Multi-site access control
made easy

THE ALL-IN-ONE ID CARD

Simplifying the management of building access controls across multiple locations

→ Using contactless RFID cards to allow secure access to buildings has become the norm. Increasingly the same access cards are also being used for additional applications such as follow-me printing, cashless vending and PC log-on.

While ID-cards are far more manageable and secure than traditional keys in disallowing entry when keys are lost, or employment terminated, when it comes to providing staff with access to geographically dispersed offices using the same card, the complexity and cost of the physical access control system required frequently escalates dramatically.

WHY MULTI-SITE PHYSICAL ACCESS CONTROL IS NORMALLY SO DIFFICULT

→ The issues that typically arise when extending building entry management systems to cover multiple sites, or offices, stem from the stand-alone nature of common door access control solutions. These systems rely on localised, off-line, access control decision-making unsuited to scalable, centralised, management.

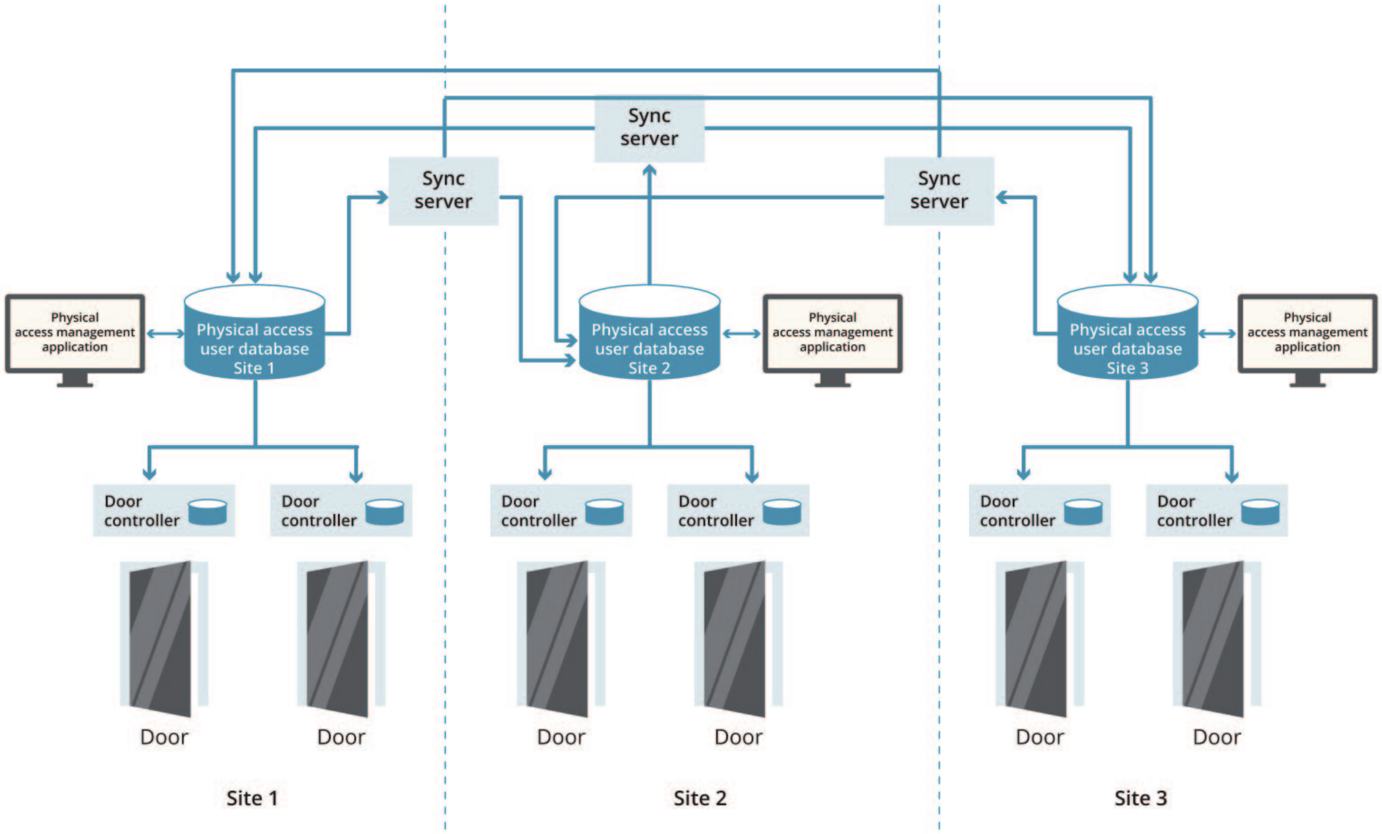
Consider the basic parallel between IT system access controls (logging-in to a PC on a network domain) and building security access controls (using an RFID contactless card to open a door): both systems require the user to provide one or more forms of identification which can be validated against a database of users and their permissions. However, while IT-resource access controls are centralised and designed to scale across all users and sites enterprise-wide in real-time, standard door access control systems rely on dispersed decision-making which requires significant investment to periodically synchronise access-rights between the systems at each site.

