



# Anti-Passback Management

## PREVENTING CARD PASSBACK

The purpose of anti-passback is to prevent a card holder from passing back his or her card to a second person to gain entry into an access-controlled area.

The anti-passback features of the Security Management System can be used to maximize security, prevent fraudulent use of cards and maintain an accurate record of the number of people who are currently in any one area (possibly for safety reasons).

The Security Management System offers two types of anti-passback: zonal and timed. Timed anti-passback is normally used to control passback around the periphery of a building or single area within a building, whereas zonal anti-passback can control passback between multiple areas within a building.

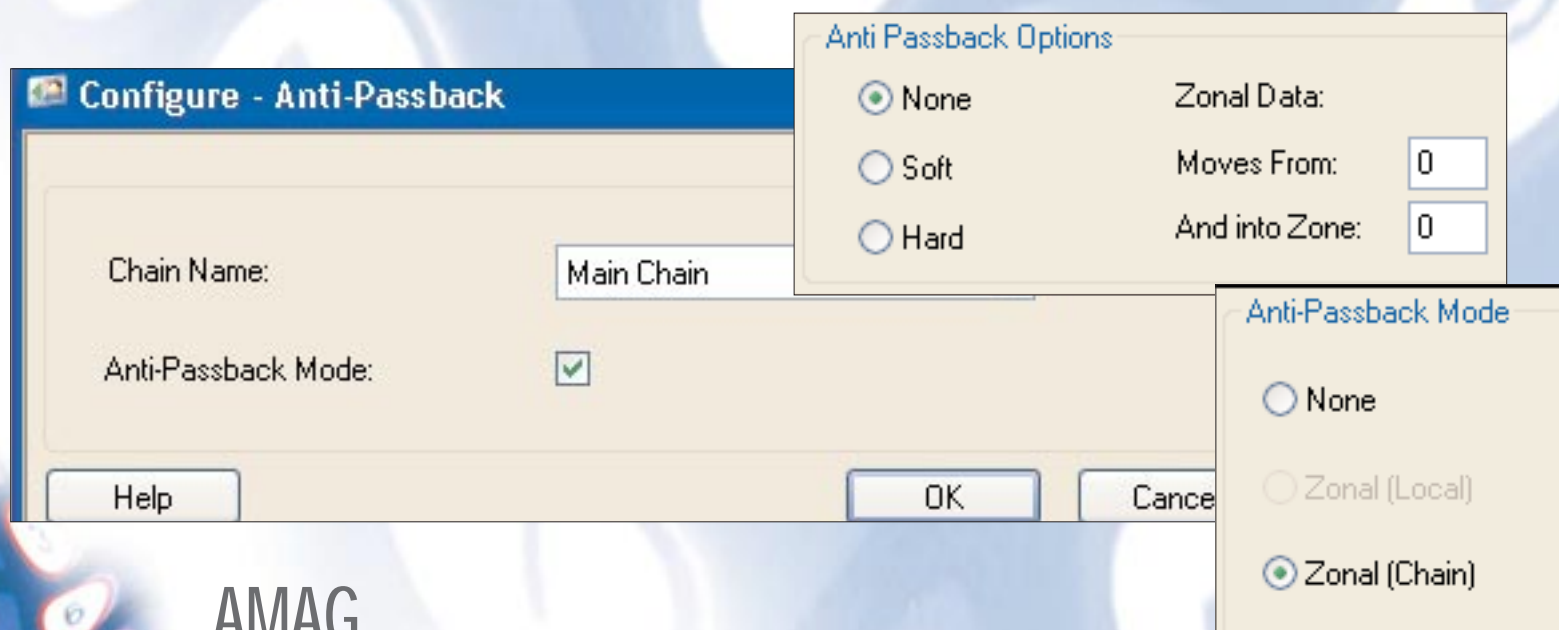
Anti-passback requires both an entry reader and exit reader to enable the system to know whether a card is in or out of an anti-passback-protected area. In addition, a turnstile or other similar barrier is required on the entrance and exit to prevent people from "tailgating".

Each reader included in anti-passback can be set up as a "hard" or "soft" anti-passback reader. Both types of reader log any infringement of the anti-passback rules, but a soft anti-passback reader allows access, a hard anti-passback reader does not.

Note: An alternative method of setting up a basic anti-passback system is to issue cards that can be used only once (as set up in the Card Holders screen). This system may be suitable in cases where the card holder always reports to an operator before gaining access, such as at visitor reception areas.

## Key Features

- Timed and zonal anti-passback methods are available
- Maximizes security
- Prevents fraudulent use of cards
- Maintains an accurate record of the number of people in an area
- Can prevent access when passback is detected
- Anti-passback checking can be disabled and re-enabled using the Configure/Anti-Passback screen
- Anti-passback can be reset for an individual card holder or for all card holders





# Anti-Passback Management

## PREVENTING CARD PASSBACK

### ● Zonal Anti-Passback

- Each reader configured for zonal anti-passback has a "from" and "to" zone number
- An anti-passback alarm/event is generated if a card's recorded "from" zone does not match the "from" zone of the reader that is being used
- Each zonal anti-passback system can have up to 63 zones
- For LAN chains, any reader in any LAN chain can be in the same anti-passback system
- For hardwired chains, readers in the same chain can be in the same anti-passback system

### ● Timed Anti-Passback

- Each reader configured for timed anti-passback has a "passback timeout" period
- An anti-passback alarm/event is generated if a card is re-used at another antipassback reader within the specified time period
- Time period is configurable between 1 and 63 minutes
- Exit readers (time period set to 0) can be used at any time without causing an alarm/event
- Use of an exit reader resets the time period for re-use of card to zero
- Any reader connected to the same node can be in the same timed anti-passback system

### ● Other Features

- Card Holders screen enables anti-passback to be reset for an individual card holder
- The "Set All Cards to Neutral" manual/scheduled command enables anti-passback to be reset for all card holders
- The Configure/Anti-Passback screen enables anti-passback to be enabled or disabled for a selected chain
- Multiple anti-passback systems can be set up from the same security management system
- All anti-passback violations are logged as alarms or events
- Readers set up for "hard" anti-passback prevent access if an anti-passback violation is detected
- Readers set up for "soft" anti-passback allow access if an anti-passback violation is detected

Note: Anti-passback is not available for readers on dial-up chains or connected to elevator nodes.

