

ANTIPASSBACK Controller V2

APBK-CTRL-V2

Handbuch



Stand: V 2.0.45 vom 2026-04-18

(C) 2026 by SMG Schließanlagen München GmbH – <https://www.smg.gmbh>

Inhaltsverzeichnis

| | |
|--|----|
| Inhaltsverzeichnis | 2 |
| Funktionsprinzip..... | 3 |
| Antipassback / Zutritts-Wiederhol Sperre | 3 |
| 4-Augen-Prinzip | 3 |
| Anwesenheitsliste | 3 |
| Server-Erweiterung | 3 |
| Wichtige Vorbemerkungen !..... | 4 |
| Hardwarekompatibilität | 4 |
| Hinweis für Umsteiger von Antipassback V1 | 4 |
| Technische Daten | 4 |
| Anschluss..... | 5 |
| Anschluss SmartRelais 1 an Antipassback..... | 5 |
| Anschluss SmartRelais 3 an Antipassback..... | 6 |
| Anschluss Türöffner / Motorschloss an Antipassback | 6 |
| Anschluss Türkontakte an Antipassback | 7 |
| Konfiguration SimonsVoss SmartRelais in der LSM-Software | 8 |
| Einstellungen vornehmen | 8 |
| SREL.ADV:..... | 8 |
| SmartRelais 3:..... | 8 |
| Konfiguration SimonsVoss SmartRelais in der AX-Manager-Software..... | 8 |
| Einstellungen vornehmen | 8 |
| für SmartRelais 3 und SREL.ADV identisch:..... | 8 |
| Programmierung | 8 |
| Inbetriebnahme des Controllers..... | 9 |
| Inbetriebnahme per WLAN | 9 |
| Inbetriebnahme per LAN | 9 |
| Konfiguration..... | 10 |
| Seite System..... | 10 |
| Seite Config – Abschnitt Network | 11 |
| Seite Config – Abschnitt Operation..... | 12 |
| Seite Config – Abschnitt MQTT | 14 |
| Seite Config – Abschnitt Access Protection..... | 15 |
| Seite Config – Abschnitt Stylesheet..... | 15 |
| Seite Config – Abschnitt Service..... | 15 |
| Seite Masters | 17 |
| Seite Locked | 17 |
| Seite Log | 18 |
| Seite LIVE | 18 |
| Logout | 18 |

Funktionsprinzip

Der hier beschriebene Controller erweitert Ihren Transponderleser um die Funktionen Antipassback, 4-Augen-Prinzip und Anwesenheitsliste.

Antipassback / Zutritts-Wiederhol Sperre

Ein Transponder, der den Eingang betätigt hat, wird für eine festgelegte Zeitdauer gesperrt, und kann den Eingang nicht noch einmal benutzen.

Wenn der Transponder am Ausgang betätigt wird, wird dieser vorzeitig für den Eingang wieder freigeschaltet.

Die Sperre bzw. Freischaltung des Transponders kann direkt nach Transponderbetätigung erfolgen, oder erst nach erfolgter Öffnung der Türe.

4-Augen-Prinzip

Ein Transponder alleine kann die Öffnung nicht durchführen.

Es muss innerhalb einer Frist von wenigen Sekunden ein zweiter Transponder am Leser betätigt werden, erst dann wird der Zugang aktiviert

Anwesenheitsliste / PresenceDashboard

Wenn Eingangs- und Ausgangs-Leser verwendet werden, kann dieser Controller eine Anwesenheitsliste für den entsprechenden Bereich erstellen.

Diese kann für den Pförtner / Telefonzentrale oder als Evakuierungsliste benutzt werden.

Server-Erweiterung

Wenn mehrere Ein- und Ausgänge existieren, können mehrere Controller zu einem Bereich verbunden werden und der Server übernimmt die Kontrolle über Freigaben und Listen.

Wichtige Vorbemerkungen !

Die Blockierliste mit den zutrittsgesperren Transpondern wird nur im Arbeitsspeicher abgelegt. Wenn also der Controller (z.B. durch Spannungsausfall) neu startet, sind die Transponder am Eingang wieder erlaubt, und am Ausgang ggf. gesperrt. Bitte nutzen Sie also eine unterbrechungsfreie Stromversorgung, oder (empfohlen) legen Sie neben der Betriebsspannung auch noch PoE mit an.