→ Adding more sites to a standard physical access control system requires the addition of dedicated synchronisation appliances, sharing data between the stand-alone door access systems at each location on a time-scheduled basis. As well as the cost of these appliances there is a great deal of complexity in managing the sequencing and priority of these synchronisation updates.

→ The proprietary nature of some access control systems means it may not be possible to link the system in newly acquired premises with those used in existing sites. Where different systems can be integrated, it is likely that the data replicated between these systems first needs to be manipulated, for compatibility, before synchronisation. Increases in the number of potential door users at a site may also mean door controllers have to be up-graded to support greater capacity.

The complexity of a typical multi-site physical access control system

Periodic synchronisation of data between sites via dedicated sync-server appliances, and scheduled update of door controllers to support localised decision-making



Sync server
Sync server
Sync server
Physical access management application
Physical access user database Site 1
Physical access user database Site 2
Physical access management application
Physical access user database Site 3
Physical access management application
Door controller
Door controller
Door controller
Door controller
Door controller
Door controller
Door
Door
Door
Door
Door
Door
Site 1
Site 2
Site 3

RISKS FROM UNCONNECTED PHYSICAL AND IT ACCESS CONTROLS

→ Separate access control systems for the physical (door) and logical (IT) worlds can lead to security risks when updates to access permission are not made in both systems at the same time.

A study of desk-based workers in the UK and US revealed that 36% were aware of having continued access to a former employer's systems or data[1].

More advanced systems try to address the gap between physical and logical access control systems through a form of pseudo-integration, where separate databases for the two systems are automatically, but only periodically, synchronised

While this avoids risks from failures of business process to ensure that users' permissions are kept up-to-date in both systems, it adds still further complexity in the synchronisation of the logical access directory with one or more physical access control databases and the management of all the databases holding this duplicated data.

[1] "One in Three Ex-employees Can Access Corporate Networks" - infosecurity-magazine.com July, 2014

