

# Rittal – Das System.

Schneller – besser – überall.



## FAQ – CMC III

Häufig gestellte Fragen (Frequently asked questions)

SCHALTSCHRÄNKE

STROMVERTEILUNG

KLIMATISIERUNG

IT-INFRASTRUKTUR

SOFTWARE & SERVICE

FRIEDHELM LOH GROUP



# Inhaltsverzeichnis

<b>Inhaltsverzeichnis .....</b>	<b>1</b>
<b>Hinweise zur FAQ – CMC III .....</b>	<b>5</b>
<b>CMC III allgemein.....</b>	<b>6</b>
Wie viele Sensoren kann man pro CMC III Processing Unit und CMC III Processing Unit Compact anschließen? .....	6
Welche Systemeigenschaften muss mein Rechner mitbringen, um das CMC III betreiben zu können? .....	6
Kann ich mehrere CMC III-Systeme auf einer Oberfläche darstellen? .....	6
Wie können die Daten des CMC III in andere Systeme eingebunden werden? .....	6
Können die Daten des CMC III auch über BACnet oder Modbus übertragen werden? .....	6
Kann man die Meldungen mehrerer CMC III-Systeme über nur eine GSM-/ISDN-Unit versenden? .....	7
Ist die „3124.200 Schnittstellenkarte für Kühlgeräte mit Comfortregelung“ kompatibel zum CMC III? .....	7
Kann ich eine Standard CMC III PU zum Einbau in ein LCP oder in ein RiMatrix S verwenden? Sind dafür Anpassungen der Firmware nötig? .....	7
Welche SD-Karten und USB-Sticks kann ich verwenden? .....	7
Kann eine Kamera an das CMC III angeschlossen werden? .....	8
<b>CMC III Softwarekonfiguration .....</b>	<b>9</b>
Wie richte ich einen Alarm ein? / Die Alarmierung per E-Mail oder SMS funktioniert nicht, was muss man beachten? .....	9
Nach dem Auswählen eines Sensors und dem Klick auf „Alarm Configuration“ werden in dem Fenster keine Werte zum Auswählen aufgelistet. Wie kann dies behoben werden? .....	10
Was ist der Unterschied zwischen einem „Virtual Device“ und einem „Task“? .....	11
Wie viele Meldungen kann das CMC III im Logging speichern? .....	11
Können die Logging-Meldungen gelöscht werden? .....	11
Kann man die Konfiguration eines Systems sichern und auf einem anderen Gerät wieder herstellen? .....	12
Wie wird die Konfiguration eines CMC III Systems gesichert / auf ein anderes System kopiert? .....	12
Kann ein firmeneigenes Zertifikat zur verschlüsselten Datenübertragung auf das CMC III gespielt werden? .....	12

Eine Anmeldung über den Internet Explorer ist trotz neuester Version nicht möglich, da die Buttons grau sind. Welche Einstellungen sind hier vorzunehmen? .....	13
Welche Einstellungen müssen zum Aufbau einer Verbindung über SNMPv3 vorgenommen werden? .....	14
Welche Einstellungen sind in der Software der Axis®-Webcam vorzunehmen, wenn trotz erfolgter Konfiguration kein Live-Bild zu sehen ist? .....	15
<b>Charts (Aufzeichnung gemessener Werte).....</b>	<b>17</b>
Können die Messwerte eines CMC III Systems gespeichert werden?.....	17
In welchen zeitlichen Abständen schreibt das System die Werte auf den Speicher? .....	17
Wie können die gespeicherten Werte angezeigt werden? .....	17
Was passiert, wenn ich das System neu starte?.....	17
Kann ich die Messwerte vom System herunterladen und weiter verarbeiten?.....	17
Wie viele Messpunkte können insgesamt pro Datei gespeichert werden? .....	17
Können nachträglich Werte zu einer Datei hinzugefügt werden? .....	18
<b>Einbau und Verkabelung .....</b>	<b>19</b>
Die Infrarot-Sensoren erkennen die Tür nicht im geschlossenen Zustand, was muss man beachten?.....	19
Wie ist die Pinbelegung des „7030.190 Universalsensors“ bei Verwendung der S <sub>0</sub> - bzw. der Wiegand-Schnittstelle? .....	19
Die CMC III I/O-Unit soll mit mehreren Störmeldekontakten eines Gerätes verbunden werden. Wie muss die Verkabelung erfolgen? .....	20
Wie schließt man z. B. eine Lampe an den Relais-Ausgang an? .....	20
<b>Türsteuerung mit CAN-Bus Access .....</b>	<b>21</b>
Wie viele Racks können mit einem CMC III-System gesteuert werden? .....	21
Wie viele Lesesysteme muss man installieren? .....	21
Ist es möglich mit einem Lesesystem immer nur bestimmte Türen freizugeben?.....	21
Wie viele Karten oder Zahlencodes können im System hinterlegt werden? .....	22
Kann man mit einem Zahlencode oder einer Transponderkarte ein externes Schloss, z.B. einen Summer, öffnen oder ein Magnet schalten? .....	22
Welcher Karten-Standard wird beim „7030.230 CMC III Transponderleser“ unterstützt? .	22
Können auch andere Kartentypen integriert werden? .....	22
Ist es möglich eine oder mehrere Türen nur freizugeben, wenn zwei Karten oder zwei Zahlencodes verwendet werden (4-Augen-Prinzip)? .....	22
Kann man in der Software einstellen, dass ein Benutzer eine Karte und einen Zahlencode braucht? .....	23

**Flexibel gestaltbare Weboberfläche (Dashboards) und mobile Webseite..... 24**

Warum ist nach dem Update der Reiter „Dashboards“ und der Button auf der Startseite nicht sichtbar? ..... 24

Ein Auto-Logout ist erfolgt und meine Änderungen sind verloren gegangen, woran kann dies liegen? ..... 24

Welche mobilen Betriebssysteme und Geräte werden unterstützt? ..... 24

Welche Werte werden auf der mobilen Webseite angezeigt? ..... 24

Wie viele Fenster können auf der mobilen Webseite angezeigt werden? / Wie viele Werte sollten maximal auf dem Dashboard für die mobile Webseite konfiguriert werden? ..... 24

# Hinweise zur FAQ – CMC III

Die vorliegende FAQ bezieht sich auf die Softwareversion V3.15.20\_10 des CMC III. Die enthaltenen Erläuterungen können ggf. von älteren Versionen abweichen.

# CMC III allgemein

## **Wie viele Sensoren kann man pro CMC III Processing Unit und CMC III Processing Unit Compact anschließen?**

Die maximale Anzahl der anschließbaren Sensoren ist 32 pro CMC III Processing Unit und 4 pro CMC III Processing Unit Compact. Diese Zahl ist jedoch nicht für jeden Sensor gültig und unterscheidet sich je nach Sensortyp. Eine Übersicht über die maximale Anzahl anschließbarer Sensoren pro Processing Unit ist im System-Handbuch 35 ab Seite 549 zu finden. Alternativ kann auch das CMC III Sales-Tool als Produkt-Konfigurator verwendet werden, das auf [www.Rittal.de](http://www.Rittal.de) und im Downloadbereich auf [www.RiMatrix5.de](http://www.RiMatrix5.de) zum Download bereit steht.

## **Welche Systemeigenschaften muss mein Rechner mitbringen, um das CMC III betreiben zu können?**

Außer einem Standard-Webbrowser wird keine spezielle Software benötigt. Rittal empfiehlt immer die aktuellste Version eines Browsers zu verwenden. Ebenfalls wird empfohlen Mozilla Firefox oder Google Chrome zu verwenden, da der Internet Explorer nicht alle Funktionen des Systems darstellen kann.