Bitte gehen Sie sorgfältig bei der Programmierung vor.
In bestimmten Konfigurationen können Zustände wie Dauer-Auf oder Dauer-Zu auftreten (siehe weiter unten). So kann die Türe ungesichert bleiben, oder nicht mehr zu begehen sein. SMG kann für solche Programmierfehler nicht haftbar gemacht werden!

Hardwarekompatibilität

Das Antipassback ist kompatibel mit folgenden Transponder-Lesern:

SimonsVoss:

SmartRelais 3: SREL3.CTR.ADV.G2(.ZK) in Verbindung mit SREL3.EXT(2).G2.W o.ä.
(SmartRelais 2 MH: wird derzeit nicht unterstützt!)

SmartRelais 1 Advanced: SREL.ADV (nur G1!)

Kartenleser anderer Hersteller:

mit Wiegand 26-bit-Schnittstelle

Verwenden Sie möglichst Leser des gleichen Herstellers.

Hinweis für Umsteiger von Antipassback V1

Die Controller-Generation V2 erfordert die Verwendung von Wiegand 26-bit.

Bitte ggf. die Programmierung der SmartRelais / Kartenleser anpassen!

Technische Daten

| | |
|------------------|--|
| Eingangsspannung | 7-36V DC Gleichspannung und/oder PoE |
| Maße | 175 mm (B) * 92 mm (T) * 40 mm (H) |
| Eingänge | 2 Leser, jeweils Wiegand0 und Wiegand1 2 potentialfreie Eingänge DI1 und DI2 gegen DGND |
| Ausgänge | 2 Schaltrelais, Wechsler, Strom: max. 10A, Spannung: max. 230VAC bzw. max. 30VDC |
| Kommunikation | WLAN 2,4 GHz, LAN Fast-Ethernet 100MBit |
| Reaktionszeit | 0,1 s – 0,2 s |

Anschluss

Klemmenbezeichnungen am APBK-CTRL-V2

| Klemme | Belegung / Funktion |
|-----------------|--|
| DI1 | Türkontakt Eingang (optional) |
| DI2 | Türkontakt Ausgang (optional) |
| DI3 | Leser Eingang Wiegand D0 |
| DI4 | Leser Eingang Wiegand D1 |
| DI5 | Leser Ausgang Wiegand D0 |
| DI6 | Leser Ausgang Wiegand D1 |
| DI7 | Reserviert |
| DI8 | Reserviert |
| DGND | Gemeinsame Masse für die Leser und die Türkontakte (!) |
| CH1 – NO/NC/COM | Schaltausgang für Eingang (und ggf. Ausgang) |
| CH2 – NO/NC/COM | Schaltausgang für Ausgang |
| + | Spannung „+“ 7 VDC – 36 VDC |
| - | Gemeinsame Masse Spannungsversorgung und Dateneingänge/Leser |
| ETH | Ethernet-Anschluss |
| ANT | Anschluss für WiFi-Antenne (beiliegend) |

Anschluss SmartRelais 1 an Antipassback

Bei der Verkabelung zwischen SmartRelais 1 und dem APBK-CTRL gehen Sie bitte wie folgt vor:

| APBK | SREL1 | Bemerkung | Kabel-Farbe |
|--------------|-------|--|-------------|
| DI3 bzw. DI5 | F1 | Wiegand für Eingang bzw. Ausgang | |
| DI4 bzw. DI6 | F2 | Wiegand für Eingang bzw. Ausgang | |
| DGND | - | Kann auch auf – am APBK gelegt werden, wenn dort die Leser-Massen angeschlossen werden | |

Minus-Pole von SREL, Controller und DCOM müssen miteinander verbunden sein !

Gerne können Sie in obiger Tabelle die von Ihnen verwendete Kabelfarbe zu Dokumentationszwecken eintragen.

