AIM

AIM delivers a secure and
standardized approach to integrating
identity and access control

AIM

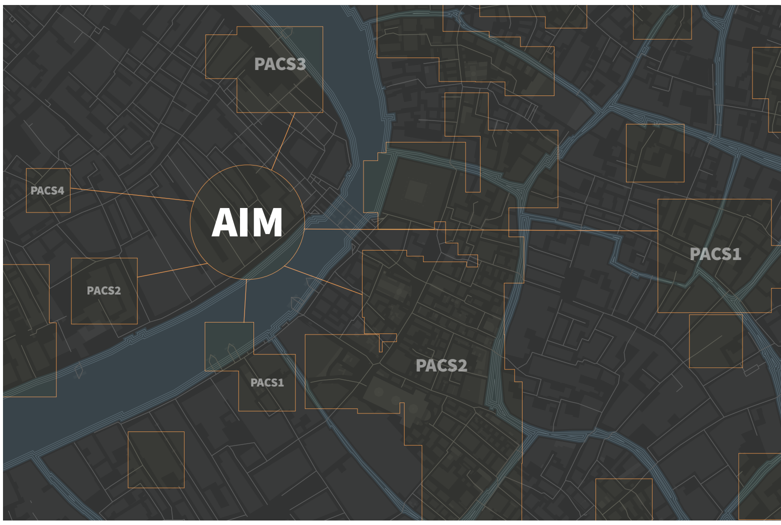
CONTENTS

WHAT IS AIM?

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

AIM's main function is to ensure the logical and physical access privileges associated with an employee's role are always synchronized. This enables a company to ensure a person is physically present before permitting access to databases or applications.

AIM supports all forms of business from multinationals with locations across the globe to multi-tenancy environments.



ACCESS CONTROL SYSTEM INTEGRATION

- Single badge usage
- Card format management
- Partition management

IDENTITY MANAGEMENT

- One time enrolment
- Physical and logical user, groups and role management
- Active directory support

VARIOUS ADDONS

- HR system support
- Visitor management support
- Two factor authentication

ADVANTAGES OF AIM

ACCESS MANAGEMENT

Ensuring the logical and physical access privileges associated with an employee's role are always synchronized. This enables a company to verify a person is physically present before permitting access to buildings and assets.

INTEROPERABILITY

AIM enables interoperability by automating the process of enabling access cards, credentials or roles associated in one vendor's access control system to be used at entry points associated with a different access control system or biometrics system.

ADMIN EXPERIENCE

The use of AIM and the associated harmonisation considerably reduces the administrative effort for the initial administration and the ongoing maintenance of user profiles and group rights.

USER EXPERIENCE

Reducing multiple access cards for users and ensure correct access to privileged assets is assigned.

BUSINESS CONTINUITY

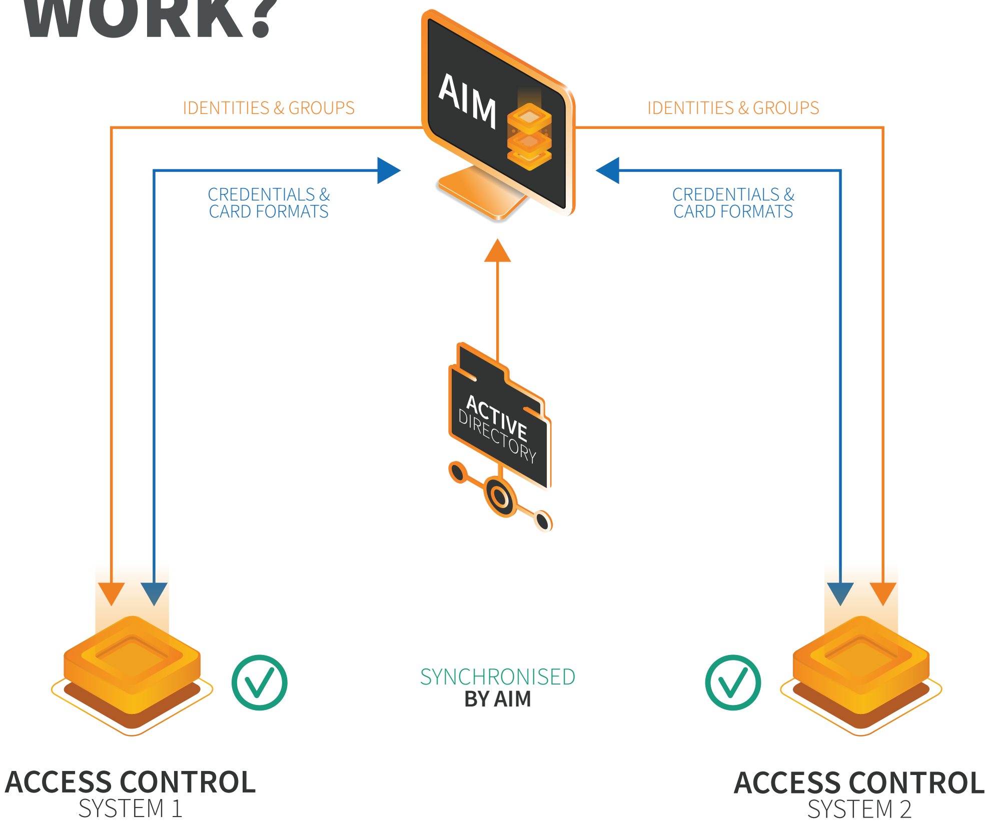
Organisations can centrally manage access and quickly identify potential security threats related to duplicate badges and users.