## **Kann ich mehrere CMC III-Systeme auf einer Oberfläche darstellen?**

Die Darstellung von mehreren CMC III-Systemen auf einer Oberfläche ist ohne ein zusätzliches System nicht möglich. Um eine solche Übersicht zu erhalten, müssen die Werte des CMC in eine Management Software eingebunden werden. Rittal bietet hierzu die Data Center Infrastructure Management (DCIM) Software „RiZone“ an, die alle Rittal-Komponenten automatisch erkennt. Weitere Informationen zu „RiZone“ finden Sie auf unserer Homepage über folgenden Link:

[RiZone auf www.Rittal.de](http://www.Rittal.de)

## **Wie können die Daten des CMC III in andere Systeme eingebunden werden?**

Das CMC III unterstützt ab Softwareversion V3.11.00 die zwei Standard-Protokolle „SNMPv1/2c/3“ und „OPC-UA“ und ab Softwareversion V3.15.00 das Standard-Protokoll „Modbus/TCP“. Mittels dieser Protokolle können die Daten über das Netzwerk abgefragt und höheren Managementsystemen bereitgestellt werden. Die MIB für SNMP kann auf [www.Rittal.de](http://www.Rittal.de) und im Downloadbereich von [www.RiMatrix5.de](http://www.RiMatrix5.de) heruntergeladen werden. Für OPC-UA ist keine solche Datei notwendig, da die Komponentenerkennung über das Protokoll automatisch geregelt wird. Für die Verwendung von Modbus/TCP muss das CMC III-System bereits voll ausgebaut und am Laufen sein, damit man sich eine Liste der Variablen per FTP vom Live-System herunterladen kann. Die Liste der Variablen kann vom /download/docs-Verzeichnis heruntergeladen werden, der Dateiname ist „ModbusMap.cmc3“.

## **Können die Daten des CMC III auch über BACnet oder Modbus übertragen werden?**

Das CMC III unterstützt nur SNMPv1/2c/3, OPC-UA und Modbus/TCP. Das Protokoll BACnet ist nicht implementiert. Modbus/TCP kann über die Netzwerkschnittstelle verwendet werden, Modbus/RTU wird hingegen nicht unterstützt. Wenn eine Anbindung über andere

Protokolle gefordert ist, muss ein Protokoll-Konverter von einem Dritthersteller eingesetzt werden, der die Daten von SNMP, OPC-UA oder Modbus/TCP in das jeweilige Protokoll umsetzt. Diese Leistung wird nicht von Rittal gestellt und muss vom jeweiligen Anwender oder Anbieter selbstständig durchgeführt werden.

**Kann man die Meldungen mehrerer CMC III-Systeme über nur eine GSM-/ISDN-Unit versenden?**

Es können ab Softwareversion V3.15.00 bis zu sechs CMC III Processing Units mit nur einer GSM/ISDN Unit verwaltet werden. Dazu wird eine GSM oder ISDN Unit an eine CMC III PU angeschlossen. Die anderen fünf CMC III PUs müssen mit dieser per Netzwerk kommunizieren können. In der SMS-Konfiguration der CMC III PU mit angeschlossener GSM/ISDN Unit werden die IP-Adressen der anderen CMC III PUs hinterlegt. Gleichzeitig muss die IP-Adresse der CMC III PU mit GSM/ISDN Unit als Trap-Receiver in der SNMP-Konfiguration der anderen CMC III PUs angegeben werden. Auf diese Weise kann in der „Alarm Configuration“ der Sensoren festgelegt werden, welche Alarmmeldungen an die CMC III PU mit GSM/ISDN Unit weitergeleitet und somit per SMS versendet werden sollen.

**Ist die „3124.200 Schnittstellenkarte für Kühlgeräte mit Comfortregelung“ kompatibel zum CMC III?**

Nein, die „3124.200 Schnittstellenkarte für Kühlgeräte mit Comfortregelung“ (RTT I/O-Unit) kann nicht an das CMC III angeschlossen werden. Zur Anbindung der RTT Kühlgeräte können jedoch die standardmäßig in einer CMC III Processing Unit / -Compact integrierten digitalen Eingänge verwendet werden. Diese werden mit den Störmeldekontakten des Klimagerätes verbunden. Dadurch entfällt die Schnittstellenkarte komplett.

**Kann ich eine Standard CMC III PU zum Einbau in ein LCP oder in ein RiMatrix S verwenden? Sind dafür Anpassungen der Firmware nötig?**

Generell kann eine Standard CMC III PU vom Lager in ein LCP oder in ein RiMatrix S eingebaut werden. Um die Systeme jedoch korrekt betreiben zu können, muss ein spezielles Patchfile für das jeweilige LCP / RiMatrix S System auf die CMC III PU kopiert werden, um die CMC III PU kompatibel mit dem System zu machen. Das Patchfile kann über den Service der Firma Rittal angefordert werden und muss dann nur noch per FTP in den „Update“-Ordner der CMC III PU kopiert werden. Eine CMC III PU aus einem LCP/RiMatrix S kann umgekehrt auch über ein Patchfile wieder in den Standardmodus versetzt werden.

**Welche SD-Karten und USB-Sticks kann ich verwenden?**

Es können SD-Karten als auch USB-Sticks mit bis zu 32 GB verwendet werden.

Es kann jeder USB-Stick mit Stecker Typ A vom Markt verwendet werden. Der Stick muss lediglich „FAT“ (auch FAT32, etc.) formatiert sein. Es wird USB 2.0 unterstützt.

Bei den SD-Karten kann es vorkommen, dass ein kleiner Teil der am Markt erhältlichen Karten nicht mit dem CMC III funktioniert. Auch SD-Karten vom gleichen Typ können durch verschiedene Chargen beim Hersteller unterschiedliche Elektronik-Bauteile haben, weshalb nicht alle Karten des gleichen Typs mit dem CMC III kompatibel sind. Rittal empfiehlt den Einsatz von industrietauglichen SD-Karten.

Die verwendete SD Karte / der verwendete USB Stick wird vom System jeweils auf den belegten Speicher überwacht. Ist der Speicher zu 80 % voll, wird eine Warnmeldung ausgelöst, ist der Speicher zu 90 % voll wird eine Alarmmeldung ausgelöst.

**Kann eine Kamera an das CMC III angeschlossen werden?**

In die Weboberfläche des CMC III kann eine Netzwerkkamera von „Axis®“ integriert werden, jedoch nicht bei einer CMC III PU Compact. Die Kamera muss die Axis®-eigene API „VAPIX®“ in der Version 3 unterstützen. Die Bilder der Kamera werden in diesem Fall über das Netzwerk per Stream in die Weboberfläche eingebunden. Der direkte Anschluss einer Kamera an das CMC III ist nicht möglich. Die dargestellten Bilder können mit einem Alarm verknüpft und bei Auftreten dieses Alarms auf einer SD-Karte oder einem USB-Stick gespeichert werden.

Einzige Ausnahme ist der Internet Explorer. Wird dieser verwendet, kann das Live-Bild der Kamera nicht angezeigt werden, da der Internet Explorer die verwendete Stream-Funktion nicht unterstützt. Beim Opera-Browser muss der Passwortschutz der Kamera deaktiviert werden.

**Welche Verschlüsselungsprotokolle werden unterstützt?**

Seit der Softwareversion V3.15.20\_6 akzeptiert das CMC III nur noch TLS-Verschlüsselung bei HTTPs-Aufrufen. Versucht sich ein Browser per SSL (1.0, 2.0 oder 3.0) zu verbinden, wird dies vom CMC III nicht beantwortet, da auch SSL 3.0 bereits als entschlüsselbar gilt.