Scalable physical access control

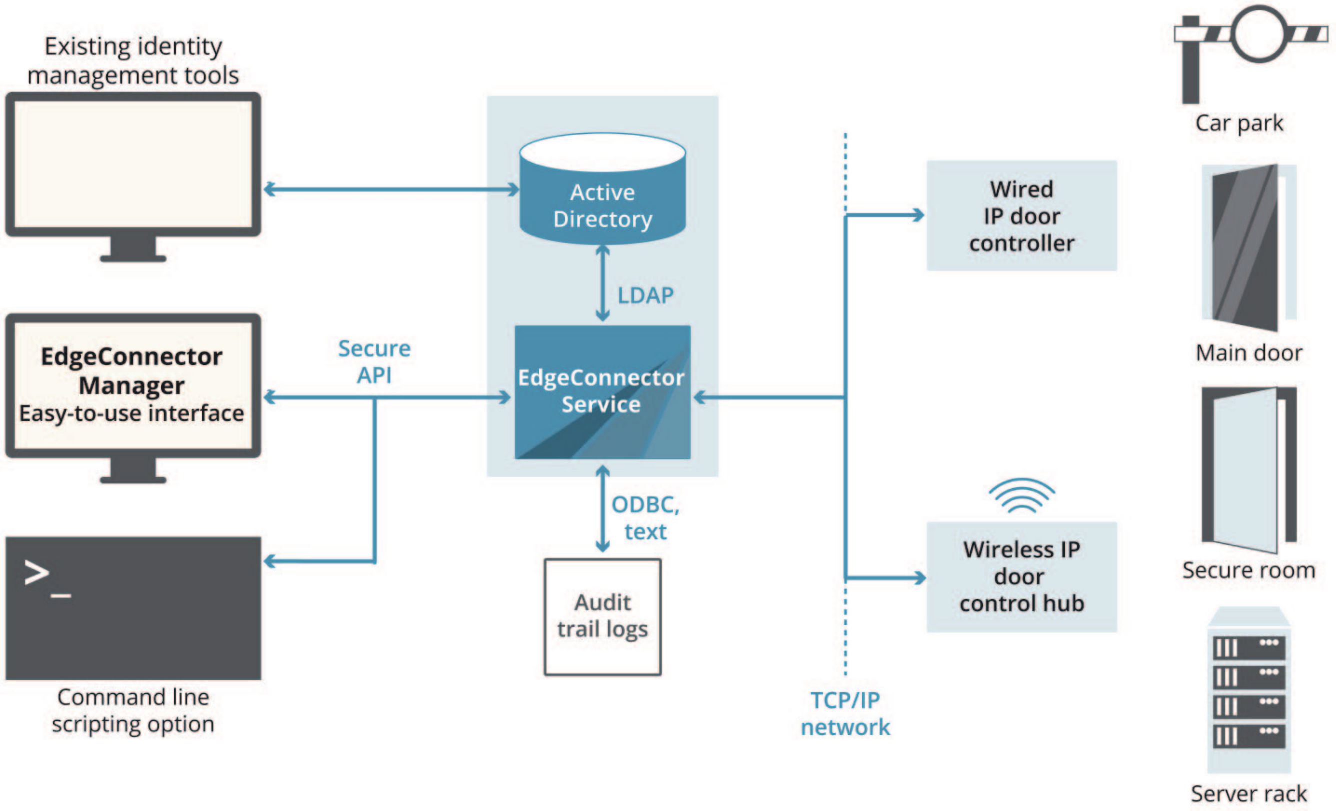
The solution

A STREAMLINED AND SCALABLE SOLUTION

→ The far simpler solution to managing a scalable physical access control system is to leverage the power and flexibility of IT system access controls, which have been developed by leading global technology companies in accordance with established security best practices, and already extend to all users in an organisation across any number of sites. In addition there are significant security benefits to adopting a converged approach to managing physical and logical access, including support for compliance with many data protection standards and regulations (see appendix I).

EdgeConnector provides the streamlined solution - converged physical and logical access control using Active Directory as a common database. From Active Directory, or a linked identity management application, role-based rights can be extended to include door and server cabinet access. Additionally, logical access rights for users can be adjusted in real-time based on knowledge of their location from door interactions, so for example, credit card payment processing applications can be made inaccessible unless users are within secure areas compliant with PCI DSS requirements.

Because EdgeConnector utilizes the existing LAN/WAN and Active Directory to manage user permissions for physical access, any door, no matter where it is located, can be controlled through the IP network in just that same way as logical access is controlled for a user logging-in at any workstation on the network. Similarly, the network resilience, Active Directory replication and back-up protection provisions already in-place automatically support the physical access control infrastructure, too.



