

Introduction to anti-passback feature used in Access Control System

Anti-passback principles:

Tailgating is when one user enters with a valid card read, and several people enter without using their cards. **Anti-passback** can be implemented to help alleviate this problem, by tracking whether the card is inside the secure area or outside. The anti-passback feature is most commonly used in this situation: where there is both an “in” reader at the entry gate and an “out” reader at the exit gate. The anti-passback feature requires that for every use of a card at the “in” reader, there be a corresponding use at the “out” reader before the card can be used at the “in” reader again. So long as the sequence is “in – out – in – out – in - out”, everything works fine. However, if a user swipes his card at the “in” reader to get in, and then passes his card back to a friend, the card would not work the second time when it was swiped by the friend. The attempt to use the card a second time would create an “in – in” sequence that is a violation of the anti-passback rules, and this is why access would be denied.

Some typical situations:

- A. When someone enters the entry gate following others without his own authentication, he or she cannot get through the exit gate through his own authentication even his authentication is a valid one. It's the same when someone gets through the entry gate following others without his own authentication, he or she cannot get through the entry gate through his own authentication.
- B. When someone gets through the gate, and then he or she “passes back” that card, say through a window or another door, to an unauthorized user, who then uses the same card to access the building, he or she cannot get through. The password authentication is the same.
- C. When someone get through the Fingerprint/Card/Password authentication, he or she doesn't access, then he or she cannot get through the gate even the authentication is a valid one.

(The three anti-passback typical situations above are supported by Anti-passback function of the Access Control Terminal ZD2F20.)

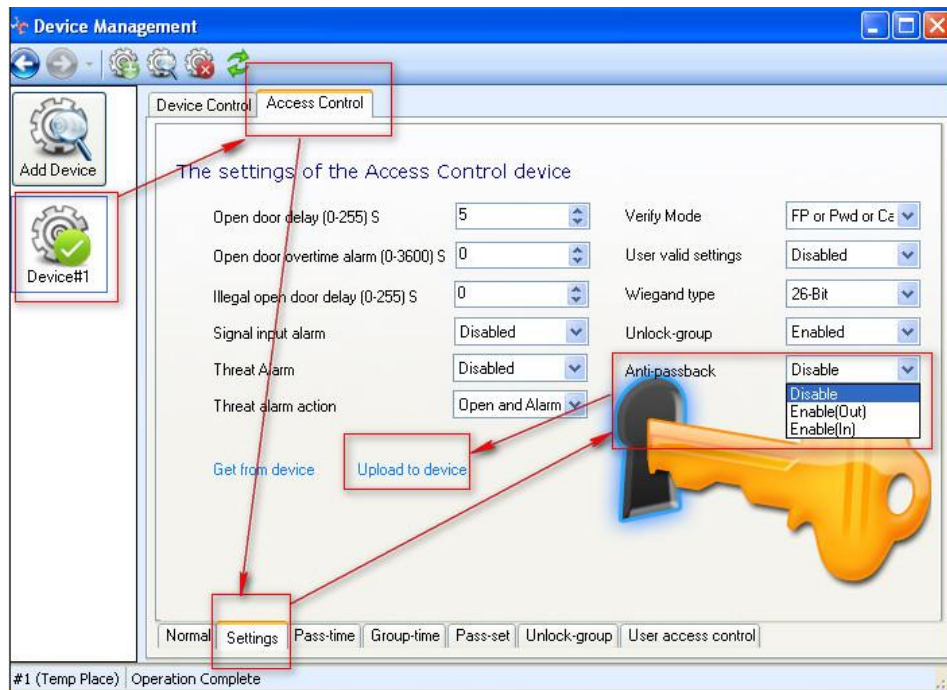
To use anti-passback, areas must be set up first:

- **Apply the anti-passback function in ZD2F20**

Method 1: set the anti-passback through the RIMS software.

Connect the ZD2F20 to the RIMS software (the version must be or upon V1.0.1.3210).

Click **Device Management** -> **Access Control** -> **Settings** to find out the **anti-passback**. Then set the configuration option, then click **upload to device**.

