SIEMENS

SiPass®
integrated

Anti-Passback

- **Hard, Soft and Timed Re-entry Exclusion Anti-Passback modes**
- **Maintain awareness of the location of cardholders at all times**

An important part of access control is not only monitoring the authenticity of cardholders entering a facility, but also ensuring that their movements throughout the facility do not contravene your security requirements.

Complementing the security benefits of knowing where your cardholders are at all times are additional advanced features, including fail-safe Anti-Passback in case of communications disruption, Mustering reports for emergency situations, an operator-controlled forgive feature for passback exceptions and a complete Audit Trail history of all Anti-Passback transactions.

Features

- Definable areas with multiple entry and exit points
- Hard, Soft, and Timed Re-entry Anti-Passback modes
- Passback violation alarms
- All passback events recorded in the Audit Trail
- Configurable, enforceable population limits for areas
- One-click Mustering reports
- Trigger Events based on area population limits

Benefits

Anti-Passback allows you to define the natural zones, or areas, within your facility which are accessed by card readers. As cardholders move through these areas by badging their card, SiPass automatically logs their location.

This allows you to enforce a strict “path“ throughout your facility, by ensuring that cardholders cannot enter or leave an area to which they have gained, or are attempting to gain, unauthorised access.

It also allows SiPass to maintain an exact count of the number of cardholders in any of the areas at your facility. When the specified limit for the area has been reached, SiPass can raise an alarm, start an automated event task or routine, and/or prevent further cardholders from entering the area until another cardholder leaves.

You may also elect to strictly enforce your Anti-Passback rules and deny access (Hard Anti-Passback) or merely alert the operator to the violation, but permit access (Soft Anti-Passback). Either way, the access attempt and the result are recorded in the Audit Trail.

In the event of a communications failure between the Advanced Central Controller (ACC) and the SiPass Server, the ACC is able to continue enforcing the Anti-Passback rules for the areas that it oversees. This intelligent, stand-alone behaviour ensures that communications loss does not jeopardize the security of any facility under SiPass access control.

Required

One of the following core packages is required:

Type	Part no	Designation
ASL5000-ST	6FL7820-8AA00	SiPass Starter
ASL5000-SE	6FL7820-8AA10	SiPass Standard Edition
ASL5000-OA	6FL7820-8AA20	SiPass Optima

Details for ordering

SiPass Anti-Passback is a feature of all SiPass core packages.

Issued by
Siemens Building Technologies
Fire & Security Products GmbH & Co. oHG
D-76187 Karlsruhe

www.sbt.siemens.com

Printed in the Federal Republic of Germany
on environment-friendly chlorine-free paper.

Document No. **A24205-A335-B224**
Release 09.2004