

Additional instructions CMC III PU - Access Configuration: Two-factor authentication (2FA) and Four-eyes principle

Software version 3.17.30_5 introduces a new tab in the CMC III PU web interface: " Access Configuration ". In the tab, access rights can be assigned to users and Two-factor authentication (2FA) and the Four-eyes principle can be activated.

Case 1: Deactivated Two-factor authentication and deactivated Four-eyes principle

Monitoring | Configuration | Logging | Tasks | Charts | Dashboards | **Access Configuration**

Access

Filter

Options

4 Eyes (Disabled) ☐ Timeout (Seconds) 30
2 Factor Authentication ☐ Timeout (Seconds) 30

Important Information With the 4 eyes principle, the input must be made via the same device. Therefore, the 4 eyes principle is deactivated when 2 factor authentication is activated. If you would like to use the 4 eyes principle, you can achieve this by assigning the factors to different users accordingly.

Type	Code	User	Device(s)	Information
Key	1001	admin	CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Key	1002		CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Key	1003		CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Crd	000000009401313A		CMCIII-GRF2 A	
Crd	00000000BE97114A		CMCIII-GRF2 A	
Crd	E00700001A5E1423		CMCIII-GRF2 A	
Crd	000000003D5E38CA		CMCIII-GRF2 B	
Crd	70188003F9FF12E0		CMCIII-GRF2 B	

Edit Add Delete

Fig. 1: Deactivated Two-factor authentication and deactivated Four-eyes principle

If Two-factor authentication and the Four-eyes principle are deactivated, a pin code or transponder card is sufficient to unlock the handles assigned to a user.

Case 2: Deactivated Two-factor authentication and activated Four-eyes principle

Monitoring | Configuration | Logging | Tasks | Charts | Dashboards | **Access Configuration**

Access

Filter

Options

4 Eyes (Enabled) ☒ Timeout (Seconds) 30
2 Factor Authentication ☐ Timeout (Seconds) 30

Important Information With the 4 eyes principle, the input must be made via the same device. Therefore, the 4 eyes principle is deactivated when 2 factor authentication is activated. If you would like to use the 4 eyes principle, you can achieve this by assigning the factors to different users accordingly.

Type	Code	User	Device(s)	Information
Key	1001	admin	CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Key	1002	AccessAck	CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Key	1003		CMCIII-GRF2 A, CMCIII-GRF2 B, CMCIII-GRF2 C	
Crd	000000009401313A		CMCIII-GRF2 A	
Crd	00000000BE97114A		CMCIII-GRF2 A	
Crd	E00700001A5E1423		CMCIII-GRF2 A	
Crd	000000003D5E38CA		CMCIII-GRF2 B	
Crd	70188003F9FF12E0		CMCIII-GRF2 B	

Edit Add Delete

Fig. 2: Deactivated Two-factor authentication and activated Four-eyes principle

If a handle is assigned to the user "AccessAck", the Four-eyes principle is automatically activated. Only the handles that are assigned to the user "AccessAck" and another user at the same time can be unlocked. For this purpose, both users must use the same transponder reader or the same Coded lock.

Case 3: Activated Two-factor authentication and deactivated Four-eyes principle

The screenshot shows the 'Access Configuration' page. Under 'Options', '4 Eyes (Disabled)' is unchecked and '2 Factor Authentication' is checked. Both have a timeout of 60 seconds. An 'Important Information' note states: 'With the 4 eyes principle, the input must be made via the same device. Therefore, the 4 eyes principle is deactivated when 2 factor authentication is activated. If you would like to use the 4 eyes principle, you can achieve this by assigning the factors to different users accordingly.'

Type	Code	User	Device(s)	Information
Key	1001	admin	CMCIII-GRF2 A	
Key	1002	Test1	CMCIII-GRF2 A, CMCIII-GRF2 C	
Key	1003	guest	CMCIII-GRF2 B	
Crd	000000009401313A	cmc	CMCIII-GRF2 A	
Crd	00000000BE97114A	guest	CMCIII-GRF2 A	
Crd	E00700001A5E1423		CMCIII-GRF2 A	
Crd	000000003D5E38CA		CMCIII-GRF2 B	
Crd	70188003F9FF12E0		CMCIII-GRF2 B	
Key	1004		CMCIII-GRF2 B	

Buttons: Edit, Add, Delete

Fig. 3: Activated Two-factor authentication and deactivated Four-eyes principle

When Two-factor authentication is activated, a transponder card and a pin code (or alternate device via Wiegand interface) are required to unlock a handle. The two codes required to unlock a handle can be assigned to one or more users.

ATTENTION: If a handle is assigned to the user "AccessAck" and Two-factor authentication is enabled, the Four-eyes principle is still displayed as active, but the Four-eyes principle is ignored in that case (see info on the web interface). The timeout is also set to the value that is set for Two-factor authentication (5...60 seconds).

The screenshot shows the 'Access Configuration' page. Under 'Options', '4 Eyes (Enabled)' is checked and '2 Factor Authentication' is also checked. Both have a timeout of 60 seconds. The 'Important Information' note is the same as in Fig. 3.

Type	Code	User	Device(s)	Information
Key	1001	admin	CMCIII-GRF2 A	
Key	1002	AccessAck	CMCIII-GRF2 A, CMCIII-GRF2 C	
Key	1003	guest	CMCIII-GRF2 B	
Crd	000000009401313A	cmc	CMCIII-GRF2 A	
Crd	00000000BE97114A	guest	CMCIII-GRF2 A	
Crd	E00700001A5E1423		CMCIII-GRF2 A	
Crd	000000003D5E38CA		CMCIII-GRF2 B	
Crd	70188003F9FF12E0		CMCIII-GRF2 B	
Key	1004		CMCIII-GRF2 B	

Buttons: Edit, Add, Delete

Fig. 4: Four-eyes principle still displayed as active is ignored by the CMC III PU