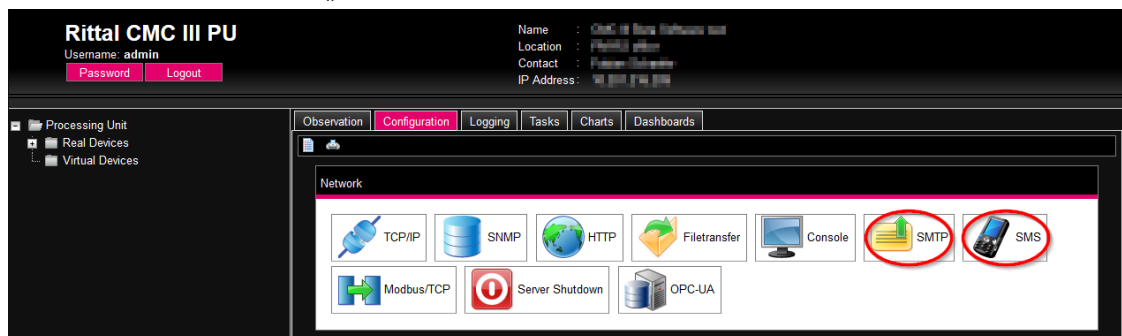
# CMC III Softwarekonfiguration

**Wie richte ich einen Alarm ein? / Die Alarmierung per E-Mail oder SMS funktioniert nicht, was muss man beachten?**

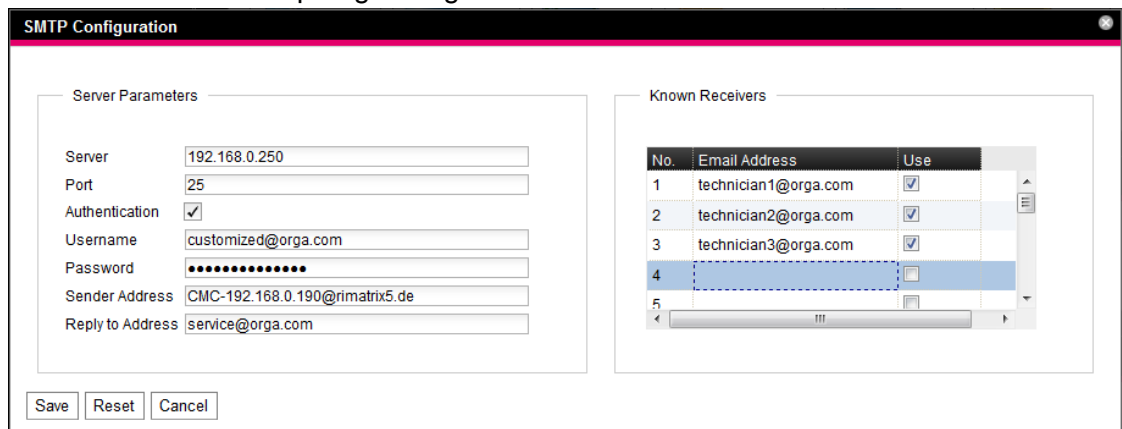
Die Alarmierungen werden in zwei Schritten konfiguriert:

## 1. Generelle Konfiguration:

Wechseln Sie in die generelle Konfiguration. Markieren Sie dazu auf der linken Seite im Baum den obersten Punkt „Processing Unit“ durch einen Klick auf diesen und öffnen Sie dann den Reiter „Configuration“. Für die Konfiguration der E-Mail-Adressen klicken Sie auf das Feld „SMTP“, für die Konfiguration einer SMS-Unit klicken Sie auf das Feld „SMS“.



Nachdem Sie das jeweilige Feld angewählt haben, erscheint ein neues Fenster. Geben Sie in diesem Fenster auf der linken Seite die generelle Konfiguration des E-Mail-Servers/der SMS-Unit ein. Auf der rechten Seite können Sie in der Tabelle bis zu 16 E-Mail/SMS-Empfänger eingeben.

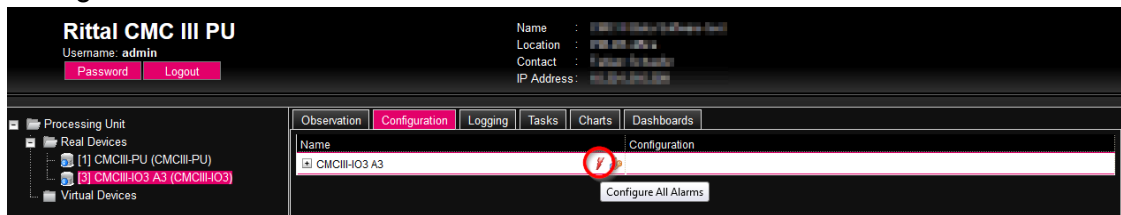


Schalten Sie hier den jeweiligen Empfänger ein, indem Sie hinter diesem den Haken setzen. Ist der Haken nicht gesetzt, wird keine Alarmmeldung an diesen Empfänger versendet.

## 2. Konfiguration des Sensors:

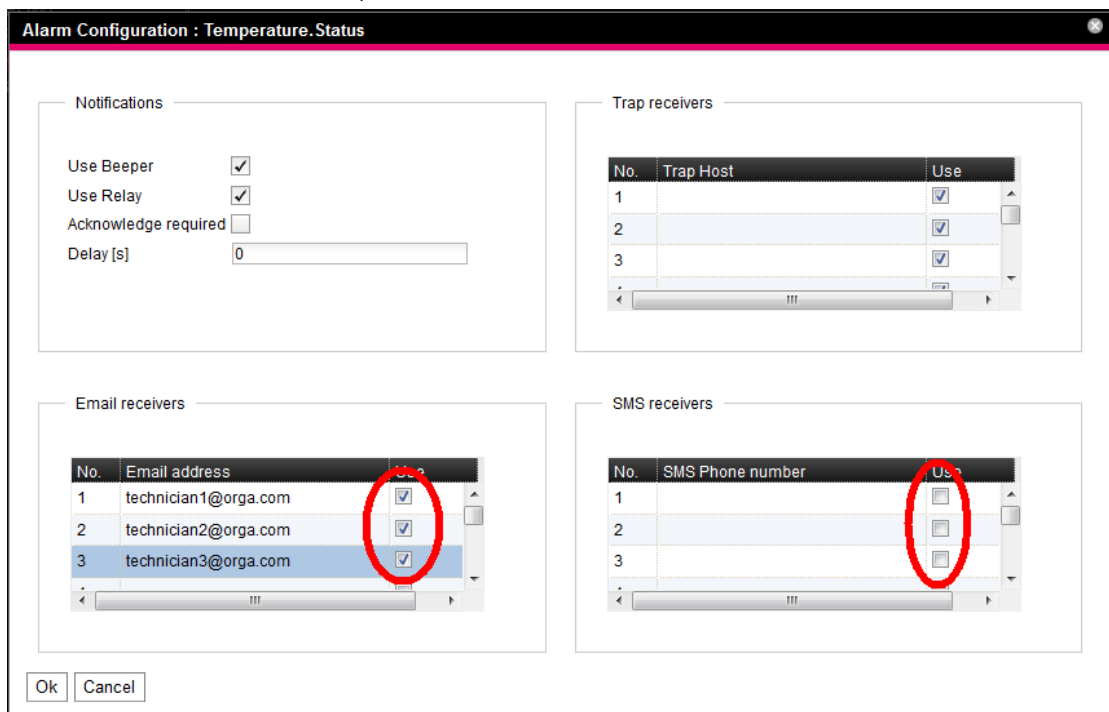
Wechseln Sie in die Alarm-Konfiguration des jeweiligen Sensors, für den eine Alarmmeldung versendet werden soll. Markieren Sie diesen dafür auf der linken Seite

im Baum, indem Sie auf diesen klicken. Wechseln Sie anschließend in den Tab „Configuration“ und wählen Sie das rote Blitzsymbol zum Aufrufen der „Alarm Configuration“.



Wählen Sie in dem darauf erscheinenden Fenster den jeweiligen Messwert aus, für den Sie eine Alarmmeldung versenden wollen. Klicken Sie diesen an, um ihn zu markieren und wählen Sie anschließend den Button „Edit“.

Es wird ein weiteres Fenster geöffnet, in dem Sie nun noch die jeweiligen Empfänger erneut einschalten müssen, indem Sie hinter diesen die Haken setzen.



Die Empfänger werden hier automatisch aus der generellen Konfiguration übernommen und können hier nicht geändert werden.

Bestätigen Sie anschließend diese Konfiguration über den Button „Ok“ und speichern Sie die Konfiguration mit einem Klick auf „Save“ im Fenster „Alarm Configuration“.