Anschluss SmartRelais 3 an Antipassback

Bei der Verkabelung zwischen SmartRelais 3 Advanced Controller und dem APBK-CTRL gehen Sie bitte wie folgt vor:

| APBK | SREL1 | Bemerkung | Kabel-Farbe |
|--------------|-------|--|-------------|
| DI3 bzw. DI5 | O1 | Wiegand für Eingang bzw. Ausgang | |
| DI4 bzw. DI6 | O2 | Wiegand für Eingang bzw. Ausgang | |
| DGND | - | Kann auch auf – am APBK gelegt werden, wenn dort die Leser-Massen angeschlossen werden | |

Minus-Pole von SREL, Controller und DCOM müssen miteinander verbunden sein !

Gerne können Sie in obiger Tabelle die von Ihnen verwendete Kabelfarbe zu Dokumentationszwecken eintragen.

Anschluss Türöffner / Motorschloss an Antipassback

| APBK | Türöffner | Bemerkung | Kabel-Farbe |
|-----------|-----------|--|-------------|
| CH1 COM | A | Ungeschalteter Pol des Türöffners Eingangstüre | |
| CH1 NO/NC | B | Geschalteter Pol für Türöffnung Eingangstüre | |
| CH2 COM | A | Ungeschalteter Pol des Türöffners Ausgangstüre | |
| CH2 NO/NC | B | Geschalteter Pol für Türöffnung Ausgangstüre | |

Die oben genannten Ausgänge sind potentialfreie Kontakte (Relais).

Sollte das Stellglied der Türe ein Potential zu benötigen, ist dies mit einzuschleifen.

Bitte beachten Sie dabei die maximale Belastbarkeit des Relaisausgangs am APBK-CTRL von 10 A bei maximal 230 VAC oder maximal 30 VDC !

Der gemeinsame Anschluss (ungeschalteter Pol) ist die jeweils mittlere der drei Klemmen.

Links und rechts davon sind die Umschalter NO (normally open) und NC (normally closed)

Gerne können Sie in obiger Tabelle die von Ihnen verwendete Kabelfarbe zu Dokumentationszwecken eintragen.

Sicherheits-Hinweis:

Bitte überlegen Sie, ob Sie das Relais des Kartenlesers/SmartRelais in Serie mit dem Schaltkontakt des Antipassbacks schalten:

Ein nicht berechtigter Transponder kann so nicht fehlerhaft Zutritt erhalten, und die Öffnungszeit der Türe kann in der Software der Schließanlage festgelegt werden (solange der Wert im Antipassback länger ist, als der Wert der Schließung). Manche Kartenleser liefern die Kartennummer auch dann an, wenn der Transponder nicht berechtigt ist, so dass das Antipassback öffnet.

Anschluss Türkontakte an Antipassback

| APBK | Türkontakt | Bemerkung | Kabel-Farbe |
|------|------------|---|-------------|
| DI1 | A | Türkontakt Eingang | |
| DI2 | A | Türkontakt Ausgang | |
| DGND | B | Hier von den Türkontakten den anderen Pol anschließen | |

Es ist nicht erforderlich, ein Potential anzulegen. Falls der Kontakt potentialbehaftet ist, müssen sich die Spannungen im Bereich von 5 VDC – 36 VDC bewegen!

Gerne können Sie in obiger Tabelle die von Ihnen verwendete Kabelfarbe zu Dokumentationszwecken eintragen.

Sicherheits-Hinweis:

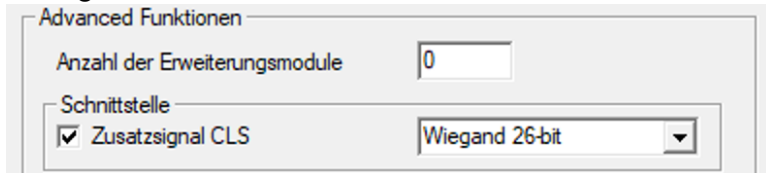
Die Verwendung von Türeingängen ist nicht erforderlich.
Wenn die Funktion jedoch aktiviert ist, müssen die Kontakte auch angeschlossen sein und funktionieren, da sonst die Transponder nicht gesperrt werden.

