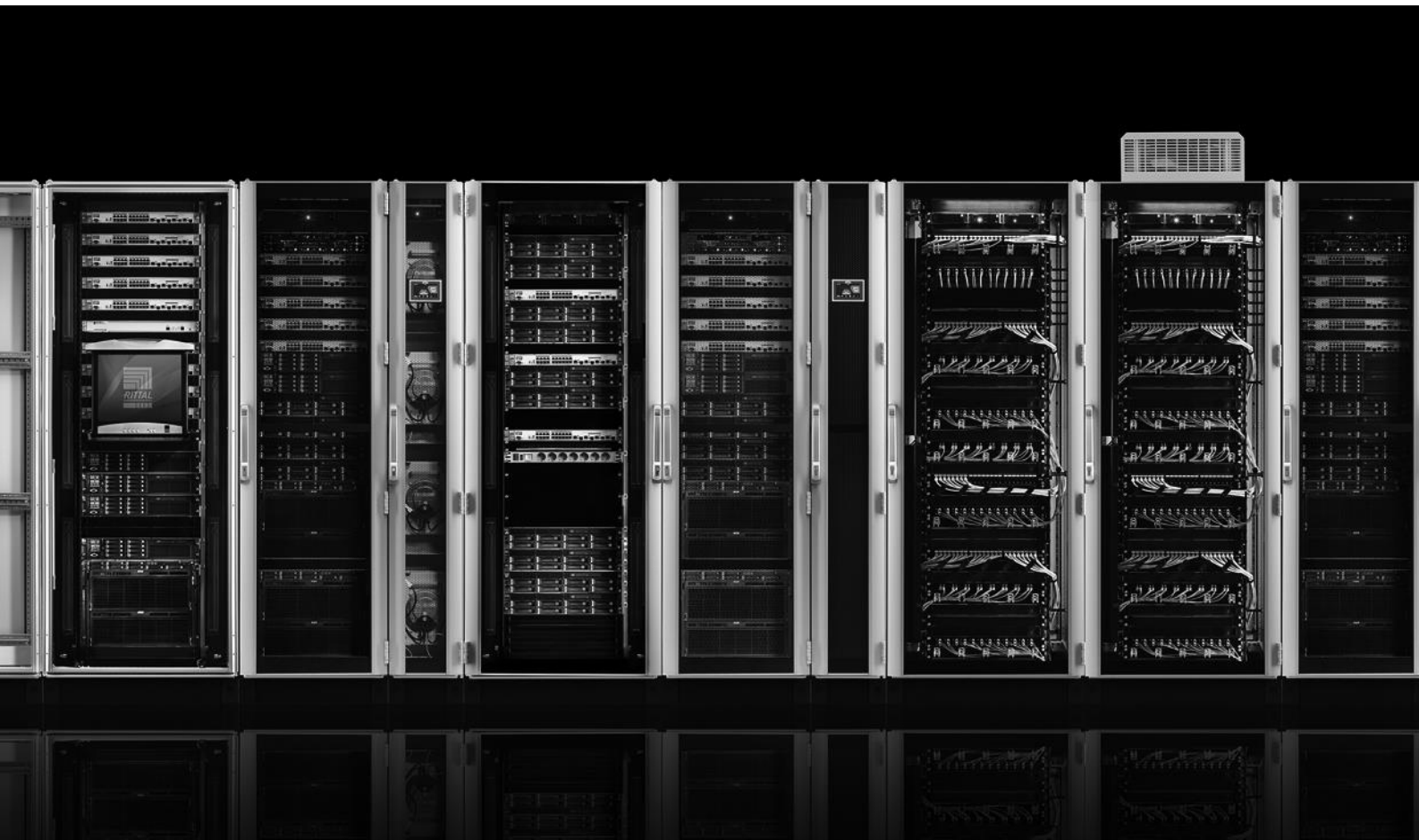


# **Rittal – The System.**

**Faster – better – everywhere.**



## **FAQ – CMC III** **Frequently asked questions**

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



# Table of contents

<b>Table of contents.....</b>	<b>1</b>
<b>Notes on these FAQ – CMC III .....</b>	<b>5</b>
<b>CMC III general .....</b>	<b>6</b>
How many sensors can be connected to each CMC III Processing Unit and CMC III Processing Unit Compact? .....	6
What system characteristics does my computer need in order to be able to operate the CMC III? .....	6
Can I represent multiple CMC III systems on a user interface?.....	6
How can the CMC III data be included in other systems? .....	6
Can the CMC III data also be transferred via BACnet or Modbus? .....	6
Can the messages from several CMC III systems be sent using a single GSM/ISDN unit? .....	7
Is the 3124.200 interface card for cooling units with Comfort controller compatible to the CMC III? .....	7
Can I use a standard CMC III PU for installation in a LCP or in a RiMatrix S? Will modifications need to be made to the firmware? .....	7
Which SD cards and USB sticks can be used?.....	7
Is it possible to connect a camera to the CMC III? .....	7
Which Data Encryption Standard is used for the network communication? .....	8
<b>CMC III software configuration.....</b>	<b>9</b>
How do I define an alarm? The alarming as e-mail or SMS does not function correctly, what can be the reason? .....	9
After selecting a sensor and clicking on "Alarm Configuration", no values for selection are listed in the window. How can I rectify this? .....	10
What is the difference between a "virtual device" and a "task"? .....	11
How many messages can the CMC III store in the logging? .....	11
Can the logging messages be deleted? .....	11
Can a system configuration be saved and recreated on another device? .....	11
How do I save/copy the configuration of a CMC III system onto another system? .....	12
Is it possible to copy a company-own certificate to the CMC III for encrypted communication? .....	12
The Login with Internet Explorer is not possible because the buttons are inactive, although if I use the newest version. Which configurations should be done? .....	13