### **Nach dem Auswählen eines Sensors und dem Klick auf „Alarm Configuration“ werden in dem Fenster keine Werte zum Auswählen aufgelistet. Wie kann dies behoben werden?**

Sind in dem Fenster „Alarm Configuration“ keine Werte eines Sensors aufgelistet, ist dieser noch nicht am System angemeldet. Dies erkennen Sie an dem Symbol, mit dem der Sensor im linken Bereich der Weboberfläche angezeigt wird. Ist der Sensor noch nicht angemeldet,

wird dort ein Zylinder mit einem grünen Plus angezeigt. Schließen Sie zum Anmelden zunächst das Fenster. Klicken Sie dann mit der rechten Maustaste in die Meldungsliste am unteren Rand der Weboberfläche oder in die Sensorliste am linken Rand. Wählen Sie dann die Aktion „Acknowledge Devices“, bzw. „Acknowledge All Devices“. Alternativ können Sie auch für 3 Sekunden die „C“-Taste an der Front der CMC III PU drücken. Danach ist der Sensor angemeldet und die Alarm Konfiguration kann durchgeführt werden.

### **Was ist der Unterschied zwischen einem „Virtual Device“ und einem „Task“?**

Ein „Virtual Device“ ist ein virtueller Sensor, der je nach Art eine bestimmte Aktion ausführt. Ein „Two-Level Controller“ schaltet zum Beispiel in Abhängigkeit von einem Eingangswert einen Ausgang, während ein „Access Controller“ einen Ausgang schaltet und dann als Griff erkannt wird, sodass dieser mit einem Lesesystem ausgelöst werden kann. Ein Virtual Device kann ebenfalls über SNMP und OPC-UA abgefragt werden. Bei einem Virtual Device gibt es jedoch nur eine feste Aktion, die dieses ausführt und es gibt nur eine einzige Eingangsvariable, nach der geregelt wird. Diese ist zudem unabhängig vom Status („OK“ / „Warning“ / „Alarm“) des jeweiligen Sensors.

Mit einem Task kann man hingegen viele verschiedene Eingangswerte verknüpfen und auch verschiedene Aktionen ausführen. Mittels logischen Verknüpfungen können somit definierte Zustände über mehrere Sensoren hinweg eine Aktion auslösen. Ein Task regelt dann nach den jeweiligen Zuständen der Sensoren („OK“ / „Warning“ / „Alarm“) und kann auch mit einem Zeitraum verknüpft werden. Als Aktion können neben dem Schalten eines Ausgangs auch andere Aktionen – z.B. das Versenden einer E-Mail oder das Unterdrücken eines Alarms – ausgelöst werden. Ein Task ist im Vergleich zu einem Virtual Device damit viel flexibler, kann aber nicht per SNMP abgefragt werden und das System ist auf 16 Tasks begrenzt.

### **Wie viele Meldungen kann das CMC III im Logging speichern?**

Für die Logging-Meldungen ist ein fest definierter Bereich von 1 MB im Speicher des Systems reserviert. Dieser besteht aus 2 Blöcken á 500 kB. Das System schreibt einen solchen Block zunächst voll und beginnt dann mit dem Zweiten. Ist der zweite Block mit Meldungen gefüllt, wird der erste und älteste Block gelöscht. Die Anzahl der Meldungen ist abhängig von der Länge der einzelnen Logging-Zeilen. Als Richtwert kann man mindestens 5.000 Logging-Einträge annehmen.

Wenn Logging-Einträge dauerhaft gespeichert werden sollen, müssen diese mit FTP oder SFTP regelmäßig auf einem externen Server kopiert werden. Alternativ unterstützt das CMC III auch das Syslog-Protokoll, um Logging-Meldungen direkt bei Auftreten automatisch an einen externen Syslog-Server zu senden.

### **Können die Logging-Meldungen gelöscht werden?**

Nein, ein vollständiges Löschen der Log-Meldungen ist nicht möglich. Auf der Webseite kann man sowohl die Liste der Meldungen filtern, als auch die aktuelle Anzeige löschen. Die Meldungen selbst bleiben aber auf dem System bestehen. Per FTP oder SFTP kann man die Log-Dateien ebenfalls nur herunterladen, aber nicht löschen.

**Kann man die Konfiguration eines Systems sichern und auf einem anderen Gerät wieder herstellen?**

Sowohl die Konfiguration der Sensoren, als auch die generelle Konfiguration eines CMC III Systems kann ab Softwareversion V3.11.00 gesichert und auch wiederhergestellt werden. Es ist jedoch zu beachten, dass die Konfiguration der Sensoren bei dem Ausgangssystem, als auch bei dem System, auf das die Konfiguration kopiert werden soll, in exakt der gleichen Reihenfolge sind (gleicher Index eines Sensortyps in der Sensorliste auf der linken Seite der Weboberfläche). Ist dies nicht der Fall, überspringt das System die Sensorkonfiguration und kopiert nur die allgemeine Konfiguration aus der Konfigurationsdatei.

Die Netzwerkeinstellungen (IP-Adresse, Netzmaske, Gateway) werden nicht kopiert.

Das Ausgangssystem und das Zielsystem müssen außerdem die gleiche Softwareversion haben.

**Wie wird die Konfiguration eines CMC III Systems gesichert / auf ein anderes System kopiert?**

Zum Sichern der Konfiguration muss eine FTP-Verbindung zum CMC III System hergestellt werden. Navigieren Sie dort in den Ordner „download“. Die Konfigurationsdatei hat die Bezeichnung „cmcllsave.cfg“. Kopieren Sie diese Datei auf Ihren lokalen Rechner.

Zur Wiederherstellung dieser Konfiguration kopieren Sie diese Datei auf das Zielsystem per FTP in den Ordner „upload“.

Die Datei „cmcllsave.cfg“ enthält eine Checksumme, mit der die Datei bei Aufspielen zunächst von der CMC III PU überprüft wird. Wird die Datei mit einem Textbearbeitungsprogramm von Hand auf dem lokalen Rechner verändert, stimmt diese Checksumme nicht mehr und die Datei wird vom System verworfen. Eine Anpassung der Datei per Hand ist nicht möglich.

Nachdem die Datei aufgespielt wurde, führt die CMC III PU die Wiederherstellung selbstständig aus. Im Logging des CMC III können die Wiederherstellungspunkte im Anschluss detailliert nachvollzogen werden.

**Kann ein firmeneigenes Zertifikat zur verschlüsselten Datenübertragung auf das CMC III gespielt werden?**

Es ist ab Softwareversion 3.15.20\_6 möglich ein eigenes Zertifikat auf eine CMC III PU zu übertragen, damit dieses vom System zur verschlüsselten Verbindung zum Webserver verwendet wird. Die Zertifikats-Datei muss ab der Softwareversion 3.15.20\_10 den Namen „https.crt“ haben (vorher: „rittalcmc.ssl“) und Private Key und Certificate gleichzeitig enthalten.

```

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgk.....
.....
.....ChjfoEAKhFFAXFRE=
-----END PRIVATE KEY-----

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

```

Nach der Erstellung der Datei „https.crt“ muss diese per Datei-Upload (z. B. SFTP) auf das /upload-Verzeichnis des CMC III hochgeladen werden. Das Verzeichnis wird zyklisch nach dem Vorhandensein dieser Datei untersucht. Wird die Datei gefunden, erfolgt eine Überprüfung des Zertifikats. Ist diese Überprüfung positiv, wird die Datei als neue Zertifikat-Datei für den Webserver verwendet. Im Fehlerfall wird das Zertifikat wieder gelöscht und das Standard-Zertifikat von Rittal verwendet. Neben einem Log-Eintrag auf der Webseite wird auch eine Log-Datei **'https.crt.status'** im /upload-Verzeichnis erzeugt, aus der ersichtlich ist, ob das neue Zertifikat erfolgreich installiert wurde.

