Gallagher Command Centre

Command Centre Anti-Passback and Anti-Tailgating

Technical Information Paper

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2026. All rights reserved.

Document History

Edition	Date	Comment
1.0	20/11/2016	First Release
2.0	24/03/2026	Updated to new Template

1 Background

Gallagher Command Centre provides comprehensive methods for managing people movement.

This paper explains the features available as part of anti-passback and anti-tailgating.

Anti-passback and anti-tailgating are complementary features. Anti-passback controls entry process whereas anti-tailgate controls exit processes.

2 Compatibility

- Gallagher Command Centre (All Versions)

3 Definitions

3.1 Anti-passback

A card used to access a zone may not be used for re-entry to the same zone unless it has been used to exit from that zone. The purpose for this feature is to stop a person already in the zone from passing their card back to a second person to allow the second person to enter the same zone on the one card.

The terms “hard anti-passback” and “soft anti-passback” are often used in system specifications.

3.1.1 Hard anti-passback

Hard anti-passback means that access is not permitted and an alarm is raised if an attempt to break the anti-passback rule is made.

3.1.2 Soft anti-passback

Means access is granted but an alarm may (or may not) be raised if the anti-passback rule is broken.

3.2 Anti-tailgating

A card cannot be used to exit a zone unless it is recorded as being present in the zone.

Copyright © Gallagher Group Limited

4 Implementation

4.1 Anti-passback modes

Command Centre allows three different modes for anti-passback.

The access zone may be set up to;

(i) be “hard” where access is denied and an alarm is raised,
(ii) allow access but generate an alarm, or
(iii) allow re-entry to specified access groups.

Note: Anti-tailgating may also be set up in one of these 3 modes.

The first two options provide flexibility in the way the system is to be operated for all card users. The third option allows specific groups of people to be excluded from the anti-passback rules. This is useful for people with specific responsibilities such as guards and people with exclusive operational needs.

4.2 Where to use these features

These features are often a requirement for high security sites. The reasons for restricting people from a zone may be for reasons of information security or access to controlled materials.

The card user may have the required security clearance to access information in an area but if the card is passed back to a second person, does that person have the required clearance? Do you need to know exactly who has entered an area?

As a backup to this situation, if a person is illegally in an area, you will want to know when they are attempting to leave. An alarm resulting from the attempt to leave could be used to alert a guard, who can then escort the person from the area.

5 System Specification Example

When used with **Zone Counting**[1] and **Dual Card Authorisation**[2] a system can be set up to manage the number of people in a specific zone.

A system specification might be:

If access to an area of a site is required, the system must only allow two or more people to be present at any time.

a. The access door is set up to require dual card authorization for the first entry attempt.
b. When the two people have entered, the zone count records two people as being present. Because the zone count has incremented to two, the door mode changes to secure mode, meaning single card entries are permitted.
c. Each additional person entering the door increments the zone count for the area.

Copyright © Gallagher Group Limited

d. As people leave, the zone count decrements.
e. When the zone count reaches two people present, the exit mode reverts to dual card authorization.
f. If the two remaining people exit the zone as required, the system treats the total process as being legitimate. The zone count records as zero.
g. If a person remains in the zone and then attempts to exit, the exit will be refused. An alarm will be generated for the appropriate action to be taken.

[1] Zone Counting – Each valid entry through a door requires a valid card and the door must be opened. This will increment a counter for the zone

[2] Dual Card Authorisation – Two valid but different cards are required to access a door.

Copyright © Gallagher Group Limited