How should a management software be configured regarding encryption to poll the CMC III over SNMPv3? .....	15
If I cannot see the live picture of the Axis webcam, although it is configured correctly in the CMC III. What should be changed in the software of the webcam? .....	15
<b>Charts (record of measured values) .....</b>	<b>17</b>
Can I save the measurements from a CMC III system? .....	17
At what intervals are values recorded in the system memory? .....	17
How can I display the saved values? .....	17
What happens if I reboot the system? .....	17
Can I download and edit the measurements from the system? .....	17
How many measurement points in total may be stored in each file? .....	17
Can values be added retrospectively to a file? .....	18
<b>Installation and wiring.....</b>	<b>19</b>
The infrared sensors do not detect the door in its closed state, what needs to be considered? .....	19
What is the pin assignment of the 7030.190 universal sensor when the S <sub>0</sub> or the Wiegand interface is used? .....	19
If the CMC III I/O Unit is to be connected with several fault-message contacts of a device, how must it be wired? .....	20
How, for example, is a lamp connected to the relay output? .....	20
<b>Door control with CAN bus access .....</b>	<b>21</b>
How many racks can be controlled with a CMC III system? .....	21
How many reader systems must be installed? .....	21
Can a reader system be used to release selected doors only? .....	21
How many cards or number codes can be stored in the system? .....	22
Can a number code or a transponder card be used to open an external lock, e.g. a door buzzer, or activate a magnet? .....	22
What card standard does the 7030.230 CMC III Transponder Reader support? .....	22
Can other card types also be integrated? .....	22
Is it possible to release one or more doors if two cards or two numerical codes are used (4-eyes principle)? .....	22
Can the software be set in such a way that users need a card and a numerical code? ....	22
<b>Flexibly designable Web interface (dashboards) and mobile website .....</b>	<b>23</b>
Following an update, why are the "Dashboards" tab and the button on the homepage no longer visible? .....	23

There has been an auto-logout and my changes have been lost. What are the possible causes? .....	23
Which mobile operating systems and devices are supported? .....	23
Which values are displayed on the mobile website? .....	23
How many windows can be displayed on the mobile website? / What is the maximum number of values that should be configured on the dashboard for the mobile website? ...	23

## **Notes on these FAQ – CMC III**

These FAQs refer to software version V3.15.20\_10 of the CMC III. Some of the explanations may vary from older versions.

## CMC III general

### **How many sensors can be connected to each CMC III Processing Unit and CMC III Processing Unit Compact?**

The maximum number of sensors that can be connected is 32 per CMC III Processing Unit and 4 per CMC III Processing Unit Compact. This number, however, does not apply to every sensor and differs depending on the sensor type. An overview of the maximum number of sensors that can be connected to each Processing Unit is provided on page 549 in System Catalogue 35. Alternatively, the CMC III Sales Tool used as product configurator can also be downloaded from [www.Rittal.com](http://www.Rittal.com) and from the [www.RiMatrix5.com](http://www.RiMatrix5.com) download area.

### **What system characteristics does my computer need in order to be able to operate the CMC III?**

Apart from a standard Web browser, no special software is needed. Rittal recommends that you should always use the most up-to-date browser version. We also recommend using Mozilla Firefox or Google Chrome, because Internet Explorer is unable to replicate all of the system's functions.

### **Can I represent multiple CMC III systems on a user interface?**

The representation of multiple CMC III systems on a user interface requires an additional system. To obtain such an overview, the CMC values must be included in a management software. For this purpose, Rittal offers the "RiZone" Data Centre Infrastructure Management (DCIM) software that automatically detects all Rittal components. Further information about "RiZone" can be found on our homepage using the following link:

[RiZone at www.Rittal.com](http://www.Rittal.com)

### **How can the CMC III data be included in other systems?**

As of software version V3.11.00, the CMC III supports the two standard protocols "SNMPv1/2c/3" and "OPC-UA" and from software version V3.15.00 the standard protocol "Modbus/TCP". These protocols can be used to query data via the network and make the data available to higher-level management systems. The MIB for SNMP can be downloaded from [www.Rittal.com](http://www.Rittal.com) and from the [www.RiMatrix5.com](http://www.RiMatrix5.com) download area. Such a file is not required for OPC-UA because the component detection is controlled automatically by the protocol. When using Modbus/TCP, the CMC III system must already be fully configured and operational, in order to be able to download a list of variables from the live system via FTP. The list of variables can be downloaded out of the folder /downloads/docs and has the file name "ModbusMap.cmc3".

### **Can the CMC III data also be transferred via BACnet or Modbus?**

CMC III supports only SNMPv1/2c/3, OPC-UA and Modbus/TCP. The BACnet protocol is not implemented. Modbus/TCP may be used via the network interface, but Modbus/RTU is not supported. If a connection using other protocols is required, a third-party protocol converter must be used to convert the data from SNMP, OPC-UA or Modbus/TCP to the associated protocol. This service is not provided by Rittal and must be performed by the associated user or service provider.

**Can the messages from several CMC III systems be sent using a single GSM/ISDN unit?**

From software version V3.15.00 onwards, up to six CMC III Processing Units may be administered with just one GSM/ISDN unit. To this end, a GSM or ISDN unit is connected to a CMC III PU. The other five CMC III PUs must communicate with the latter via the network. The IP addresses of the other CMC III PUs are stored in the SMS configuration of the CMC III PU with connected GSM/ISDN unit. At the same time, the IP address of the CMC III PU with GSM/ISDN unit must be defined as a trap receiver in the SNMP configuration of the other CMC III PUs. In this way, the operator may specify in the alarm configuration of the sensors which alarm messages are to be forwarded to the CMC III PU with GSM/ISDN unit and sent as text messages.

**Is the 3124.200 interface card for cooling units with Comfort controller compatible to the CMC III?**

No, the 3124.200 interface card for cooling units with Comfort controller (RTT I/O Unit) cannot be connected to the CMC III. The digital inputs integrated as standard in a CMC III Processing Unit / Processing Unit Compact can be used, however, to connect the RTT cooling units. They are connected with the fault signal contacts of the climate control unit. This avoids the need for an interface card.

**Can I use a standard CMC III PU for installation in a LCP or in a RiMatrix S? Will modifications need to be made to the firmware?**

Generally speaking, a standard CMC III PU may be installed in a LCP or in a RiMatrix S in its delivered state. However, in order to operate the systems correctly, a special patch file for the respective LCP / RiMatrix S system must be copied onto the CMC III PU to make the CMC III PU compatible with the system. The patch file can be requested from Rittal, and should then be copied into the "Update" folder of the CMC III PU via FTP. A CMC III PU of a LCP/RiMatrix S can be set back also to a "default"-PU with a patch file.

**Which SD cards and USB sticks can be used?**

SD cards and USB sticks with up to 32 GB may be used.

Any USB stick currently on the market may be used, provided it has a type A connector. The stick simply needs to be FAT formatted (including FAT32, etc.). USB 2.0 is supported.

A small proportion of the SD cards currently available on the market may not function correctly with the CMC III. SD cards could differ in their electronic components even they are from the same type because they may be part of different charges. This could be a reason, why SD cards from the same type may not function correctly. Rittal recommends using SD cards for industrial usage.