Multiple sites within a single domain, cloud based or hosted in-house

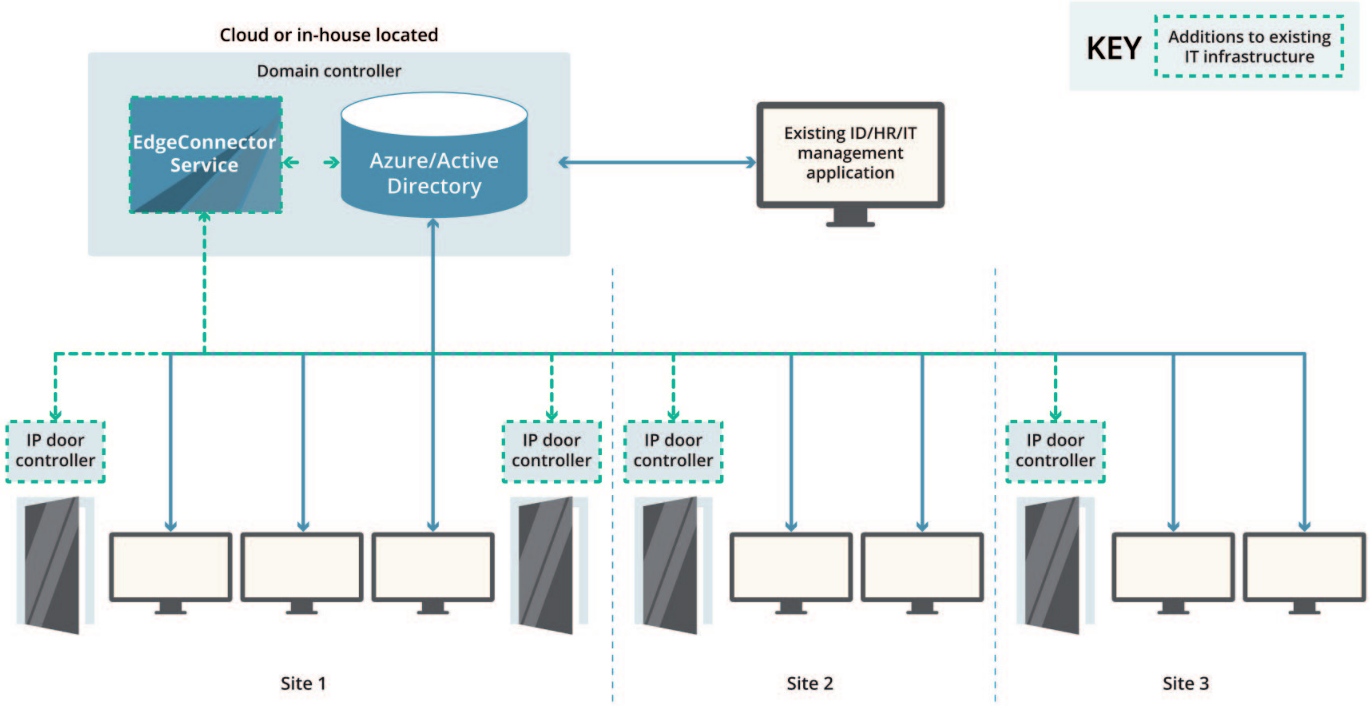
EXAMPLE APPLICATION - REGIONAL OFFICES & RETAIL CHAINS

→ Organisations that provide services locally through a number of sites, dispersed regionally, nationally or globally, can have all their access controlled doors connected to their WAN. The local IP-based door controllers receive a user's card credentials from the card-reader at the door, and over the WAN ask the EdgeConnector service to validate the access request for those credentials.

The EdgeConnector service typically runs alongside the central Active Directory database, which may be in-house or cloud hosted, and handles all access control requests from all the door controllers on the entire network. If the user's permissions allow, the IP door controller will be instructed to release the door to allow them access.

This solution model provides access to many thousands of users internationally.