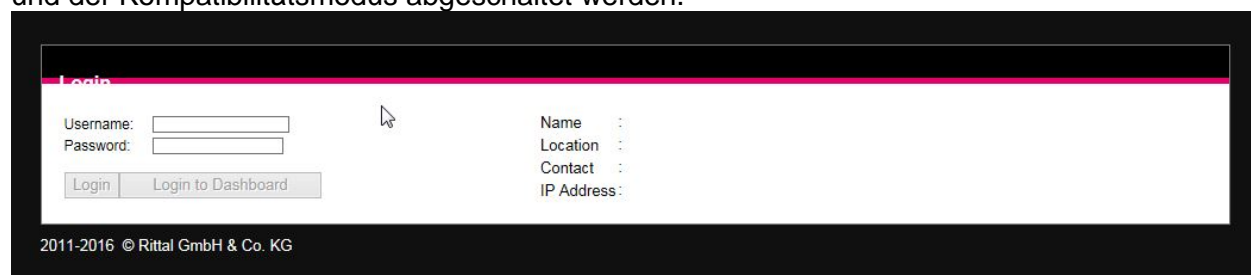
Folgendes Beispiel zeigt die Erstellung eines Zertifikats für das CMC III in Linux mittels OpenSSL:

```
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
```

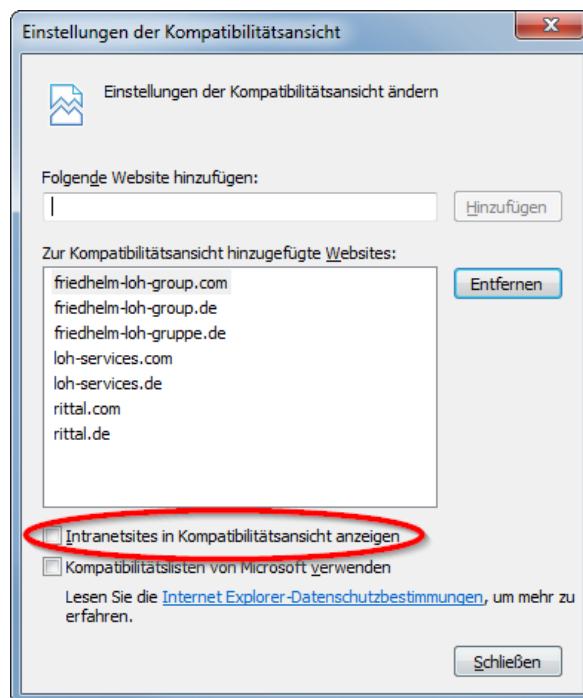
Ab der Softwareversion 3.15.20\_10 werden auch Zertifikate mit einer Zertifizierungskette unterstützt.

### **Eine Anmeldung über den Internet Explorer ist trotz neuester Version nicht möglich, da die Buttons grau sind. Welche Einstellungen sind hier vorzunehmen?**

Der Internet Explorer unterstützt in den neueren Versionen einen Kompatibilitätsmodus, um vor allem Webseiten im eigenen Netzwerk (Intranetsites) ohne Änderungen darstellen zu können. Für das CMC III muss jedoch die neueste Version des Internet Explorer verwendet und der Kompatibilitätsmodus abgeschaltet werden.



Dieser Modus kann generell für alle Intranetseiten deaktiviert werden. Klicken Sie dazu auf die Einstellungen des Internet Explorers in der rechten oberen Ecke (Zahnrad-Symbol). Wählen Sie die „Einstellungen der Kompatibilitätsansicht“ und deaktivieren Sie dort den Punkt „Intranetsites in Kompatibilitätsansicht anzeigen“.



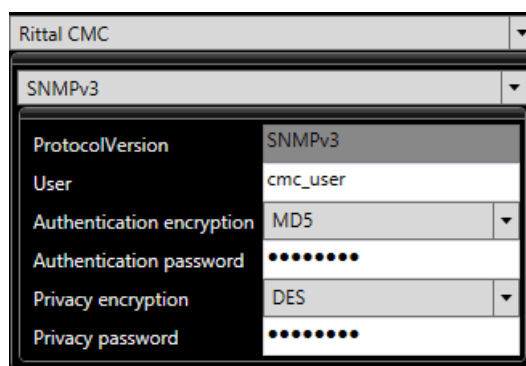
Alternativ kann die Kompatibilitätsansicht auch über die Entwicklertools abgeschaltet werden. Öffnen Sie dazu über die Einstellungen oder mit „F12“ die Entwicklertools im Internet Explorer. Unter „Emulation“ muss der Dokumentenmodus auf die neueste Technik (z.B. „10“ oder „Edge“) gestellt werden.



Im Unterschied zur generellen Abschaltung der Kompatibilitätsansicht muss die Einstellung in den Entwicklertools jedoch bei jedem neuen Aufruf der Seite vorgenommen werden.

### Welche Einstellungen müssen zum Aufbau einer Verbindung über SNMPv3 vorgenommen werden?

Die Verbindung über SNMPv3 erfolgt verschlüsselt. Als Verschlüsselungsverfahren sind unterschiedliche Methoden gängig, weshalb zur Verbindung mit dem CMC III die richtige Methode eingestellt werden muss. Meist wird in „Authentication“- und „Privacy“-Verschlüsselung unterschieden. Als „Authentication“-Verschlüsselung verwendet das CMC III die Methode „MD5“, zur „Privacy“-Verschlüsselung wird „DES“ verwendet. Das im CMC III konfigurierte Passwort zum entsprechenden Benutzer im SNMP-Dialog wird für beide Verschlüsselungen gleich verwendet.



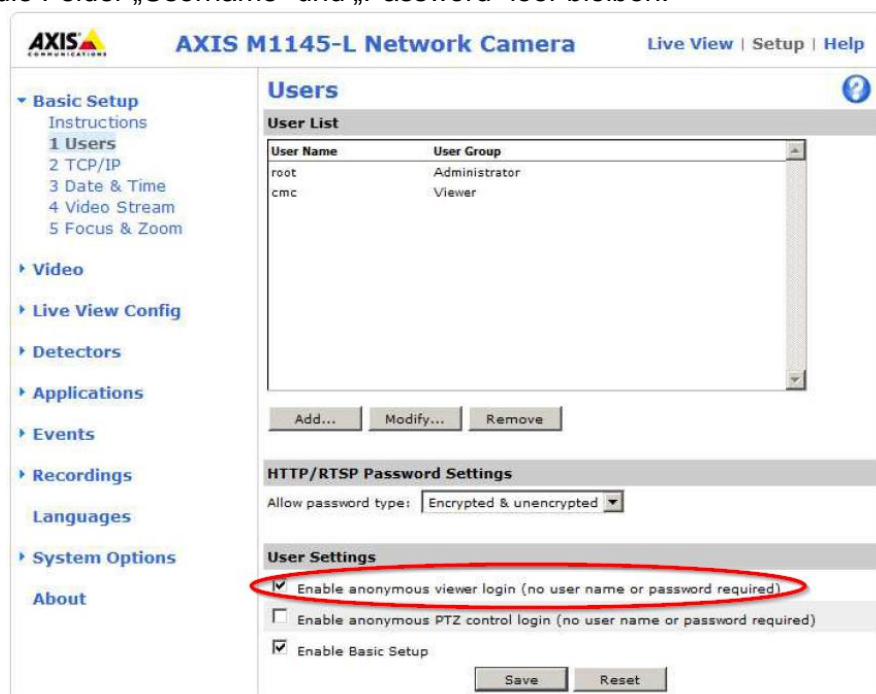
ProtocolVersion	SNMPv3
User	cmc_user
Authentication encryption	MD5
Authentication password	.....
Privacy encryption	DES
Privacy password	.....

**Welche Einstellungen sind in der Software der Axis®-Webcam vorzunehmen, wenn trotz erfolgter Konfiguration kein Live-Bild zu sehen ist?**

Grundsätzlich sollte vor der Integration der Axis®-Webcam in das CMC III ein Update der Firmware der Axis®-Webcam durchgeführt werden. Das Update kann auf der Webseite von Axis® heruntergeladen werden.