The SD card or USB stick used is monitored by the system to gauge the amount of memory used. Once the memory is 80% full, a warning message will be given, and once it is 90% full, an alarm message will appear.

**Is it possible to connect a camera to the CMC III?**

A network camera from "Axis®" may be integrated into the Web interface of the CMC III, but this does not apply to a CMC III PU Compact. The camera must support Axis®'s own API

"VAPIX®", version 3. The camera images are streamed into the Web interface via the network. It is not possible to connect a camera directly to the CMC III. The images shown may be linked to an alarm, and if the alarm is triggered, stored on an SD card or USB stick. The only exception to this is Internet Explorer. If using Internet Explorer, live images from the camera cannot be displayed, because Internet Explorer does not support the streaming function used. When using Opera as a browser, password protection on the camera must be deactivated.

**Which Data Encryption Standard is used for the network communication?**

With software version V3.15.20\_6 and newer, the CMC III only accepts TLS-encryption for HTTPS-connections. If a browser tries to connect via SSL (1.0, 2.0 or 3.0), the CMC III does not reply, because also SSL 3.0 obtains to be decipherable.



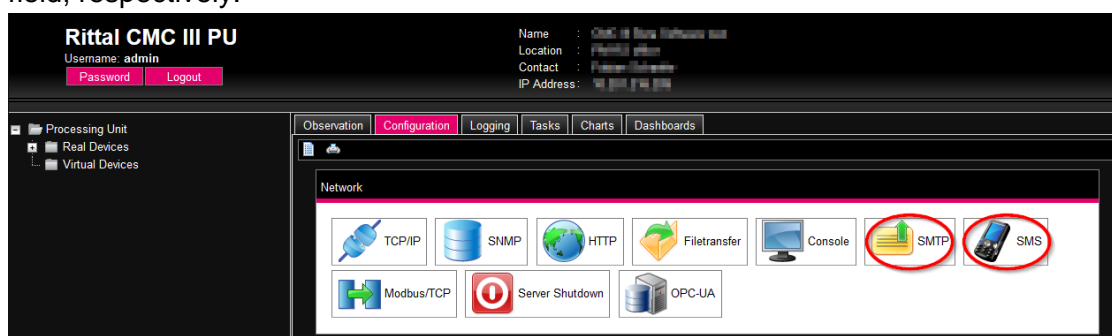
# CMC III software configuration

**How do I define an alarm? The alarming as e-mail or SMS does not function correctly, what can be the reason?**

The alarms are configured in two steps:

1. General configuration:

Switch to the general configuration. To do this, mark the uppermost "Processing Unit" item on the left-hand side in the tree by clicking it and then open the "Configuration" tab. To configure the e-mail addresses or an SMS unit, click the "SMTP" or "SMS" field, respectively.



A new window opens after you have selected the associated field. Enter the general configuration of the e-mail server / SMS unit on the left-hand side in this window. You can enter a maximum of 16 e-mail / SMS receivers in the table on the right-hand side.

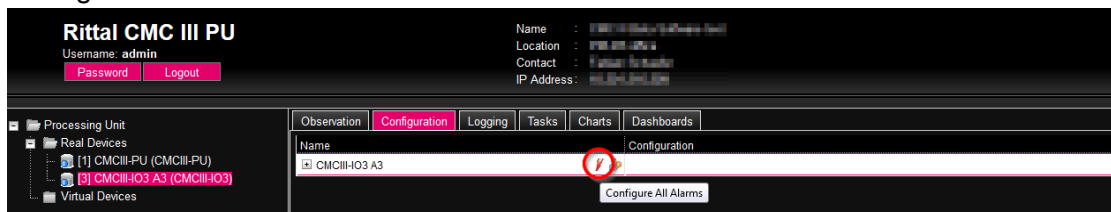
No.	Email Address	Use
1	technician1@orga.com	<input checked="" type="checkbox"/>
2	technician2@orga.com	<input checked="" type="checkbox"/>
3	technician3@orga.com	<input checked="" type="checkbox"/>
4		<input type="checkbox"/>
5		<input type="checkbox"/>

Save Reset Cancel

Switch on the associated receiver by setting the appended tick. If the tick is not set, no alarming will be sent to this receiver.

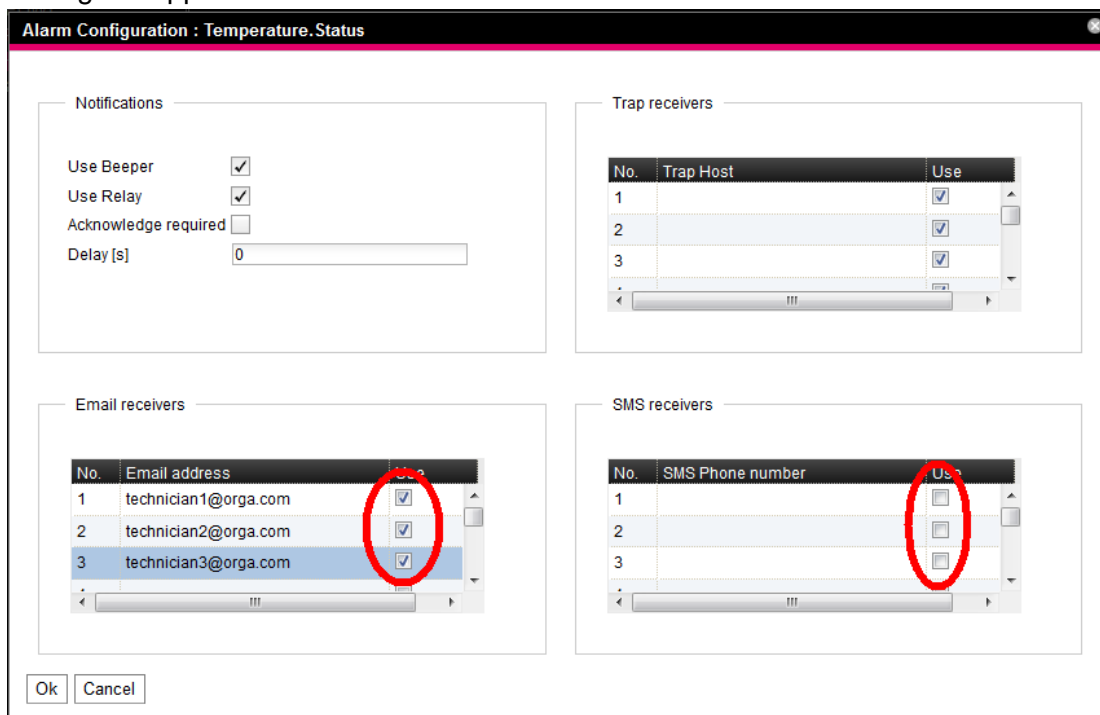
## 2. Configuration of the sensor:

Switch to the alarm configuration of the associated sensor for which an alarm message should be sent. Mark it on the left-hand side in the tree by clicking it. Then switch to the "Configuration" tab and select the red lightning symbol to activate "Alarm Configuration".