Konfiguration SimonsVoss SmartRelais in der LSM-Software

Einstellungen vornehmen

SREL.ADV:

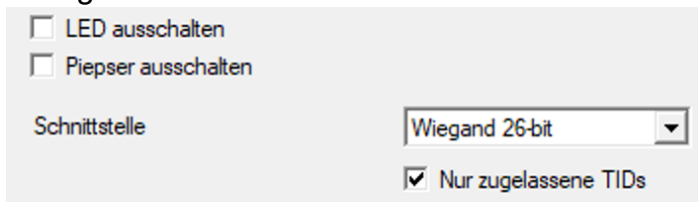
In den Eigenschaften der Schließung im Reiter Konfiguration/Daten auf den Knopf „Erweiterte Konfiguration“ klicken und in der erscheinenden Maske folgende Einstellungen vornehmen:



Die Maske über OK verlassen.

SmartRelais 3:

In den Eigenschaften der Schließung im Reiter Konfiguration/Daten auf den Knopf „Erweiterte Konfiguration“ klicken und in der erscheinenden Maske folgende Einstellungen vornehmen:



Die Maske mit OK verlassen.

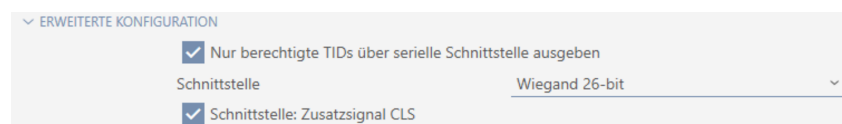
Konfiguration SimonsVoss SmartRelais in der AX-Manager-Software

Einstellungen vornehmen

für SmartRelais 3 und SREL.ADV identisch:

In den Eigenschaften der Schließung unter Konfiguration im Bereich „Erweiterte Konfiguration“ nebenstehende Einstellungen auswählen.

Die restlichen Einstellungen wie gewohnt vornehmen.



Programmierung

Im Anschluss an die Konfiguration bitte das SmartRelais wie gewohnt programmieren. Je nach verwendetem Modell:

- SREL.ADV über Aktiv-Programmiergerät Smart.CD
- SREL3 über USB-Direktverbindung oder über das Netzwerk.

Inbetriebnahme des Controllers

Werkseitig stellt das Antipassback eine Konfigurationsoberfläche auf dem eingebauten WLAN oder auf dem LAN-Port zur Verfügung.

Wollen Sie per WLAN konfigurieren, schließen Sie bitte **kein** LAN-Kabel an.

Inbetriebnahme per WLAN

Diese Oberfläche ist bei Werkseinstellungen ab Einschalten nach ca. 20 Sekunden für 2 Minuten verfügbar, falls kein LAN-Kabel angeschlossen ist.

Bitte verbinden Sie sich mit Ihrem Mobiltelefon/Tablet/Computer mit folgendem WLAN:

SSID: APBK
WLAN-Key: MyAntipassback

Bei erfolgreicher Verbindung können Sie mit dem Browser Ihrer Wahl auf folgender Webseite die Konfiguration vornehmen: (siehe Kapitel „Konfiguration“)

<http://192.168.4.1>

Inbetriebnahme per LAN

Der Controller bezieht seine IP-Adresse standardmäßig per DHCP aus dem Netzwerk. Bei Bedarf können Sie später im Abschnitt Config – Network auch eine feste LAN-Konfiguration mit IP-Adresse, Netmask, Gateway und DNS hinterlegen.

Bitte sehen Sie in Ihrem DHCP-Server nach, welche IP-Adresse der Antipassback-Controller bekommen hat.

Nun können Sie in Ihrem Browser mittels
<http://<IP>> die Konfigurations-Oberfläche aufrufen.

Alternativ können Sie das Config-Interface aufrufen über:
<http://<Seriennummer>>

oder

<http://<Seriennummer>.local>
soweit dies in Ihrer Infrastruktur unterstützt wird.

Sicherheits-Hinweis:

Bitte beachten Sie, dass zwar die WLAN-Verbindung verschlüsselt ist, aber der Web Server des Controllers aus Performance-Gründen auf eine Verschlüsselung verzichtet. Sollten Sie die Schnittstelle nicht nur zur Konfiguration nutzen, sondern auch zur Interaktion, gehen Sie auf Ihre IT zu und fragen nach geeigneten Maßnahmen wie z.B. VLAN.

Konfiguration

Beim Aufruf der Benutzeroberfläche des Antipassback-Controllers werden erst einmal nur Statusinformationen angezeigt.