AIM also enables the continued use of existing access solutions without having to give up the advantages of unified processes and central data maintenance.

PROBLEMS ORGANISATIONS FACE

- Users having multiple identities across security systems that do not communicate with each other.
- Multiple owners of a user's identity in more than one access control system which can be amended, creating conflict without each owner being aware nor notified.
- Manual process to reconcile user's multiple identities which have been created on more than one system in the same organisation.
- Changes that are made in one system are not registered in the other, resulting in a risk of users gaining unauthorised access.

HOW DOES AIM WORK?



Identities (cardholders/users) and group rights are taken from an authoritative data source - here from the active directory

Credentials (card information & formats) are shared between all systems

AIM supports open protocols like PLAI and proprietary integrations offering a platform agnostic RESTful API for managing and brokering identities across multiple platforms

The API needs to be exposed via a web service over HTTPS.

Mapping of employee directory systems or in most cases LDAP entities such as users, groups, organisational units which are then integrated into physical access or biometrics systems.
Containers mapped into the access control space.

AIM is “in charge” of the access control system that are registered against it.

The adapter must expose a RESTful web service with specific interfaces and behaviour to be compatible with AIM.

OPEN STANDARDS VS. PROPRIETARY INTERFACES

While proprietary integration is still required, most of the work can now be handled in a standardised way. This reduces project costs and resources required throughout whilst eliminating the need to do multiple integrations.

PROPRIETARY

- ⊕ Can do complex deeper integrations

- ⊖ Additional engineering cost
- ⊖ Different API’s libraries
- ⊖ Overhead in retaining knowledge
- ⊖ Difficult deployment
- ⊖ Subject to change

OPEN

- ⊕ One time development cost
- ⊕ Improved compatibility
- ⊕ Less training involved
- ⊕ Easy configuration and deployment

- ⊖ Limited to CRUD (create, read, update and delete) operations
- ⊖ Sometimes misses system specific functionality

KEY BENEFITS

Using AIM as a central administration system simplifies and accelerates the entire identity management process.

- ✓ Improve security and compliance by centrally managing access to critical infrastructure and assets via one source of authority.
- ✓ Introduce one identity across the entire enterprise with credentials that can be used on multiple security systems, meaning one credential will work across all locations.
- ✓ Defer capital cost of standardising on one access control system by supporting interoperability of market leading access control technologies and biometrics systems
- ✓ Reduce migration costs by utilising Match user selection feature which identifies anomalies, duplicates a name changes to ensure data integrity across the different connection platforms.
- ✓ Seamless migration of user Access Control System databases: If a migration is your decided path, AIM consolidates the security systems via the migration process by identifying duplicate records and ensuring on-demand synchronisation so the data- set is always up-to-date.
- ✓ Less administrative time spent on badge loss or duplicate cards. Reduce operational administration through easy aggregation of changes to users, credentials, locations and roles.
- ✓ Off-boarding and changes to corporate structure: In case of on-boarding new teams, acquisitions or off-boarding current employees, AIM enables these processes to be centrally managed ahead of time in a coordinated manner where access to IT and physical security are synchronised ensuring HR processes are followed.
- ✓ Physical Security Information Management (PSIM): Extend your security coverage to include management of critical events and door control.
- ✓ Provide reporting on user activity and fault reports.
- ✓ Temporary access and visitor management: Provide flexible capabilities for managing visitors, contractors and individuals who require temporary access to your facilities.
- ✓ Introduce one identity across the entire enterprise with credentials that can be used on multiple security systems, meaning one credential will work across all locations.
- ✓ Facilitate the provision of one badge which provides access across all locations (for supported hardware).
- ✓ Facilitate the use of mobile credentials for supported hardware.

AIM LICENCE MODEL

	EXPRESS	**BASIC**	**PROFESSIONAL**	**ENTERPRISE**
Max. adapters	up to 3	up to 5	up to 10	unlimited
Max. users	up to 3000	up to 5000	up to 25000	unlimited

INCLUDED IN EVERY LICENCE

- ✓ Access control system credentials synchronisation
- ✓ Cardholders management
- ✓ Credentials management
- ✓ Groups and roles management
- ✓ Events streaming for access control environment health
- ✓ Match user selection across different security systems

advancis

WWW.ADVANCIS.NET