Addition of physical access controls to existing IT access management using EdgeConnector - in a single-domain environment



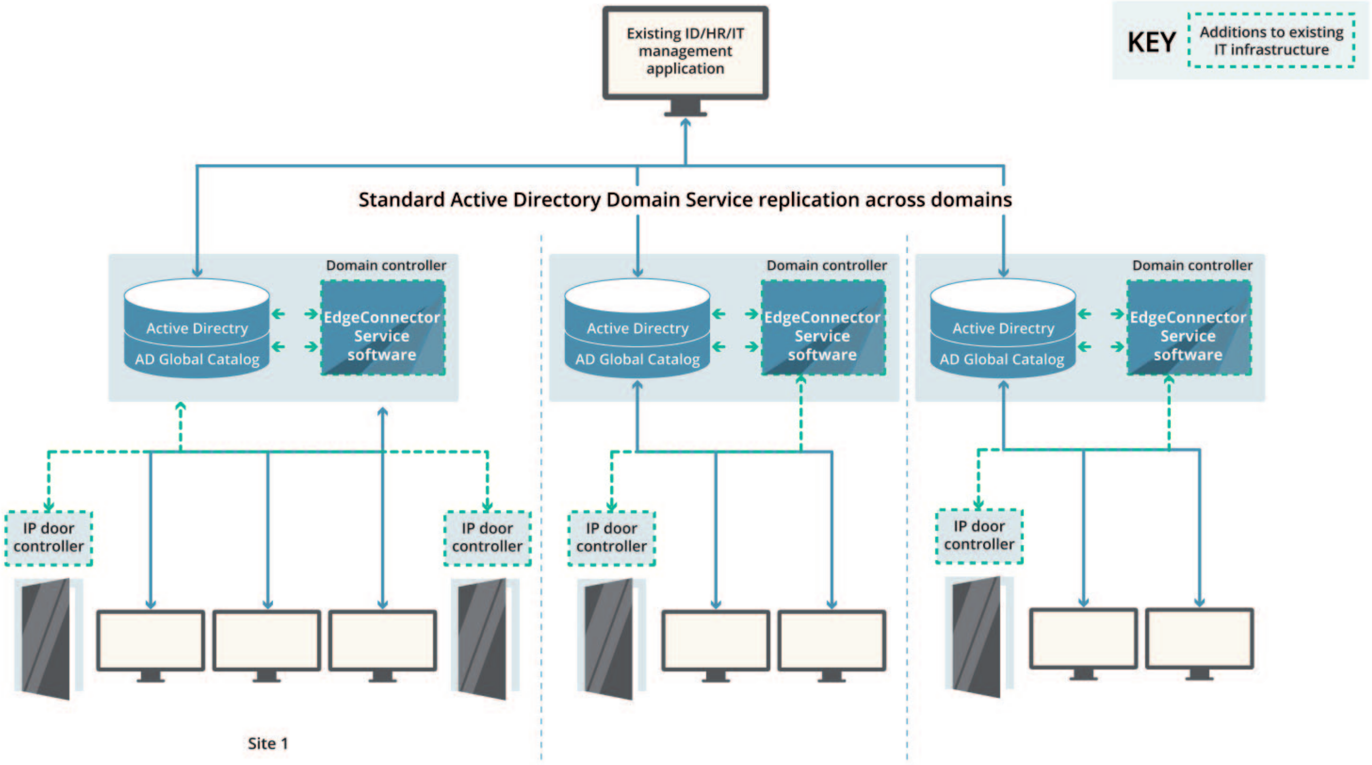
Additional sites from business acquisition - domain forest

EXAMPLE APPLICATION - INTERNATIONAL FINANCIAL SERVICES

→ Often business expansion through acquisition leads to the evolution of an IT network consisting of multiple domains within a 'domain forest'. Active Directory manages users across these domains through its ability to automatically create a read-only Global Catalog of users. The Global Catalog is replicated to all the domains within an established trust relationship, allowing a user from any domain to have their credentials validated when requesting access from within any other domain. This also makes it possible for a user turning up at any site to have their RFID access card, or other security credentials, verified to allow entry where permitted by their role-based security profile.