Um die Konfiguration zu prüfen und zu ändern, ist eine Authentifizierung erforderlich. Klicken Sie hierzu auf den Knopf „Login“ und Sie werden nach Benutzername und Passwort gefragt.

Als Login stehen im Auslieferungszustand zur Verfügung:

Benutzer „user“ mit Passwort „user“

Benutzer „admin“ mit Passwort „admin“

Diese Website fordert Sie auf, sich anzumelden.

Benutzername

Passwort

Abbrechen

Anmelden

Im Folgenden werden sämtliche Optionen der Benutzeroberfläche besprochen, aber einige Optionen stehen dem Benutzer „user“ nicht zur Verfügung.

Seite System

Hier werden grundlegende Informationen zum Controller, Netzwerk, Zuständen und Zählern dargestellt.

Im Abschnitt „Network“ lässt sich auf einen Blick ersehen, ob der Controller mittels LAN oder WLAN kommuniziert, und welche IP-Adressen er erhalten hat.

Im Abschnitt States werden Zustandsinformationen zum Zeitpunkt des Ladens der Seite angezeigt:

„Mode“ – shared entry/exit oder split entry/exit

„Local Lock List: OFF oder ON

Zeitzone, Uhrzeit und die Zustände der beiden Türen.

Sowie der Status des letzten Firmware-Updates.

Unter Counters werden Statistikinformationen aus dem laufenden Betrieb dargestellt, und unter Diagnostics derzeit noch Warnungen und Parameter wiedergegeben.

Unten im Bereich Actions stehen Funktionen wie

„Open Entry“ – den Eingang für die Standard-Öffnungszeit öffnen

„OTA-Update“- Firmware-Update durchführen, siehe weiter unten

„View Locked“ – Anzeige der Liste der geblockten Transponder

„Reboot“ – startet den Controller neu

Seite Config – Abschnitt Network

Hier werden die Kommunikations-Einstellungen für den Antipassback-Controller festgelegt.:

Antipassback Controller

Version: 2.0.41 | Hostname: APBK-M3N9-X4AR-WUJRX | Serial: APBK-M3N9-X4AR-WUJRX

System **Config** Masters Locked Log LIVE Logout

Network

Hostname:

Network-Mode:

WiFi SSID:

WiFi Password:

AP auto-off after STA/LAN uptime (minutes, 0=off):

Time Zone:

Hostname:

bei einem frisch ausgeliefertem Antipassback-Controller steht hier üblicherweise die Seriennummer des Controllers, so wie in der Versionszeile genannt.

Gerne können Sie diesen Hostnamen an Ihre Bedürfnisse und Konventionen anpassen. Bitte beachten Sie, dass dieser Hostname in Ihrem Netz eindeutig sein muss. Konsultieren Sie hierzu ggf. Ihre IT-Abteilung.

Network-Mode:

Es stehen folgende Einstellungen für den Betrieb im Netzwerk zur Verfügung:

- auto: LAN bevorzugt, wenn kein LAN angeschlossen ist, dann per WLAN
- WIFI only: WLAN wird benutzt. Hierfür bitte SSID und Passwort pflegen.
- Lan only: LAN wird benutzt. WLAN-AP schaltet nach der eingestellten Zeit ab.

WiFi-SSID und WiFi-Password:

Bitte geben Sie ggf. Hier ihre WLAN-Zugangsdaten ein, an dem sich der Controller anmelden soll.

Use DHCP for LAN:

Ist diese Option aktiviert, bezieht der Controller seine LAN-Konfiguration per DHCP. In diesem Fall bleiben die statischen LAN-Felder ausgeblendet.

LAN Static IP, LAN Netmask, LAN Gateway und LAN DNS:

Wenn DHCP deaktiviert wird, erscheinen diese Felder. Alle vier Werte müssen vollständig im korrekten IPv4-Format eingetragen werden. Ungültige oder unvollständige Angaben werden nicht gespeichert.

AP auto-off after ST/LAN uptime (minutes, 0=off)

Nach dieser Zeit wird das WLAN des Controllers heruntergefahren, wenn LAN oder Ihr eigenes WLAN verbunden ist.