In the opened window, select the associated measured value for which an alarm message should be sent. Mark it by clicking it and then click the "Edit" button.

A new window opens in which you must switch the associated receivers on again by setting the appended tick.



The receivers are taken automatically from the general configuration and cannot be changed here.

Click the "OK" button to confirm this configuration and then click "Save" in the "Alarm Configuration" window to save the configuration.

**After selecting a sensor and clicking on "Alarm Configuration", no values for selection are listed in the window. How can I rectify this?**

If there are no sensor values listed in the "Alarm Configuration" window, the sensor is not yet logged on to the system. This is indicated by the sensor symbol in the left-hand section of the Web interface. If the sensor is not yet logged on, a cylinder with a green "plus" symbol will

appear there. To log on, first close the window. Then right-click on the list of messages at the bottom of the Web interface or on the list of sensors on the left, and select the action "Acknowledge Devices" or "Acknowledge All Devices". Alternatively, keep the "C" button on the front of the CMC III PU held down for 3 seconds. The sensor will then be logged on and alarm configuration can be carried out.

#### **What is the difference between a "virtual device" and a "task"?**

A "virtual device" is a virtual sensor that performs a specific action depending on its category. For example, whereas a "two-level controller" switches an output depending on an input value, an "access controller" switches an output that will then be recognised as a handle so it can be triggered with a reader system. A virtual device can also be queried using SNMP and OPC-UA. A virtual device, however, only performs one fixed action and there is only a single input variable used for control. This is also independent of the status ("OK"/"warning"/"alarm") of the associated sensor.

In contrast, many different input values can be linked with a task that can also perform various actions. This means defined states can use logical links to trigger an action over several sensors. A task then regulates the sensors ("OK"/"warning"/"alarm") depending on the associated states and can also be linked with a time period. Not only the switching of an output, but also other actions, such as the sending of an e-mail or the suppression of an alarm, can be triggered as action. Consequently, although a task is much more flexible than a virtual device, it cannot be queried by SNMP and the system is limited to 16 tasks.

#### **How many messages can the CMC III store in the logging?**

A permanently defined area in the system memory of 1 MB is reserved for logging messages. This area consists of two blocks each of 500 kB. The system first writes one such block full and then begins with the second block. If the second block becomes full with messages, the first (and oldest block) will be deleted. The number of messages depends on the length of the individual logging lines. As a guideline, you can expect at least 5,000 logging entries to be accommodated.

If you want these logging entries to be permanently saved, they must be copied at regular intervals onto an external server via FTP or SFTP. Alternatively, the CMC III also supports the Syslog protocol, whereby logging messages can be sent automatically to an external Syslog server as soon as they occur.

#### **Can the logging messages be deleted?**

No, the complete deletion of the logging messages is not possible. Although, on the website, the list of the messages can be filtered and the current display deleted, the messages themselves are retained on the system. The log files can also only be downloaded but not deleted by FTP or SFTP.

#### **Can a system configuration be saved and recreated on another device?**

From software version V3.11.00 and above, both the configuration of the sensors and the general configuration of a CMC III system may be saved and recreated. However, please note that the sensor configuration in both the original system and the new system into which the configuration is being copied must have exactly the same sequence (same index for a sensor type in the sensor list on the left-hand side of the Web interface). If not, the system

will ignore the sensor configuration, and will only copy the general configuration from the configuration file.

The network settings (IP address, network mask, gateway) are not copied.

The outgoing system and the target system must also have the same software version.

### **How do I save/copy the configuration of a CMC III system onto another system?**

In order to save the configuration, first make an FTP connection to the CMC III system, and navigate to the "download" folder. The name of the configuration file is "cmcllsave.cfg". Copy this file onto your local computer.

To recreate this configuration, copy this file into the "upload" folder on the target system via FTP.

The "cmcllsave.cfg" file contains a checksum which is used to check the file as it is copied from the CMC III PU. If the file is manually edited on the local computer with a word processing program, this checksum will no longer be correct, and the file will be rejected by the system. The file cannot be modified manually.

Once the file has been copied, the CMC III PU will automatically recreate the settings.

Afterwards, full details of the recreation process can be found in the log file of the CMC III.

### **Is it possible to copy a company-own certificate to the CMC III for encrypted communication?**

With software version 3.15.20\_6 and higher, it is possible to upload an own certificate to the CMC III PU, which is used by the system for encrypted communication with the webserver.

With Softwareversion 3.15.20\_10 and newer, the file must be named as "https.crt" (with lower software version before: "rittalcmc.ssl") and must include the Private Key and the Certificate in the same file.

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgk.....
.....
.....ChjfoEAKrhFFAXFRE=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwI.....
.....
.....53HVfdbypHM9Qg==
-----END CERTIFICATE-----
```

After creating the file "https.crt", it must be copied to the /upload-folder on the CMC III via FTP or SFTP. The system does a cyclical inspection for that file in this folder. If a new file is found, the certificate is checked by the system. In case of a positive result from that check, the certificate from the new file is used by the system for the webserver. If the result is negative and the certificate is wrong, the system deletes the new certificate and uses the standard Rittal-certificate again. Beside an entry in the logging on the Website, a file is

created in the same directory, in which is written the state of the upload of the certificate and if the new one is used. The file is named "https.crt.status" and can be opened with a standard text-editor program.

These steps are logged in the internal CMC III logging, which can be found also on the website or via FTP/SFTP.

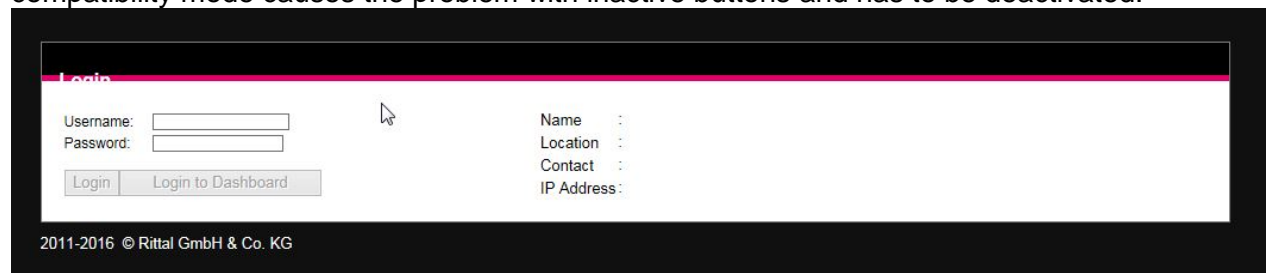
The following example shows how a certificate is created for the CMC III on a Linux system with OpenSSL:

