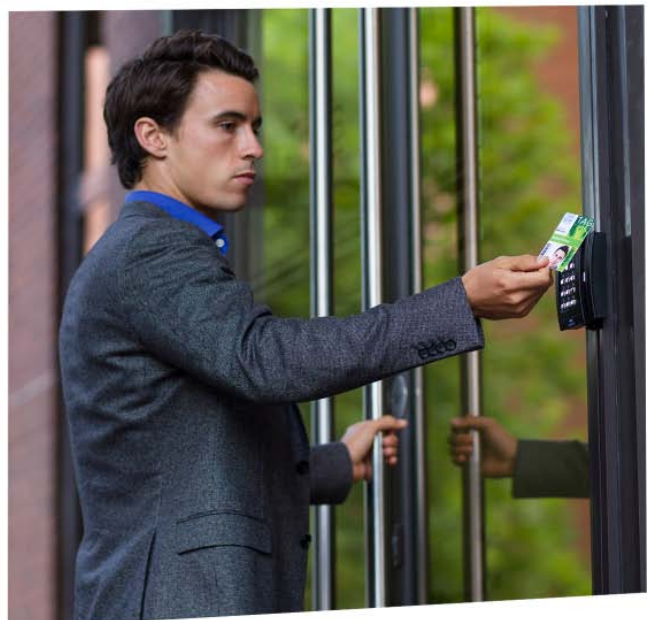# EdgeConnector

Door access control truly integrated into the IT domain

Enhanced security   **Simple management**   **Easy installation**

The benefits of truly integrated physical and logical security

EdgeConnector seamlessly integrates the management of physical door access into your existing IT-user administration tools, typically based on Microsoft Active Directory, with no need for an additional database.

The streamlined EdgeConnector architecture delivers converged, role-based, physical and logical access decision-making in real-time without complexity.

EdgeConnector is intrinsically scalable through its utilization of existing network infrastructure; providing access control for a server rack to whole buildings across multiple sites worldwide, and for any number of users.

Enhanced security & compliance

- **Remove risk.** Rescind unified physical and logical access rights in real-time, without the delays inherent in updating separate databases and control systems.

- **Limit sensitive data and application access to secure areas.** Each user's door interactions identifies their whereabouts, enabling IT system access to be controlled based on their location.

- **Demonstrate compliance.** Audit trail reporting can show each user's physical movements and IT system access history combined.

- **Exploit the latest card security technologies.** Concurrent operation with different card types enables the phased migration to new and more secure card technologies.

"Organizations must limit physical access to information systems, equipment and the respective operating environments to authorized individuals"

EU GDPR   PCI-DSS   ISO27001
Sarbanes-Oxley   FISMA
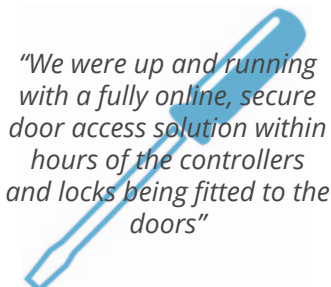**HIPAA   ISAE3402   SSAE16**