Time Zone:

Wählen Sie hier die Zeitzone, in der der Controller seine Uhrzeit stellen soll

Seite Config – Abschnitt Operation

Hier wird die Funktionsweise festgelegt.

| | |
|--|-----------------------------------|
| Operation | |
| Lock time (seconds, max. 2147483): | <input type="text" value="3600"/> |
| Door opener pulse (ms): | <input type="text" value="1000"/> |
| Delay before relay switches (ms, 0=no delay): | <input type="text" value="0"/> |
| Four-eyes window (seconds, 0=off): | <input type="text" value="0"/> |
| <input type="checkbox"/> Only lock when door contact opens within <input type="text" value="5"/> seconds (max. 15) | |
| <input checked="" type="checkbox"/> Exit opens always - even without an existing lock | |
| <input checked="" type="checkbox"/> Split entry/exit (entry: CH1 + DI1, exit: CH2 + DI2) | |
| <input checked="" type="checkbox"/> PresenceDashboard active | |
| Presence unknown after <input type="text" value="12"/> hours (0=never) | |
| Logging-Level: | <input type="text" value="info"/> |

Lock time:

Anzahl der Sekunden, wie lange der Transponder gesperrt sein soll
zulässiger Wertebereich 0s bis 2147483s (das sind über 24 Tage)

Door opener pulse (ms):

Wie lange soll der Relaiskontakt betätigt bleiben?

Für Schalttransponder oder Fluchtwegsicherungen üblicherweise ca. 800 ms,

für elektrische Türöffner: üblicherweise ca. 3000 ms - 8000 ms,

für Motorschlösser: je nach Hersteller und Modell: zwischen 500 ms und 8000 ms

Delay before relay switches:

Wartezeit, BEVOR das Relais einschaltet in Millisekunden.

In der Regel 0.

Eine Wartezeit ist möglicherweise nötig, um einer Kamera Zeit zu geben, die Vereinzlung anzufahren oder um dem Pförtner Zeit für ein Veto zu geben.

Four-eyes-window (seconds):

Innerhalb Welcher Zeit muss der zweite Transponder am Kartenleser vorgezeigt werden, um gewertet zu werden?

Üblicherweise 8-15 Sekunden

Standard ist 0, also Option deaktiviert.

Achtung: das Verwenden dieser Option deaktiviert die Blockierfunktion für die Transponder und kann nur alternativ zur Antipassback-Funktion eingesetzt werden!

Only lock when door contact opens within X seconds:

Falls die Möglichkeit besteht, dass die Vereinzelnungsanlage wieder verriegelt, bevor der Zutritt erfolgt ist, kann ein Türkontakt mit angeschlossen werden. Wenn sich dieser Kontakt ändert, wird dies als Öffnung gewertet. Der Transponder wird nur auf die Blockierliste gesetzt, wenn der Türkontakt innerhalb von den X Sekunden sich ändert.

Achtung: Ist diese Option gesetzt, ohne dass ein Türkontakt angeschlossen ist, wird die Antipassback-Funktion ausgehebelt!

Exit opens always – even without an existing lock:

Auch, wenn der gelesene Transponder nicht auf der Blockierliste steht, wird der Ausgang trotzdem geöffnet. Somit kann niemand eingesperrt werden. Im Log des Antipassback-Controllers sind diese Vorgänge separat erkennbar.

Achtung: ist diese Option aktiviert und die Option „Split entry/exit“ deaktiviert, dann wird bei Betätigung des Ausgangsleser der gemeinsame Kontakt des Eingangs geöffnet und unkontrollierter Zutritt ist ggf. möglich!

Split entry/exit:

Ist diese Option aktiviert, werden für Eingang und Ausgang unterschiedliche Relais angesteuert:

Eingang: CH1

Ausgang: CH2

Wenn die Option deaktiviert ist, werden bei Buchungen an beiden Lesern das Relais CH1 betätigt.

Achtung: ist diese Option deaktiviert und die Option „Exit opens always“ aktiviert, so wird das gemeinsame Relais CH1 auch bei nicht regelkonformen Betätigungen des Ausgangslesers freigegeben! Es könnte unerwünschter Zutritt entstehen.