```
openssl req -x509 -nodes -days 1825 -subj /C=DE/L=Herborn/OU="Rittal GmbH & Co. KG" -newkey rsa:2048 -md5 -keyout rittalcmc.ssl -out rittalcmc.ssl
```

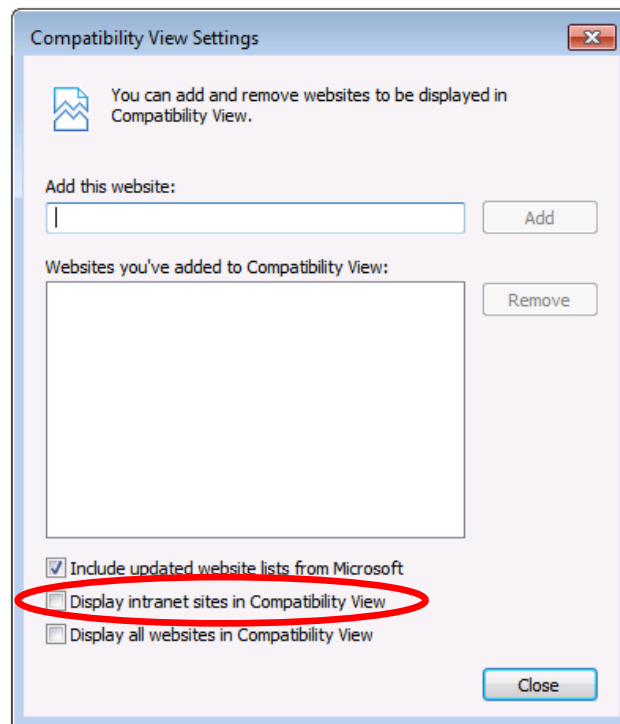
The softwareversion 3.15.20\_10 and newer supports also certificates with a certification chain.

**The Login with Internet Explorer is not possible because the buttons are inactive, although if I use the newest version. Which configurations should be done?**

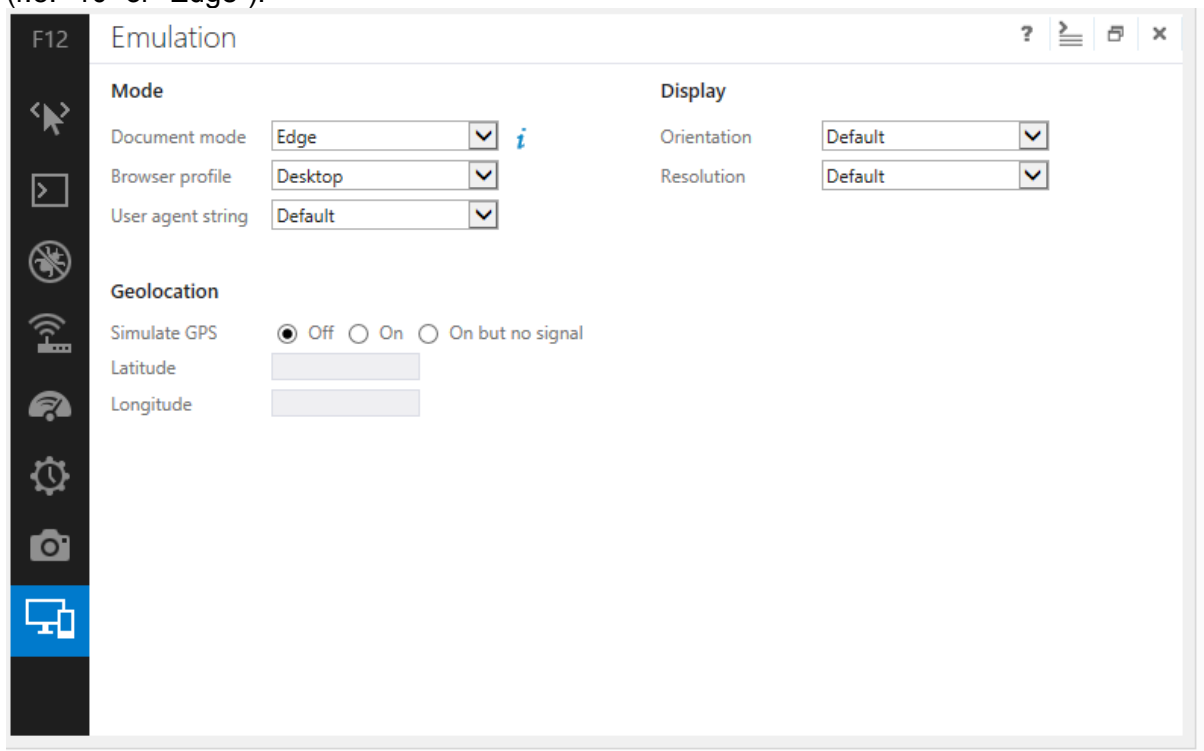
The Internet Explorer has in the later versions an option which is called compatibility mode, to show websites in an internal network (intranet sites) without any configuration changes. For the website of the CMC III, the latest version of the Explorer must be used and the compatibility mode causes the problem with inactive buttons and has to be deactivated.



The compatibility mode can be deactivated in general for all intranet sites. Click on the configuration button of the Internet Explorer in the right topper corner (gear symbol). Go to "Compatibility View settings" and deactivate the option "Display intranet sites in Compatibility View".



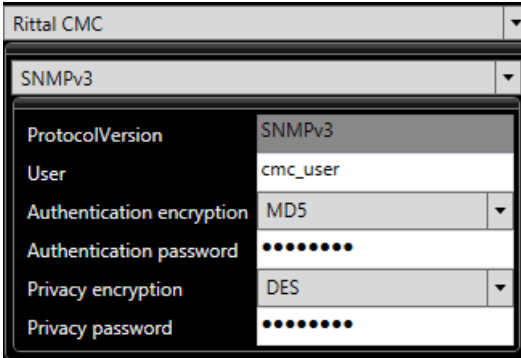
As a second way, the document mode can be changed in the developer toolbar. Open the developer toolbar through the options menu or press “F12”. In the submenu “Emulation” you can find the options for “Document mode”, which must be changed to the highest version (f.e. “10” or “Edge”).



Compared to the Compatibility View-Change this configuration has to be done every time the website is opened again.

### **How should a management software be configured regarding encryption to poll the CMC III over SNMPv3?**

The connection through SNMPv3 is encrypted. As standard encryption methods some different techniques are possible. Because of this, in the management software the correct method for the CMC III must be configured. In most cases, there is a differentiation in “Authentication”- and “Privacy”-encryption. As “Authentication”-encryption, the CMC III uses the method “MD5”, as “Privacy”-encryption the CMC III uses “DES”. The password, which is configured on the CMC III website in the SNMP dialogue, is used for both encryption methods.



Rittal CMC	
SNMPv3	
ProtocolVersion	SNMPv3
User	cmc_user
Authentication encryption	MD5
Authentication password	.....
Privacy encryption	DES
Privacy password	.....

### **If I cannot see the live picture of the Axis webcam, although it is configured correctly in the CMC III. What should be changed in the software of the webcam?**

In general it is recommended to update the firmware of the Axis®-webcam before integrate it in the CMC III. The update can be downloaded from the Axis® website.

There are two possible ways to configure the connection between the CMC III and the Axis®-webcam once again. This is necessary with special types of Axis®-webcams. In general, the rights to connect with the webcam must be changed. One solution is to allow a connection in general for everyone; the second way is to connect unencrypted.

This configuration has to be done on the webcam first and afterwards the configuration of the CMC III must be changed.

For anonymous login no user has to be configured as “Viewer” in the software of the webcam. But in the “Users” menu the option „Enable anonymous viewer login” has to be activated. Also in the configuration of the CMC III no user has to be configured and the fields “Username” and “Password” must be empty in the webcam configuration dialogue.

**AXIS M1145-L Network Camera** Live View | Setup | Help

**Basic Setup**

- Instructions
- 1 Users
- 2 TCP/IP
- 3 Date & Time
- 4 Video Stream
- 5 Focus & Zoom

**Video**

**Live View Config**

**Detectors**

**Applications**

**Events**

**Recordings**

**Languages**

**System Options**

**About**

**Users**

**User List**

User Name	User Group
root	Administrator
cmc	Viewer

Add... Modify... Remove

**HTTP/RTSP Password Settings**

Allow password type: Encrypted & unencrypted

**User Settings**

☒ Enable anonymous viewer login (no user name or password required)

☐ Enable anonymous PTZ control login (no user name or password required)

☒ Enable Basic Setup

Save Reset

For the second possible solution the user management in the software of the webcam can be kept active and an anonymous login is not possible. The option „Enable anonymous viewer login” stays active in this case but in the „Password Settings” the option “Allow password type” must be changed to “Unencrypted only”. In the CMC III configuration the username and the password have to be saved.

**AXIS M1145-L Network Camera** Live View | Setup | Help

**Basic Setup**

- Instructions