Simple management

- **No additional databases.** No duplication of user information. No maintenance, synchronization or administration of separate data.
- **Unified role-based security.** Add door access rights to existing IT security groups.
- **Use existing ID management applications.** Immediate integration with any system that uses Active Directory.
- **Easy-to-use interface.** A secure client application allows day-to-day tasks, such as user and visitor maintenance, to be managed by front-desk staff.
- **Fully scalable as standard.** Unlimited numbers of users and unlimited numbers of sites, anywhere globally on the WAN.
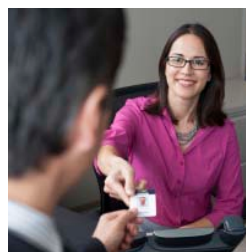
"Simple – it just works"
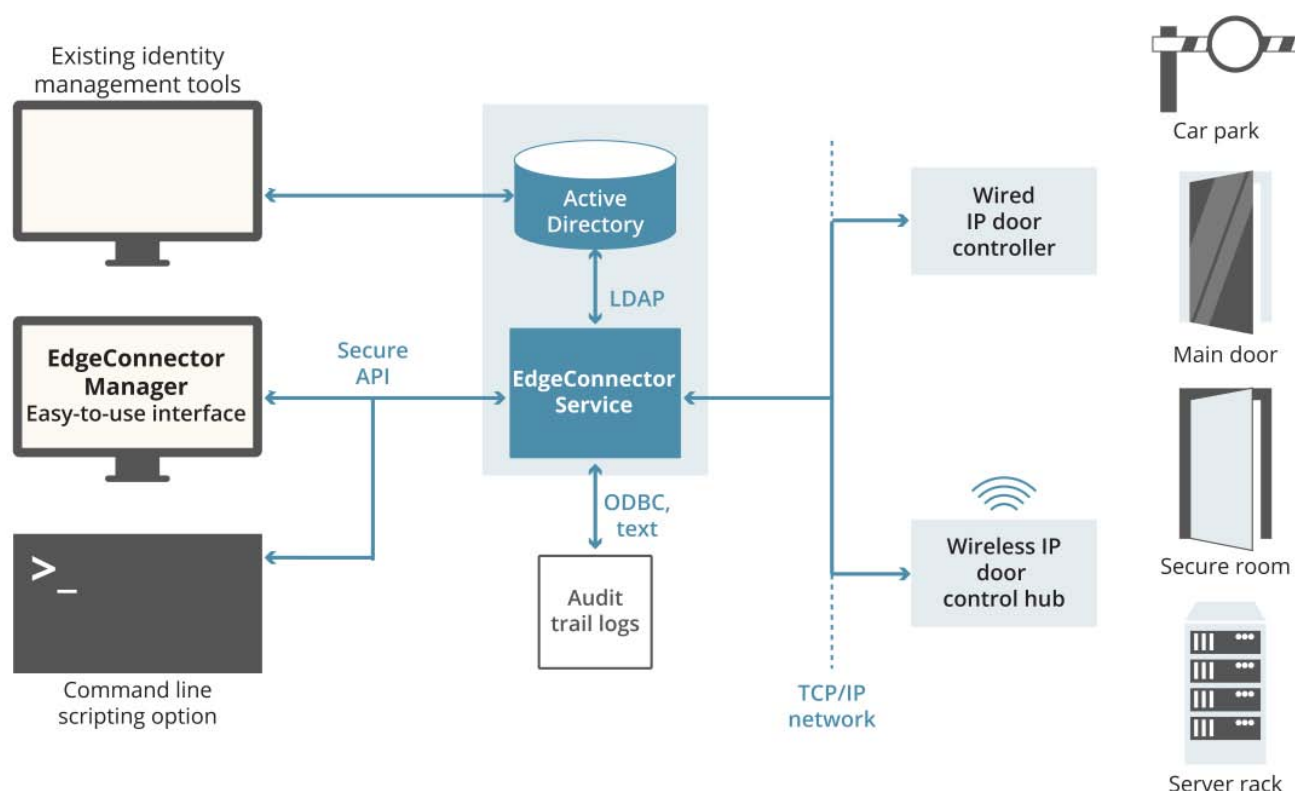
Easy installation

- **Quick set-up.** Using the existing user directory and server infrastructure avoids adding and populating new databases.

- **Zero cabling.** Wireless door locks (with integrated card readers) can be fitted to existing doors and server cabinets with little or no modification. Where wired door controllers are needed, Power-over-Ethernet (PoE) solutions require network cabling only.

- **Use existing cards.** Compatible with an extensive range of industry standard door access cards and readers.

- **Installation choice.** Use our trained installers or arrange your own installation; using our comprehensive documentation.

"We were up and running with a fully online, secure door access solution within hours of the controllers and locks being fitted to the doors"

The EdgeConnector solution architecture

EdgeConnector Manager

A secure client application that provides an easy-to-use interface for the delegated management of users, visitors, doors and schedules by non-IT staff; without compromising directory security. Other identity management applications that integrate with Active Directory can also be used for day-to-day management.

EdgeConnector Service

Typically runs on an existing Active Directory domain controller and processes door access requests from door controllers and hubs in real-time, unlike traditional access control systems. This enables various converged security applications, including location-based logon restriction and global anti-passback protection.