PresenceDashboard active:

Wenn diese Option aktiviert ist, führt der Controller eine Anwesenheitsliste. Diese ist zugänglich im Menü unter dem separaten Knopf „Presence“. Hier ist ersichtlich, welche Transponder am Eingang gesehen wurden, und wann. Er ist dann als „present“ markiert. Wird der Transponder anschließend am Ausgang gesehen, wird er als „outside“ markiert. Falls der Transponder nicht innerhalb der Zeit „presence unknown after X hours“ am Ausgang gesehen, wird er trotz möglicher Anwesenheit auf „unknown“ gesetzt, da nicht ausgeschlossen werden kann, dass er anderweitig den Bereich verlassen hat.

Logging level:

Legt fest, wie intensiv das Logging stattfindet:

- Off: kein Logging
- Warning: (empfohlen) nur Fehlermeldungen und wichtige Warnungen
- Info: Statusinformationen werden zusätzlich notiert
- Verbose: Hier wird der Controller recht gesprächig und ausführlich.

Seite Config – Abschnitt MQTT

Hier können bei Bedarf die Einstellungen für den Betrieb mit MQTT-Servern wie dem Antipassback-Server von SMG vorgenommen werden.

MQTT

- Approval and opening-command by MQTT server
- Logging to MQTT server

In diesem Abschnitt werden bei Bedarf die Kommunikationsfunktionen mit MQTT-Servern wie dem Antipassback-Server verwaltet.

Standardmäßig sind beide Optionen nicht aktiviert. Wird mindestens eine der beiden Optionen aktiviert, erscheinen zusätzliche Felder, in denen Daten erfasst werden müssen.

MQTT-Server-IP / Hostname:

Hier muss die IP oder der Hostname des MQTT-Servers eingetragen werden.

MQTT-Server-Port:

Die Portnummer Ihres MQTT-Servers. Üblicherweise 1883.

MQTT-Socket-Timeout:

Um die Funktion des Antipassback-Controllers nicht auszubremsen, wenn der MQTT-Server nicht erreichbar ist, muss hier ein Timeout eingetragen werden. Dies kann zwischen 1 und 30 Sekunden liegen. Als guter Wert im LAN haben sich 2 Sekunden herausgestellt, im WAN oder VPN ca. 4 Sekunden.

MQTT-Server Username und MQTT-Server Password:

Bitte entsprechend Ihrem MQTT-Server eintragen.

Bitte hier ggf. Handbuch des Antipassback-Servers heranziehen !

Seite Config – Abschnitt Access Protection

Der Zugriff auf die Benutzeroberfläche des Antipassback-Controllers ist nur eingeschränkt möglich, und nach Benutzerberechtigungen gestaffelt.

Hier können die Passwörter für die Nutzer „user“ und „admin“ vergeben bzw. geändert werden. Im Auslieferungszustand heißen die Passwörter „user“ bzw. „admin“.

Sicherheits-Hinweis:

Bitte ändern Sie beide Passwörter!

Advanced Config Mode:

Bitte aktivieren Sie diese Option nur nach Aufforderung durch den SMG-Kundendienst. In dem (nach dem Speichern) erscheinenden Dialog können wichtige Felder zum Timing und Debugging geändert werden. Falsche Werte führen zu Fehlfunktion und können ggf. nur durch den SMG-Techniker wieder behoben werden !

Seite Config – Abschnitt Stylesheet

Stylesheet

You can customize the web interface CSS using the following button:

[Open Stylesheet Editor](#)

In diesem Abschnitt gibt es nur einen Knopf: „Open Stylesheet Editor“.

Dieser bringt Sie in eine Maske, in der das Default-Stylesheet aufgelistet ist, und ggf. in ein Textfeld übernommen und angepasst werden kann.

So kann das Erscheinungsbild der Benutzeroberfläche angepasst werden.

Bitte beachten Sie, dass das Default-Stylesheet bei Updates angepasst werden kann, aber die Anpassungen dann nicht automatisch mit in Ihr modifiziertes Stylesheet eingepflegt wird.

Bei Updates also bitte unbedingt prüfen, ob hier Änderungen erfolgt sind.

Seite Config – Abschnitt Service

Hier finden Sie in der aktuellen Firmware zwei Knöpfe:

Service

[OTA Update](#) [Clear Lock List](#)

OTA-Update und Clear Lock List

Clear Lock List:

Hiermit werden alle Transponder, die sich auf der Blockierungsliste befinden wieder entsperrt. Sicherheitshalber erfolgt eine kurze Rückfrage:

Clear lock list?