- 1 Users
- 2 TCP/IP
- 3 Date & Time
- 4 Video Stream
- 5 Focus & Zoom

**Video**

**Live View Config**

**Detectors**

**Applications**

**Events**

**Recordings**

**Languages**

**System Options**

**About**

**Users**

**User List**

User Name	User Group
root	Administrator
cmc	Viewer

Add... Modify... Remove

**HTTP/RTSP Password Settings**

Allow password type: Unencrypted only

**User Settings**

☐ Enable anonymous viewer login (no user name or password required)

☐ Enable anonymous PTZ control login (no user name or password required)

☒ Enable Basic Setup

Save Reset



# Charts (record of measured values)

## **Can I save the measurements from a CMC III system?**

From software version V3.13.00 and above, measured values can be saved on an external SD card or USB stick. This function is not supported by the CMC III PU Compact. Up to 16 files may be defined, each containing 6 values (a maximum total of 96 values per CMC III PU). Both analog values (e.g. temperature) and status variables (e.g. door open/closed) may be recorded. However, setpoints and fixed information values (such as serial numbers) cannot be selected.

## **At what intervals are values recorded in the system memory?**

The intervals are individually configurable between 5 seconds and 86,400 seconds (= 1 day). This means that a value is only ever recorded at these set intervals. If the value changes very briefly, e.g. a peak for 1-2 seconds, it may be registered by the CMC but not recorded, because it occurs between the two preset times for recording by the system.

## **How can I display the saved values?**

The last 5,000 values are displayed in a chart on the CMC III website. You can scroll and zoom in the chart using buttons.

Use the mouse to select a point within the chart. The values measured by the system at this point will be displayed at the side edge.

## **What happens if I reboot the system?**

If the system is rebooted, no values will be recorded during this period. As soon as the CMC III is operational again, recording will continue. On the website, this period will be indicated by an empty bar in the chart.

## **Can I download and edit the measurements from the system?**

The values are stored as a ".CSV" file on the SD card or USB stick. This .csv file may be downloaded from the CMC III at any time via FTP. Alternatively, the data carrier can also be ejected via the website, removed, and read on a PC.

This .csv file format is easily integrated into a data processing system. The CMC III user manual includes a step-by-step account of how to import this type of data into Microsoft Excel, for example.

## **How many measurement points in total may be stored in each file?**

There are no fixed limits to the number of measurement points. Instead, this depends on a number of variables, such as how many measurements are to be saved per chart, at which intervals etc. The maximum number of measurement points also depends on the size of the SD-card. The values are stored in separate files for each chart which can have a maximum size of 100 MB each. If the size of the file exceeds this, the current file is saved in the backup folder in an own directory and a new file is created. This procedure is repeated until the maximum size of the SD-card is reached. It is recommended to empty the backup-folder at regular intervals.

**Can values be added retrospectively to a file?**

If the configuration of a chart changes during the process of recording, the system will delete the old file and begin a new one. In order to ensure that the measured data is not lost, the file with the measurements should be downloaded and saved beforehand. All charts will likewise be restarted if the date or time is changed.

# Installation and wiring

## The infrared sensors do not detect the door in its closed state, what needs to be considered?

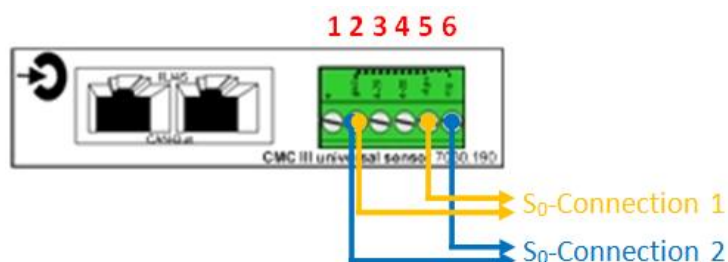
The infra-red sensors have only a specific working range. In particular for the two external sensors, 7030.120 infrared access sensor and 7030.200 CAN bus Access care must be taken to ensure that the sensors are not placed too near the door because otherwise the infrared light can no longer be reflected correctly. An overview of the possible working ranges is shown in the following table:

Sensoren	Artikel-Nummer	Sensitivity 1		Sensitivity 2		Sensitivity 3	
		min (mm)	max (mm)	min (mm)	max (mm)	min (mm)	max (mm)
CMC III Processing Unit	7030000	20	85	20	140	20	160
CMC III Processing Unit Compact	7030010	20	85	20	140	20	160
CMC III Infrarot-Zugangssensor	7030120	16	80	16	90	16	100
CMC III CAN-Bus Access	7030200	25	40	25	70	25	100

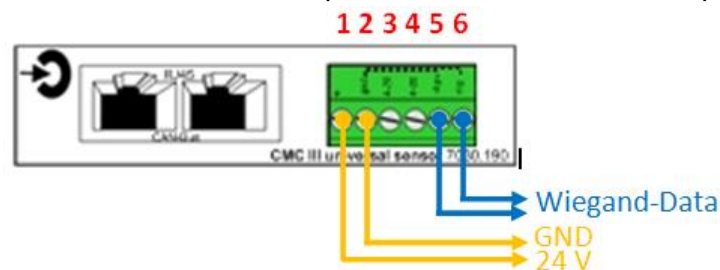