Es gibt zwei Möglichkeiten den Zugriff des CMC III auf die externe Axis®-Webcam nochmals speziell einzustellen. Dies ist nur bei manchen Kameratypen notwendig. Die beiden Möglichkeiten unterscheiden sich in der Zugriffsberechtigung auf die Webcam, die entweder anonym (ohne Benutzerverwaltung) oder mit festem Benutzernamen und Passwort erfolgen kann. Diese Einstellungen müssen zunächst in der Webcam vorgenommen und dann in den Einstellungen des CMC III entsprechend hinterlegt werden.

Für einen anonymen Login braucht auf der Kamera kein Benutzer als „Viewer“ angelegt werden. Unter dem Menüpunkt „Users“ muss der Punkt „Enable anonymous viewer login“ angewählt werden. In der Konfiguration des CMC III müssen parallel dazu im Menü unter „WebCam“ die Felder „Username“ und „Password“ leer bleiben.



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

**Users**

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



Mit der zweiten Möglichkeit bleibt die Benutzerverwaltung der Webcam aktiv und ein anonymer Zugriff ohne Login-Daten unmöglich. Dazu bleibt der Haken unter „Enable anonymous viewer login“ deaktiviert. An der Kamera muss in dafür unter „Password Settings“ der Punkt „Allow password type“ auf „Unencrypted only“ gestellt werden. Im CMC III müssen Benutzername und Passwort für die Kamera im Menü hinterlegt werden.

The screenshot shows the web interface for an AXIS M1145-L Network Camera. The left sidebar contains a navigation menu with options like Basic Setup, Video, Live View Config, Detectors, Applications, Events, Recordings, Languages, System Options, and About. The main content area is titled 'Users' and includes a 'User List' table with columns for 'User Name' and 'User Group'. The table lists two users: 'root' (Administrator) and 'cmc' (Viewer). Below the table are buttons for 'Add...', 'Modify...', and 'Remove'. A section titled 'HTTP/RTSP Password Settings' contains a dropdown menu for 'Allow password type' which is currently set to 'Unencrypted only' and is circled in red. Below this is a 'User Settings' section with three checkboxes: 'Enable anonymous viewer login (no user name or password required)', 'Enable anonymous PTZ control login (no user name or password required)', and 'Enable Basic Setup' (which is checked). At the bottom right are 'Save' and 'Reset' buttons.

User Name	User Group
root	Administrator
cmc	Viewer

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 (Aufzeichnung gemessener Werte)

## **Können die Messwerte eines CMC III Systems gespeichert werden?**

Die gemessenen Werte können ab der Softwareversion V3.13.00 auf einer externen SD-Karte oder einem USB-Stick gespeichert werden. Diese Funktion wird somit nicht von der CMC III PU Compact unterstützt. Es lassen sich bis zu 16 Dateien definieren, in denen jeweils 6 Werte mitgeschrieben werden können (insgesamt 96 Werte pro CMC III PU möglich). Dabei können sowohl analoge Werte (z.B. Temperatur), als auch Statusvariablen (z.B. Tür offen/geschlossen) mitgeschrieben werden. Setpoints und feste Informationswerte (z.B. Seriennummer) lassen sich hingegen nicht auswählen.

## **In welchen zeitlichen Abständen schreibt das System die Werte auf den Speicher?**

Die zeitlichen Abstände sind individuell konfigurierbar und können zwischen 5 Sekunden und 86400 Sekunden (= 1 Tag) betragen. Dies bedeutet, dass ein Wert immer nur in diesen zeitlichen Abständen gespeichert wird. Ändert sich dieser Wert nur kurz, z.B. ein Peak für 1-2 Sekunden, kann es sein, dass dieser zwar vom CMC registriert wird, jedoch nicht mitgeschrieben wird, da er zwischen den beiden Zeitpunkten liegt, die das System speichert.

## **Wie können die gespeicherten Werte angezeigt werden?**

Auf der Webseite des CMC III werden die letzten 5000 Werte in einer Graphik („Chart“) angezeigt. In dieser Graphik kann man über Buttons sowohl scrollen, als auch zoomen. Mit der Maus ist es möglich, einen Zeitpunkt innerhalb der Graphik zu wählen. Die Werte, die das System zu diesem Zeitpunkt gemessen hat, werden dann am seitlichen Rand angezeigt.

## **Was passiert, wenn ich das System neu starte?**

Wird das System neu gestartet, können in dieser Zeitspanne keine Werte geschrieben werden. Sobald das CMC III wieder betriebsbereit ist, wird die Aufzeichnung fortgesetzt. Diese Zeit wird auf der Webseite in der Graphik mit einem leeren Balken markiert.

## **Kann ich die Messwerte vom System herunterladen und weiter verarbeiten?**

Die Werte werden als „CSV“-Datei auf der SD-Karte oder dem USB-Stick gespeichert. Diese „CSV“-Datei kann jederzeit per FTP vom CMC III heruntergeladen werden. Alternativ kann auch der Datenträger über die Webseite ausgeworfen, herausgenommen und an einem PC ausgelesen werden.

Die Datei kann in diesem „CSV“-Format einfach in ein Datenverarbeitungssystem integriert werden. In der Bedienungsanleitung des CMC III ist Schritt für Schritt beschrieben, wie die Daten beispielsweise in Microsoft Excel eingebunden werden können.

## **Wie viele Messpunkte können insgesamt pro Datei gespeichert werden?**

Die Anzahl der Messpunkte ist nicht fest begrenzt sondern hängt von mehreren Variablen ab, z.B. wie viele Messwerte pro Chart gespeichert werden sollen, in welchen Zeitintervallen etc. Unter anderem hängt die maximale Anzahl der Messpunkte auch von der Speichergröße

der SD-Karte ab. Die Messwerte werden pro Chart in einer eigenen Datei gespeichert, diese kann eine maximale Größe von 100 MB erreichen. Überschreitet die Datei diese Größe, wird sie als Backup in den entsprechenden Ordner verschoben und eine neue Datei angelegt. Auf diese Weise speichert das System die Messwerte so lange ab, bis die maximale Speichergröße der SD-Karte erreicht ist.

Aus diesem Grund wird empfohlen, den Backup-Ordner in regelmäßigen Abständen zu leeren.

**Können nachträglich Werte zu einer Datei hinzugefügt werden?**

Wird die Konfiguration eines Charts während der Aufzeichnung geändert, löscht das System die bisherige Datei und beginnt eine Neue. Damit die gemessenen Daten nicht verloren gehen, sollte die Datei mit den Messwerten vorher heruntergeladen und gespeichert werden. Auch wenn das Datum oder die Zeit geändert wird, werden alle Charts neu gestartet.

# Einbau und Verkabelung

## Die Infrarot-Sensoren erkennen die Tür nicht im geschlossenen Zustand, was muss man beachten?

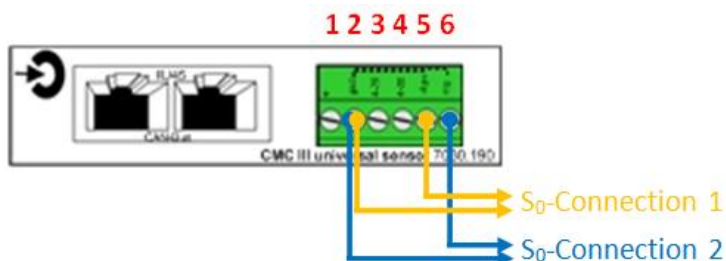
Die Infrarot-Sensoren haben nur einen bestimmten Arbeitsbereich. Besonders bei den zwei externen Sensoren „7030.120 Infrarot-Zugangssensor“ und „7030.200 CAN-Bus Access“ muss darauf geachtet werden, dass die Sensoren nicht zu nah an der Türe sitzen, da sonst das Infrarot-Licht nicht mehr richtig reflektiert werden kann. Eine Übersicht der möglichen Arbeitsbereiche ist in folgender Tabelle dargestellt:

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

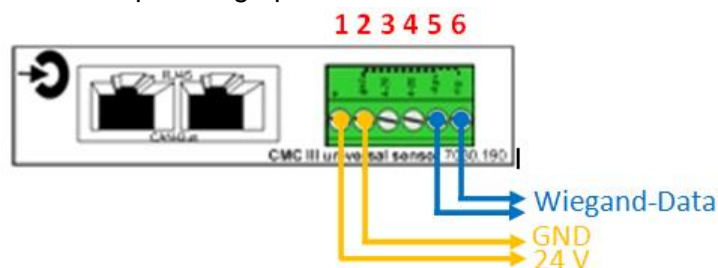
Auf der Front der Sensoren ist außerdem im Auslieferungszustand eine Schutzfolie angebracht, die die Front vor Transportschäden schützt. Diese Folie muss entfernt werden, wenn der Sensor montiert ist.