Abbrechen

OK

OTA-Update:

Springt auf eine eigene Unterseite zum Einspielen von Firmware-Updates.

OTA Firmware Update

Last Status: Ready

Keine Datei ausgewählt.

Use the compiled firmware file for the antipassback controller. After a successful upload, the device will restart automatically.

Mittels „Durchsuchen“ wählen Sie die Update-Datei, die Sie erhalten haben aus (*.bin). Anschließend mit „Start Update“ den Installationsprozess beginnen.

Achtung: Diese Funktion läuft mit Safari nicht stabil. Bitte benutzen Sie hier Firefox oder Chrome.

Achtung: ein Firmware-Update kann die Konfiguration und die Liste der Master-Transponder löschen – also bitte vor einem Update diese Informationen notieren.

Seite Masters

System Config **Masters** Locked Log LIVE Logout

Add Master Transponder

Master transponders are not added to the lock list and are always allowed locally.

TID:

Name:

Stored Master Transponders

| TID | Name | Aktion |
|------|----------|---------------------------------------|
| 4711 | Vorstand | <input type="button" value="Delete"/> |

Auf dieser Seite verwalten Sie die Master-Transponder. Master-Transponder werden nicht blockiert, sondern funktionieren immer. Über den Knopf „Save Master Transponder“ fügen Sie einen Transponder in die Liste hinzu. Hierzu muss TID ausgefüllt sein. Name ist ohne Funktion, macht es für Sie einfacher, später sie Transponder-IDs wieder zuzuordnen.

In der Liste bei „Stored Master Transponders“ werden alle registrierten (und aktiven) Master Transponder angezeigt und können mittels des „Delete“-Knopfes wieder zu normaler Funktion degradiert werden.

Die Inhalte dieser Liste werden im Controller-Flash-Speicher abgelegt und sind nach Reboot unverändert wieder vorhanden.

Seite Locked

System Config Masters **Locked** Log LIVE Logout

Locked Transponders

Local lock list is disabled because server approval is active.

Hier finden Sie die Blockierliste. Aufgelistet wird Transponder-ID und die Zeitspanne, für die noch blockiert ist. Ebenso finden Sie (als Admin!) Kommandos zur Verwaltung.

Seite Log

System Config Masters Locked **Log** LIVE Logout

Log View

Show entries:

100

Refresh

Authentication with user or admin.

```
[19:23:45 | 46:40:20] [MASTER] Saved: 4711 (Vorstand)
[19:12:19 | 46:28:54] [TIME] NTP sync successful, local time: 2026-04-20 19:12:19
[19:12:19 | 46:28:54] [MQTT] Connected
[19:12:19 | 46:28:54] [TIME] NTP sync started, TZ=Europe/Berlin
[19:12:19 | 46:28:54] [CFG] advanced_config mode changed: ON -> OFF
```

Ihr Antipassback-Controller listet hier auf, was er wann getan hat, oder was passiert ist. Wie ausführlich, das hängt von der vom Log-Level auf der Config-Seite ab.

Seite LIVE

System Config Masters Locked Log **LIVE** Logout

Live Status

| | | |
|--|---|---|
| Auto-Refresh: 2 s Pending Door Commit: idle | Entry Relay: OFF Exit Relay: OFF | MQTT Entry Approval: idle MQTT Exit Approval: idle |
|--|---|---|

Recent Live Events

| Time | Direction | TID | Decision | Detail |
|---------------------|-----------|-----|----------|--------|
| No live events yet. | | | | |

Diese Seite stellt die aktuellen Geschehnisse verständlich und übersichtlich dar. Sie ist zur Inbetriebnahme und zur Fehlersuche sehr hilfreich.

Achtung: Da diese Seite alle 2 Sekunden neu lädt, sollte sie bitte unbedingt wieder verlassen werden, wenn sie nicht mehr benötigt wird, da sie dem Antipassback-Controller viel Rechenleistung entzieht.

Logout

Mit diesem Knopf melden Sie sich von der Konfigurations-Oberfläche ab, und es erscheint wieder die minimalistische Status-Seite.