In the delivered state, a protective foil that covers the front of the sensor protects it from transport damage. This foil must be removed when the sensor is installed.

## What is the pin assignment of the 7030.190 universal sensor when the S<sub>0</sub> or the Wiegand interface is used?

If the 7030.190 universal sensor is used as S<sub>0</sub> interface, pin 5 or pin 6 (pulse) and pin 2 (GND) must be used. The universal sensor so permits the connection of two devices with S<sub>0</sub> interface:

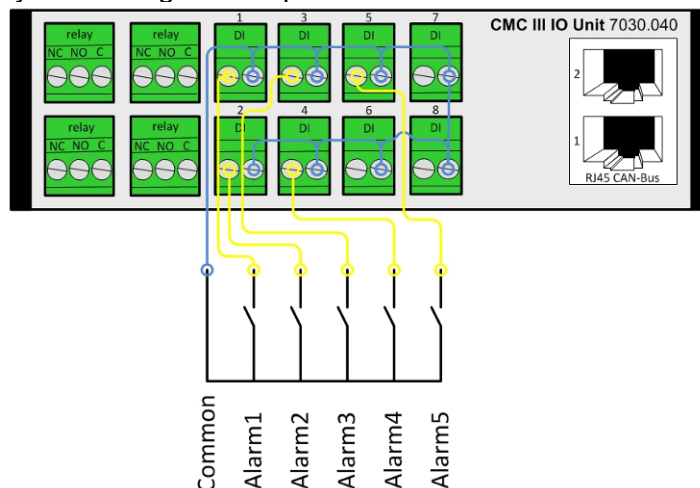


If the "7030.190 universal sensor" is used as Wiegand interface, pin 5 and pin 6 must be used as data lines. Consequently, only one reader device with Wiegand interface can be connected to a universal sensor. Pin 1 and pin 2 can also serve as 24 V power source:



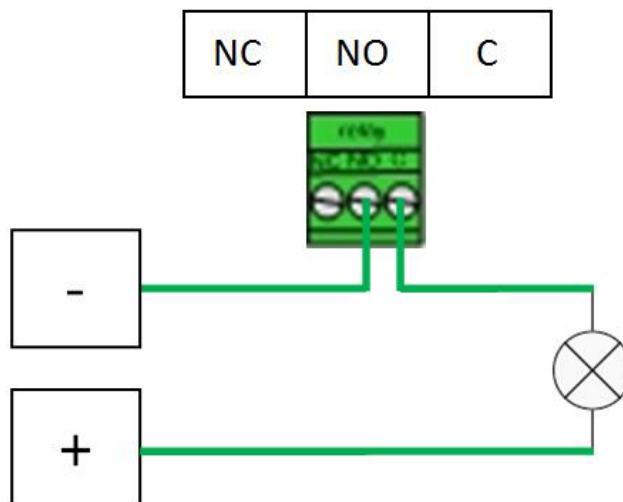
**If the CMC III I/O Unit is to be connected with several fault-message contacts of a device, how must it be wired?**

The digital inputs of the CMC III I/O Unit are connected internally to a shared GND. This makes it important that the pin assignment of the digital inputs is observed when it is connected with several fault-message contacts of a single device. The shared GND for the digital inputs is always on the right-hand pin.



**How, for example, is a lamp connected to the relay output?**

The relay outputs on the CMC III I/O Unit as well as the relay output on the rear of the CMC III Processing Unit are pure switching contacts and do not provide any 24 V power supply. This must come from an external power supply for the connection of a lamp. The relay has the connections: Common (C), Normally Open (NO) and Normally Closed (NC). The connection must be made as for a normal relay using the NO or NC and C contacts.

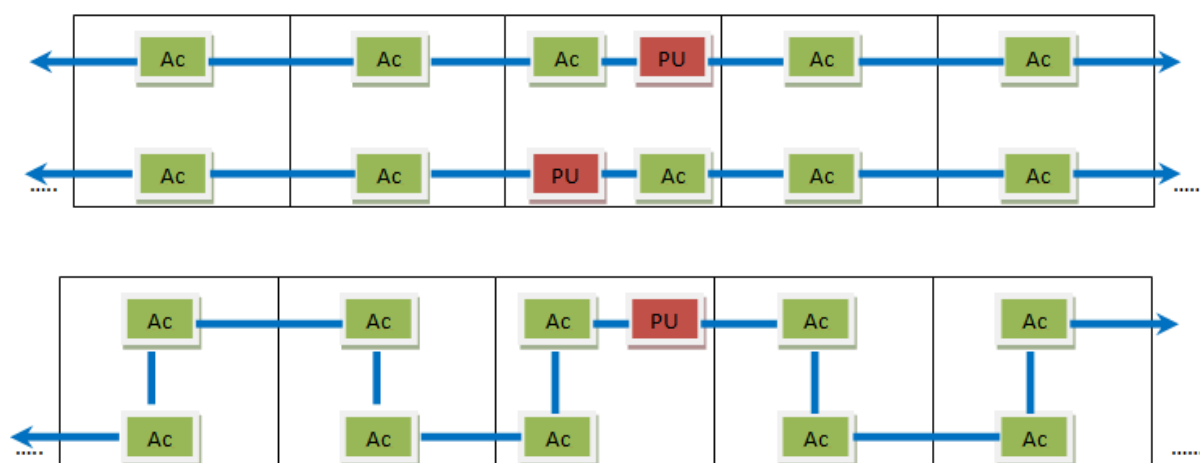


# Door control with CAN bus access

## How many racks can be controlled with a CMC III system?

Each door requires a 7030.200 CAN bus access. This means two CAN bus accesses are required for a rack with two doors.

A maximum of 16 CAN bus accesses can be connected to a CMC III Processing Unit and two CAN bus accesses to a CMC III Processing Unit Compact. If a CMC III Processing Unit is supplied only with PoE, a maximum of five handles can be connected. A system should always be configured based on how the racks are positioned. A CMC III Processing Unit with connected CAN bus access can be used for the front or rear or also for both sides.



The number of components thus depends on the configuration and on the number of doors to be monitored.

## How many reader systems must be installed?

Although the number of reader systems also depends on the application, at least one reader system should be used for each CMC III system with electromagnetic handles (without a reader system, the doors can only be opened remotely via the network or using a master key). This can then control all handles that are connected to this CMC III system, namely, a maximum of 16 units. Several reader systems can, however, also be connected to a CMC III, for example, to keep the paths from the reader system and door as short as possible. Consequently, it is better in a rack row to connect a reader system to every second or third rack. The reader systems may either be used with equal rights for all handles, or allocated to selected handles only.

## Can a reader system be used to release selected doors only?

From software version V3.15.00, the connected reader units may be assigned to the connected handles. If assigned in this way, only the respective handles may be opened with a reader system. For example, if only three handles out of 16 are assigned to a reader system, upon entering an authorised code, only these three handles will be released, and the other connected handles will remain locked. One-to-one assignment of a reader system to a handle is also supported with this function.

**How many cards or number codes can be stored in the system?**

By filling the file "access.cmc3" directly to configure the access rights, the number of programmed codes and the number of cards that can be taught on the system are unlimited. The configuration dialogue on the website is limited to 1000 cards.

**Can a number code or a transponder card be used to open an external lock, e.g. a door buzzer, or activate a magnet?**

Yes, not only a door buzzer but also a magnet can be controlled with a combination lock or a transponder reader. This requires, however, the use of a 7030.040 I/O Unit or a 7030.050 Power Unit whose outputs can be switched (I/O Unit = four relays, Power Unit = two C13 outputs).