## Wie ist die Pinbelegung des „7030.190 Universalsensors“ bei Verwendung der S<sub>0</sub>- bzw. der Wiegand-Schnittstelle?

Wird der „7030.190 Universalsensor“ als S<sub>0</sub>-Schnittstelle eingesetzt, müssen Pin 5 oder Pin 6 (Impuls) und Pin 2 (GND) verwendet werden. Ein Universalsensor ermöglicht also den Anschluss von zwei Geräten mit S<sub>0</sub>-Schnittstelle:

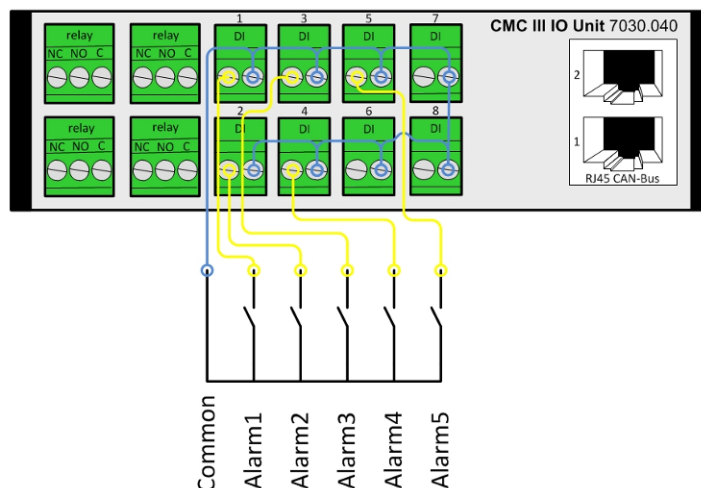


Wird der „7030.190 Universalsensor“ als Wiegand-Schnittstelle eingesetzt, müssen Pin 5 und Pin 6 als Datenleitungen verwendet werden. Es kann also nur ein Lesegerät mit Wiegand-Schnittstelle an einen Universalsensor angeschlossen werden. Pin 1 und Pin 2 können zusätzlich als 24 V Spannungsquelle dienen:



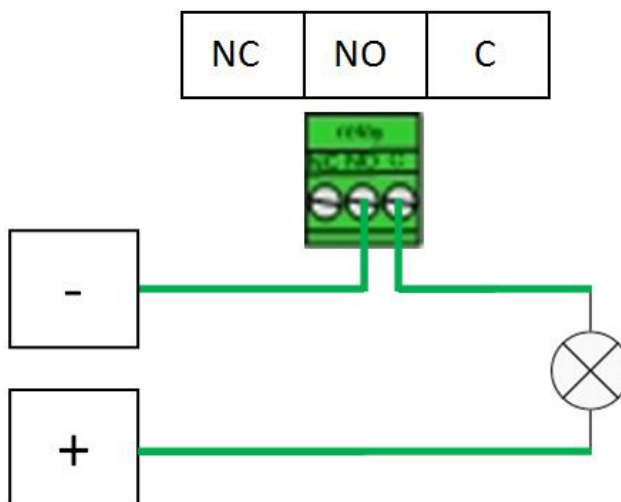
**Die CMC III I/O-Unit soll mit mehreren Störmeldekontakten eines Gerätes verbunden werden. Wie muss die Verkabelung erfolgen?**

Die digitalen Eingänge der CMC III I/O-Unit sind intern auf einen gemeinsamen GND geschaltet. Aus diesem Grund ist es wichtig, dass man die Pinbelegung der digitalen Eingänge beachtet, wenn man diese mit mehreren Störmeldekontakten eines einzelnen Gerätes verbindet. Der gemeinsame GND liegt bei den digitalen Eingängen immer auf dem rechten Pin.



**Wie schließt man z. B. eine Lampe an den Relais-Ausgang an?**

Die Relais-Ausgänge an der CMC III I/O-Unit und auch der Relais-Ausgang an der Rückseite der CMC III Processing Unit sind reine Schaltkontakte und stellen keine 24 V Spannungsversorgung dar. Diese muss bei Anschluss einer Lampe von einer externen Spannungsquelle kommen. Die Relais besitzen jeweils die Anschlüsse „Common (C)“, „Normally Open (NO)“ und „Normally Closed (NC)“. Der Anschluss muss wie bei einem normalen Relais über einen der Kontakte „NO“ oder „NC“ und „C“ erfolgen.

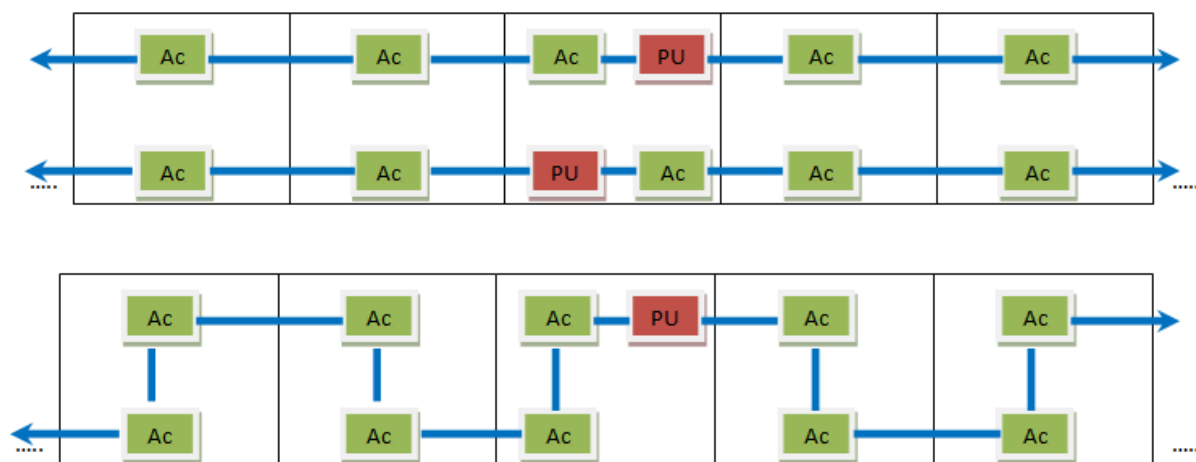


# Türsteuerung mit CAN-Bus Access

## Wie viele Racks können mit einem CMC III-System gesteuert werden?

Pro Tür wird eine "7030.200 CAN-Bus Access" benötigt. Für ein Rack mit 2 Türen sind also zwei CAN-Bus Access nötig.

Es können maximal 16 CAN-Bus Access an eine CMC III Processing Unit und 2 CAN-Bus Access an eine CMC III Processing Unit Compact angeschlossen werden. Wird eine CMC III Processing Unit nur mit PoE versorgt, können maximal 5 Griffe angeschlossen werden. Ein System sollte immer in Abhängigkeit davon aufgebaut werden, wie die Racks aufgestellt sind. Dabei kann eine CMC III Processing Unit mit angeschlossenen CAN-Bus Access sowohl für eine Front- oder Rückseite bestimmt sein, als auch für beide Seiten.



Die Anzahl der Komponenten richtet sich somit nach dem Aufbau und nach der Anzahl der zu überwachenden Türen.