Doors and cabinets

Any combination of wireless control hubs and wired IP door controllers can be used to connect any number of doors, located anywhere on the WAN. The latest encryption standards secure all access control communication over the network. Wireless door control hubs can each manage multiple doors and offer the greatest ease of installation. Wired controllers each manage a single door and provide wider configuration options, such as fire and intruder alarm integration, plus in-and-out reader operation.

System compatibility

User directory	Microsoft Active Directory including Azure cloud installations No schema extension required API also available for custom database integration
EdgeConnector Service	The service runs on Windows Server 2000 and later, including virtual, clustered and cloud-hosted environments
EdgeConnector Manager	The secure client application runs on Windows XP and later
Wired controllers & card readers	HID Edge and HID EVO controllers, plus any Wiegand or Clock and Data readers to support chosen card technology, including: HID Prox, HID iCLASS, NXP MIFARE, NXP DESFire EV1 and dual interface PKI smartcards
Wireless locks with integral readers	Aperio wireless locks configured for chosen card technology: HID iCLASS, NXP MIFARE, NXP DESFire EV1

EdgeConnector's benefits

	EdgeConnector's truly integrated solution Real-time unified physical and logical access control	Traditional access control system Separate physical and logical access control systems
Enhanced security and compliance	No delays in adding & removing both physical and logical access permissions	Separate updates or scheduled synchronisations create risk when revoking rights & hamper productivity when granting new permissions
	Supports compliance needs (such as PCI-DSS) to restrict sensitive data access to secure locations	No centralised knowledge of user location and IT resource access, in real-time, fundamentally limits any converged access control capability
	Comprehensive real-time alert generation and audit trail reporting	
	Avoidance of 'passback'* and 'tailgating'†	
Simplified management and administration	No duplication of effort to maintain user information. Able to utilise existing security groups & defined roles consistently	Isolated systems require duplication of user information and maintenance. Pseudo-integrated systems require synchronisations to be managed, adding complexity & increasing points of possible failure
	Compatible with the latest, most secure, card technologies	Typical systems lock a customer into a limited choice, or proprietary range, of card types and security systems
	Freedom from "card lock-in" enables phased migration to more secure card types	
	Leverages Active Directory's multi-server, redundancy and disaster recovery features	Additional databases need extra back-up & management provision
	Unlimited numbers of users and sites worldwide	Increases to numbers of users & sites can require additional software licensing &/or installation of replacement door controllers
Easier installation	Utilise existing MS Active Directory or other LDAP database	Additional database has to be installed, populated and maintained
	Use existing access cards. Compatible with a wide variety of card technologies and readers	Often systems are only compatible with a limited selection of cards or tags
	Leverage standard network data cabling and Power over Ethernet	Proprietary and complex wiring systems may be required
	Covers all sites on the WAN wherever they are located	Complex site-to-site synchronisation systems need to be added for multi-site operation

* 'passback': an authorised person loans their access-card to someone else to gain access
† 'tailgating': someone follows an authorised person through a door without presenting an access-card

EdgeConnector's proven track record

EdgeConnector access control systems manage physical access for many hundreds of thousands of users daily, across North America and Europe. Since its launch in 2008 EdgeConnector has been installed in leading large and medium enterprises; central and regional government departments; universities; police and national health services. In addition, EdgeConnector is used by major companies within the financial sector to meet compliance needs.

EdgeConnector is a product of Dot Origin – a leading technology solutions provider specialising in smartcard products and technologies, two-factor authentication, public-key cryptography and data encryption. Dot Origin has operated for over 16 years and built up an extensive roll of respected customers as well as establishing partnerships with industry leading vendors (such as ACS, Assa Abloy, Gemalto, HID, Identive and NXP)

Some of Dot Origin's customers:

Contact us

Tell us your requirements and let us give you a no obligation solution proposal, or request a full feature evaluation kit to see for yourself just how simple it can be to integrate physical access control into your existing IT access management system.

www.edgeconnector.com

info@edgeconnector.com

Europe & Asia

+44 (0)1428 685 861

Northern and Latin America

Toll Free: (888) 262-9642 Direct: (562) 262-9642

Dot Origin Ltd., Coopers Place, Combe Lane, Godalming, Surrey, GU8 5SZ, United Kingdom