In this case, a virtual device with the designation "Access Controller" must be created in the configuration of the CMC III and assigned the associated output, relay or C13 output. This Access Controller can then be selected in the general access configuration in which codes and cards can be assigned to a handle and will be treated by the system as a handle.

**What card standard does the 7030.230 CMC III Transponder Reader support?**

Our 7030.230 CMC III Transponder Reader supports the "Mifare" standard. A detailed description of the supported tags is contained in the technical details of the transponder reader on the website [www.Rittal.com](http://www.Rittal.com).

**Can other card types also be integrated?**

The CMC III provides the capability to integrate third-party reader units. There are two types of connection: using a digital input or using the 7030.190 Universal Sensor and its Wiegand interface.

A digital input can be connected, provided the third-party reader system has a relay output. In this case, the user administration must be made on the third-party reader system because the CMC III cannot differentiate which user opened the door.

If, however, the connection is made using the Wiegand interface, the associated code will also be transferred to the CMC III. This code can be assigned to a user and the logging lists when the user opened the door.

**Is it possible to release one or more doors if two cards or two numerical codes are used (4-eyes principle)?**

From software version V3.15.00, the 4-eyes principle may be configured directly in the CMC III software. The cards/codes may be divided into one of two authorisation levels. One card with a higher authorisation level is always needed to release the door.

**Can the software be set in such a way that users need a card and a numerical code?**

The software does not directly support a 4-eyes principle with card and code, because with this system both entries (code/card) must be made on the same reader unit. The only way of implementing a 4-eyes principle with a card and a code is by means of an additional CMC III I/O unit. In the software, you link the cards to one relay of the I/O unit and the codes to one relay of the I/O unit using a virtual device. Using a task, you may then program the handle to open when both relays are switched.

# Flexibly designable Web interface (dashboards) and mobile website

## **Following an update, why are the "Dashboards" tab and the button on the homepage no longer visible?**

If the "Dashboards" tab and the button on the homepage are no longer visible, this is because the website has not yet been reloaded and the cache hasn't been emptied. Both of these actions may be executed simultaneously using the key combination "Ctrl + F5".

## **There has been an auto-logout and my changes have been lost. What are the possible causes?**

If a dashboard is activated, the auto-logout function is deactivated. In other words, this has not occurred because a certain period of time has elapsed without activity. Instead, it is likely that a second user has made changes on the same or another dashboard, and was the first to save them. If two users are logged in to different dashboards, when one user presses the "Save" button, the second user is automatically logged out.

## **Which mobile operating systems and devices are supported?**

The mobile website may be used on smartphones and tablets with Android and Windows Phone operating systems, as well as iOS 7. Please note that iOS 8 is not currently supported.

## **Which values are displayed on the mobile website?**

The displayed values may be defined individually in a dashboard. In the CMC III configuration, you then determine which dashboard you wish to link in to when the mobile website is opened. The display windows set in the dashboard will then appear on the mobile device.

## **How many windows can be displayed on the mobile website? / What is the maximum number of values that should be configured on the dashboard for the mobile website?**

The maximum number of configurable values depends to a large extent on the mobile terminal device used. The number of displayed variables and windows should therefore be kept to a minimum, and tested for the mobile website once the dashboard has been configured.

# Rittal – The System.

---

**Faster – better – everywhere.**

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

RITTAL GmbH & Co. KG  
Auf dem Stützelberg · D-35726 Herborn  
Phone + 49(0)2772 505-0 · Fax + 49(0)2772 505-2319  
E-mail: [info@rittal.de](mailto:info@rittal.de) · [www.rittal.com](http://www.rittal.com) · [www.rimatrix5.com](http://www.rimatrix5.com)

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