EdgeConnector can be deployed as local instances that are aligned with the domain controllers at each site. Each instance of EdgeConnector is easily configured to make use of the local copy of the Global Catalog when validating access requests, while recording individual user actions on the user's 'home' domain instance of Active Directory for compliance and audit trail reporting.

Addition of physical access controls to existing IT access management using EdgeConnector - in a multi-domain environment


Existing ID/HR/IT management application
KEY
Additions to existing IT infrastructure
Standard Active Directory Domain Service replication across domains
Domain controller
Active Directory
AD Global Catalog
EdgeConnector Service software
Domain controller
Active Directory
AD Global Catalog
EdgeConnector Service software
Domain controller
Active Directory
AD Global Catalog
EdgeConnector Service software
IP door controller
IP door controller
IP door controller
IP door controller
Site 1

True integration of physical access control into existing IT access management

ABOUT EDGECONNECTOR

Organisations use EdgeConnector to manage the physical access of staff and visitors to their locations around the world every day. EdgeConnector delivers an inherently scalable physical access control solution through convergence with existing IT access management infrastructure.

Unlike other systems, the open, standards based approach of the EdgeConnector solution, with its ability to handle multiple RFID card technologies concurrently, means it may be possible to re-use existing credential reading hardware at the doors of newly acquired sites.

When you've seen EdgeConnector – you'll wonder why all physical access management systems aren't designed the same way. To find out more about EdgeConnector's converged physical and logical access control solution, including wirelessly controlled locks for easy installation, visit www.edgeconnector.com.

Enhanced security

Simple management

Easy installation

EDGECONNECTOR

Europe & Asia

+44 (0)1428 685 861

Northern & Latin America

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

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

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

Appendix I.

REGULATIONS REQUIRING PHYSICAL ACCESS CONTROL

→ **GDPR - General Data Protection Regulation**

Effective from 25 May 2018, replacing European Data Protection Directive 95/46/EC. This regulation requires prompt compulsory notification of breaches and imposes large financial penalties for non-compliance on organisations within the EU. Organisations outside the EU handling EU citizens' data will need to prove "adequacy" - in other words operate to standards equivalent to the GDPR from 2018.

Personal data is to be protected against accidental or malicious actions that could lead to unauthorised disclosure, dissemination or access; with the expectation that solutions implemented provide data protection by default.

→ **PCI-DSS - Payment Card Industry Data Security Standard**

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted.

→ **FISMA – US Federal Information Security Management Act**

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

→ **Sarbanes-Oxley – Applicable to U.S. public enterprises**

Physical access to IT infrastructure systems supporting financial reporting should be restricted to authorized personnel only, and that access should be monitored and reviewed on a periodic basis.

→ **HIPAA - Health Insurance Portability and Accountability Act passed by US Congress**

Physical measures, policies and procedures must protect a covered entities electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Appendix I.

STANDARDS REQUIRING PHYSICAL ACCESS

→ **ISO 27001 -** International standard for information security management system (ISMS) best practice, and ISO/IEC 27002 code of guidelines

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. ICT equipment, plus supporting utilities (such as power and air conditioning) should be secured.

→ **SSAE 16 and ISAE 3402 -** Professional standards for Service Organization Controls (SOC) for financial information:

Logical and physical access controls – processes must manage how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access.

→ **ANSI/TIA-942 -** Data centre infrastructure standard covers many design aspects including physical security

Best practice data centres employ a layered approach to physical access control; starting at the perimeter, segregating access rights between higher and lower security areas within the site and providing time-limited access rights to individual server racks where appropriate. Recommended implementations of these layers incorporate anti-tailgating and anti-passback measures, multi-factor identity authentication and video surveillance. Access controls for data centres need to allow for the inevitable visits of technicians to maintain equipment, their access needs to be limited to only the appropriate areas and server racks.