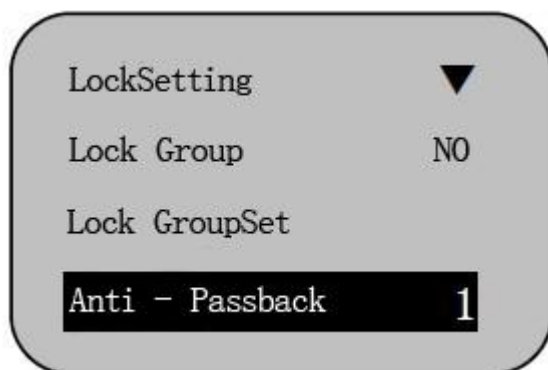


Instructions:

- 1) **Disabled:** the anti-passback is ineffective.
- 2) **Enable (OUT):** it makes the ZD2F20 Access Control Reader as the “In” Reader, and the record in the ZD2F20 is the “IN” one. The authentication record in the Sensor is the “OUT” one.
- 3) **Enable (IN):** it makes the ZD2F20 Access Control Reader as the “OUT” Reader, and the record in the ZD2F20 is the “OUT” one. The authentication record in the Sensor is the “IN” one.

Method 2: set the anti-passback through the terminal.

Press **MENUE** -> **Setup** -> **Lock Setting** -> **Anti-passback**, set the configuration, and then **save** the settings.



Parameter instruction in Access Control Terminal ZD2F20:

| Parameter in ZD2F20 | Parameter in RIMS | Input of WG Sensor | Authentication in ZD2F20 |
|---------------------|-------------------|-----------------------------------|---|
| NO | Disable | Disable | Attendance function keys F1-F4 is valid |
| 1 | Enable(OUT) | Record in Sensor is the "OUT" one | Record in ZD2F20 is the "IN" one |
| 2 | Enable(IN) | Record in Sensor is the "IN" one | Record in ZD2F20 is the "OUT" one |

ATTENTIONS:

When the ZD2F20 enable the anti-passback function, it will be a professional access control terminal, and the attendance function keys F1-F4 on the terminal are invalid automatically. (When disable the anti-passback function, the attendance function keys are valid automatically.) The records will be marked as "IN" or "OUT", or maybe the "illegal" one.

When enable the anti-passback function, it cannot authenticate again and again at the same time whatever on the Access Control Terminal ZD2F20 or the Wiegand Sensor. All the authentication records should be in the sequence of "in – out – in – out – in - out" strictly. Or the records will be recorded as "Illegal" ones.

- **Implement of Anti-passback**

Proposal A: one Access Control Terminal ZD2F20 + one ID/IC Sensor with the Wiegand signal output.

Scene A: install the Access Control Terminal ZD2F20 outside the door while installing the ID/IC Sensor inside. Configure the anti-passback as "Enable (OUT)", (the anti-passback in the terminal ZD2F20 is configured as "1", the sensor is the OUT mode.) people authenticate on the terminal ZD2F20 with Fingerprint, card or password to get through the entry gate, while authenticating on the ID/IC Sensor by swiping the card to get through the exit gate. All the authentication records should be in the sequence of "in – out – in – out – in - out" strictly.

Scene B: install the Access Control Terminal ZD2F20 inside the door, while installing the ID/IC Sensor outside. Configure the anti-passback as "Enable (IN)", (the anti-passback in the terminal ZD2F20 is configured as "2", the sensor is the IN mode.) People authenticate on the terminal ZD2F20 with Fingerprint, card or password to get through the entry gate, while authenticating on the ID/IC Sensor by swiping the card to get through the exit gate. All the authentication records should be in the sequence of "in – out – in – out – in - out" strictly.

Proposal B: two Access Control Terminal ZD2F20, one to be the (fingerprint / card / password) Sensor, and the scene description is the same with the one in the proposal A.

If you have any problems, please contact Realand.

Website: <http://www.realandbio.biz>

E-mail: realand@realandbio.com ; realand.biz@gmail.com;