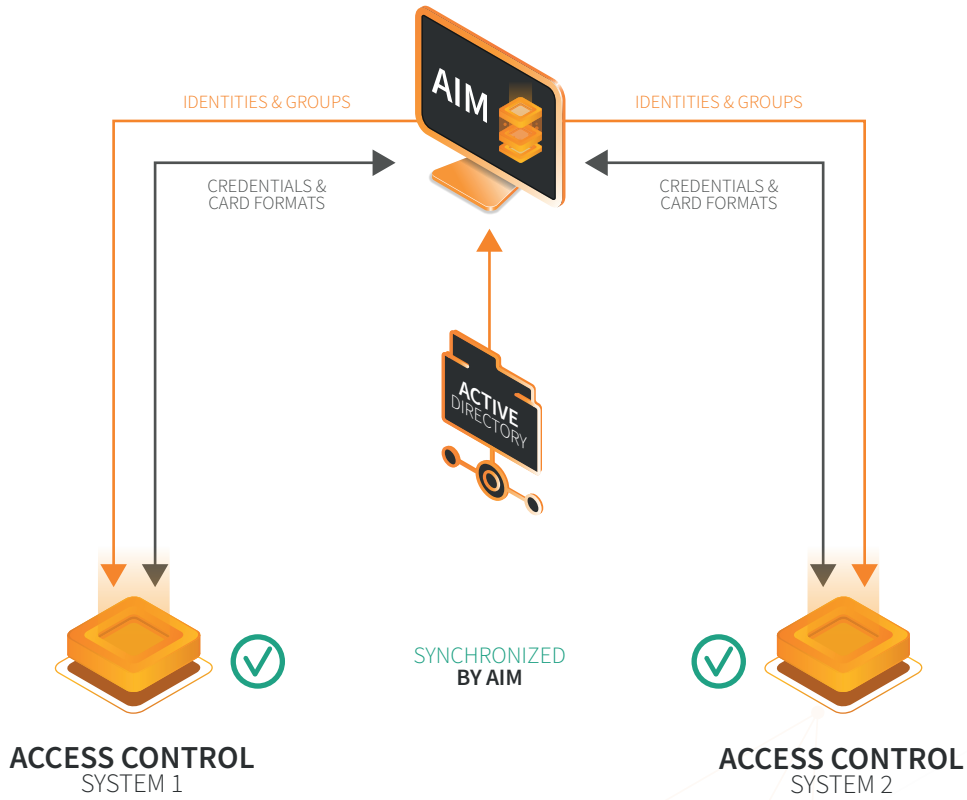# AIM

ACCESS AND IDENTITY MANAGEMENT

advancis

HOW DOES AIM WORK?

ADVANCED IDENTITY MANAGEMENT

The Advanced Identity Manager offers an optimal solution for the integration of multiple access, identity and biometrics systems in one platform.

AIM's main function is to ensure that the logical and physical access privileges associated with an employee's role are always synchronized.

AIM

IDENTITIES & GROUPS   IDENTITIES & GROUPS

CREDENTIALS &   CREDENTIALS &
CARD FORMATS   CARD FORMATS

ACTIVE
DIRECTORY

SYNCHRONIZED
BY AIM

ACCESS CONTROL
SYSTEM 1

ACCESS CONTROL
SYSTEM 2

Identities (card holders/users) and group rights are taken over from a leading data source – in this example from the Active Directory

Credentials (card information and formats) are synchronized between all access control systems

---

Synchronization of all systems

Synchronization of identities and credentials of the connected access control systems.

Leading data source

User identities and groups are propagated from a leading data source and then distributed to all systems. Leading data sources can be the Active Directory, an access control system, AIM self-registration, existing HR applications or in-house solutions currently in place.

Flexible integration

AIM supports open protocols such as PLAI, a RESTful API as well as proprietary interfaces for the connection of access control systems, biometry and other identity and visitor management systems from different manufacturers.

AIM Mobile App

With the AIM Mobile App, mobile credentials from different manufacturers can be used and managed in a unified way. This eliminates the need to carry an access card or badge.

KEY BENEFITS

UNIFIED ACCESS CONTROL

Preservation of existing systems

AIM enables to continue using the existing access control infrastructure without having to forego the benefits of standardized processes and centralized data maintenance.

Easy administration

AIM synchronizes all user and group data as well as card formats and card IDs of the connected access control systems.

This significantly eases the management effort of user and group data, as adjustments only have to be made in one system and no longer in many different ones.

Increased security

The AIM web user interface provides a unified overview of the synchronization status of all connected systems.

This facilitates the removal and offboarding of former employees ensuring all access cards and clearances can be updated, disabled or removed in a centralized way which minimizes the chance of unauthorized access to buildings and critical assets.

In addition, it is possible to filter centrally according to authorization groups in order to e.g. proactively check access rights for highly secured areas or to block the corresponding card directly.

Single badge usage

By synchronizing the card information and all card formats, access or authorization can be enabled with just one card for all connected systems (provided that the used cards support this).

LICENCE MODEL

FREE SCALABILITY – FROM SMALL TO COMPREHENSIVE SOLUTIONS

	EXPRESS	BASIC	PROFESSIONAL	ENTERPRISE
Interfaces	up to 3	up to 5	up to 10	unlimited
Users	up to 3,000	up to 5,000	up to 25,000	unlimited

INCLUDED IN EVERY LICENCE

- Web user interface
- System environment monitoring
- Card holder management

advancis