## Wie viele Lesesysteme muss man installieren?

Auch die Anzahl der Lesesysteme ist individuell. Man sollte jedoch mindestens ein Lesesystem pro CMC III-System mit elektromagnetischen Griffen einsetzen (ohne ein Lesesystem können die Türen nur Remote über das Netzwerk oder mit einem Master-Key geöffnet werden). Dieses kann dann alle Griffe ansteuern, die an diesem CMC III-System angeschlossen sind, also bis zu 16 Stück. Es können aber auch mehrere Lesesysteme an ein CMC III angeschlossen werden, um beispielsweise die Wege von Lesesystem und Tür möglichst klein zu halten. In einer Rackreihe ist es also besser, an jedem zweiten oder jedem dritten Rack ein Lesesystem zu montieren. Die Lesesysteme können entweder gleichberechtigt für alle Griffe verwendet oder nur einzelnen Griffen zugeordnet werden.

## Ist es möglich mit einem Lesesystem immer nur bestimmte Türen freizugeben?

Ab der Softwareversion V3.15.00 können die angeschlossenen Lesegeräte den angeschlossenen Griffen zugeordnet werden. Mit einer solchen Zuordnung können nur noch die jeweiligen Griffe mit einem Lesesystem geöffnet werden. Sind einem Lesesystem zum Beispiel nur drei Griffe von 16 angeschlossenen zugeordnet, so werden bei Eingabe eines berechtigten Codes auch nur diese drei Griffe freigegeben und die anderen

angeschlossenen Griffe bleiben verschlossen. Auch eine 1-zu-1-Zuordnung eines Lesesystems zu einem Griff mit dieser Funktion möglich.

**Wie viele Karten oder Zahlencodes können im System hinterlegt werden?**

Bei Konfiguration über die „access.cmc3“-Datei können beliebig viele Codes programmiert und beliebig viele Karten an das System angelernt werden. Über die Webseite sind jedoch nur bis zu 1000 Karten möglich.

**Kann man mit einem Zahlencode oder einer Transponderkarte ein externes Schloss, z.B. einen Summer, öffnen oder ein Magnet schalten?**

Ja, es kann sowohl ein Summer als auch ein Magnet mit einem Zahlencodeschloss oder einem Transponderleser gesteuert werden. Dazu muss jedoch eine „7030.040 I/O-Unit“ oder eine „7030.050 Power Unit“ eingesetzt werden, deren Ausgänge (I/O Unit = 4 Relais, Power Unit = 2 C13-Ausgänge) geschaltet werden können.

In der Konfiguration des CMC III legt man dazu ein „Virtual Device“ mit der Bezeichnung „Access Controller“ an und weist diesem den jeweiligen Ausgang – Relais oder C13-Ausgang – zu. Dieser Access Controller kann dann in der allgemeinen Zugangs-Konfiguration, in der man Codes und Karten einem Griff zuordnen kann ausgewählt werden und wird vom System als Griff behandelt.

**Welcher Karten-Standard wird beim „7030.230 CMC III Transponderleser“ unterstützt?**

Wir unterstützen mit unserem „7030.230 CMC III Transponderleser“ den „Mifare“-Standard. Eine detaillierte Beschreibung der unterstützten Tags findet man auf der Webseite [www.Rittal.de](http://www.Rittal.de) unter den Detailangaben zum CMC III Transponderleser.

**Können auch andere Kartentypen integriert werden?**

Das CMC III bietet die Möglichkeit Lesegeräte von Fremdherstellern anzubinden. Dazu gibt es zwei Möglichkeiten der Anbindung: über einen digitalen Eingang oder über den „7030.190 Universalsensor“ und dessen „Wiegand-Schnittstelle“.

Die Anbindung über einen digitalen Eingang kann dann erfolgen, wenn das Lesesystem des Fremdherstellers über einen Relais-Ausgang verfügt. Die Benutzerverwaltung muss in diesem Fall am Lesesystem des Drittherstellers vorgenommen werden und das CMC III kann nicht unterscheiden, welcher Benutzer die Tür geöffnet hat.

Erfolgt die Anbindung jedoch über die Wiegand-Schnittstelle, wird der jeweilige Code mit an das CMC III übertragen. Dieser kann dann einem Benutzer zugeordnet werden, der wiederum im Logging aufgeführt wird, wenn er die Türe öffnet.

**Ist es möglich eine oder mehrere Türen nur freizugeben, wenn zwei Karten oder zwei Zahlencodes verwendet werden (4-Augen-Prinzip)?**

Ab der Softwareversion V3.15.00 kann das 4-Augen-Prinzip direkt in der Software des CMC III konfiguriert werden. Die Karten/Codes können in eine von zwei Berechtigungsstufen eingeteilt werden. Es wird immer eine Karte mit einer oberen Berechtigungsstufe benötigt, damit die Türe freigegeben wird.

**Kann man in der Software einstellen, dass ein Benutzer eine Karte und einen Zahlencode braucht?**

Ein 4-Augen-Prinzip mit Karte und Code ist nicht direkt über die Software möglich, da beim 4-Augen-Prinzip beide Eingaben (Code / Karte) am gleichen Lesegerät erfolgen müssen. Es ist nur über eine zusätzliche CMC III I/O-Unit möglich, ein 4-Augen-Prinzip mit einer Karte und einem Code zu realisieren. Per Virtual Device verknüpft man dazu in der Software die Karten mit einem Relais der I/O-Unit und die Codes ebenfalls mit einem Relais der I/O-Unit. Über einen Task kann dann programmiert werden, dass der Griff dann öffnet, wenn beide Relais geschaltet haben.

# Flexibel gestaltbare Weboberfläche (Dashboards) und mobile Webseite

## **Warum ist nach dem Update der Reiter „Dashboards“ und der Button auf der Startseite nicht sichtbar?**

Wenn der Reiter „Dashboards“ und der Button auf der Startseite nicht sichtbar sind, wurde die Webseite noch nicht neu geladen und der Cache nicht geleert. Mit der Tastenkombination „Strg + F5“ werden beide Aktionen gleichzeitig ausgeführt.

## **Ein Auto-Logout ist erfolgt und meine Änderungen sind verloren gegangen, woran kann dies liegen?**

Wird ein Dashboard aufgerufen, ist die Auto-Logout-Funktion außer Kraft gesetzt. Es liegt also nicht daran, dass eine bestimmte Zeit ohne Aktivität vergangen ist. Vielmehr hat in diesem Fall ein zweiter User auf dem gleichen oder auf einem anderen Dashboard Änderungen vorgenommen und diese als erster gespeichert. Sind zwei User auf unterschiedlichen Dashboards eingeloggt, so wird bei Betätigen des „Save“-Buttons der zweite User automatisch ausgeloggt.

## **Welche mobilen Betriebssysteme und Geräte werden unterstützt?**

Die mobile Webseite kann auf Smartphones und Tablets mit Android- und Windows Phone-Betriebssystem, sowie mit iOS 7 verwendet werden. iOS 8 ist zurzeit nicht kompatibel.

## **Welche Werte werden auf der mobilen Webseite angezeigt?**

Die angezeigten Werte können in einem Dashboard individuell festgelegt werden. In der Konfiguration des CMC III wird dann noch eingestellt, auf welches Dashboard beim Aufruf der mobilen Webseite verlinkt werden soll. Die im Dashboard eingestellten Anzeigefenster werden dann auf dem mobilen Gerät angezeigt.

## **Wie viele Fenster können auf der mobilen Webseite angezeigt werden? / Wie viele Werte sollten maximal auf dem Dashboard für die mobile Webseite konfiguriert werden?**

Die Anzahl der maximal konfigurierbaren Werte ist stark von den verwendeten mobilen Endgeräten abhängig. Die Anzahl der der angezeigten Variablen und Fenster sollte deshalb möglichst gering gehalten und nach Konfiguration des Dashboards für die mobile Webseite getestet werden.



# Rittal – Das System.

---

**Schneller – besser – überall.**

- Schaltschränke
- Stromverteilung
- Klimatisierung
- IT-Infrastruktur
- Software & Service

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.de](http://www.rittal.de) · [www.rimatrix5.de](http://www.rimatrix5.de)

SCHALTSCHRÄNKE

STROMVERTEILUNG

KLIMATISIERUNG

IT-INFRASTRUKTUR

SOFTWARE & SERVICE

FRIEDHELM LOH GROUP

