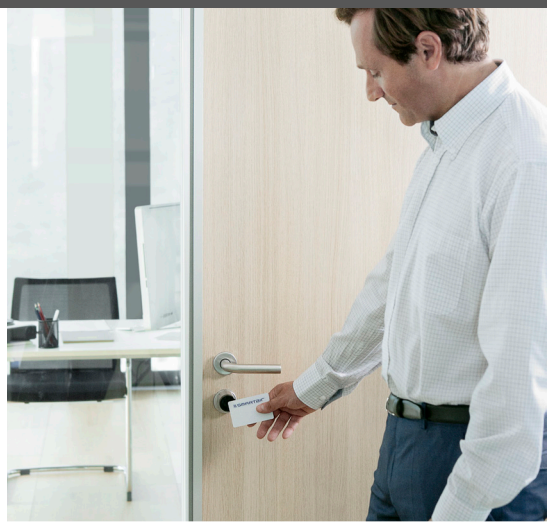
IFSEC GLOBAL

Sponsored by

ASSA ABLOY
Opening Solutions

The Wireless Access Control Report 2021

The move towards convenience with mobile access and integrated systems



IFSEC GLOBAL

Sponsored by
ASSA ABLOY
Opening Solutions

Contents

IFSEC GLOBAL

Sponsored by
ASSA ABLOY
Opening Solutions

Introduction

Report written by
James Moore
Editor of IFSEC Global

Wireless devices continue to evolve. In the context of a global market expected to reach $141 billion by 2025, we are ever more accustomed to using technology that no longer requires the physical presence of wires to provide a stable and trusted connection.[1] It's a market that has come on leaps and bounds in just a short amount of time – a trend that is perhaps best characterised in events such as Apple's decision to remove a headphone jack from its new devices in 2016.

This transformation continues to impact upon the access control market. Growth has been driven by advances in the stability, and most importantly, security, of wireless technology, as traditional access methods have given way to electronic, wireless solutions, that utilise advances in the likes of Bluetooth Low Energy and Wi-Fi 6. In particular, there is a shift towards the use of mobile, or virtual keys, in access control. Businesses and their employees are now growing ever-more accustomed to utilising their smartphone as a payment method, access card for their workplace, and everything in between. Indeed, reports from market analyst specialist, Omdia, show that the "global market for mobile credentials experienced nearly 150% growth between 2017 and 2018".[2] Even if they're not likely to fully replace the use of physical cards in the near future, this is some growth and suggests a hybrid model may be on its way.

Results from this report, compared to previous iterations we have produced, demonstrate a continued move towards wireless systems for businesses of all sizes: 37% now have some form of wireless technology within their physical access control systems, compared to 31% two years ago – a figure that was already a substantial increase from the 2016 report.[3]

And, these trends have continued amongst a turbulent year of upheaval and business disruption. The global COVID-19 pandemic has no doubt caused hundreds of thousands of businesses to place projects and investments on hold, but the demand for contactless building entry systems that wireless solutions work hand-in-hand with has never been higher. It is encouraging to see that the security sector has remained relatively resilient throughout. Our findings suggest that many security managers are intent on upgrades, such as mobile credentials in the near future (page 6), perhaps suggesting that the pandemic has only accelerated a trend that was taking place anyway.

[1] Markets & Markets, Wireless Connectivity Report, October 2020 https://www.marketsandmarkets.com/Market-Reports/wireless-connectivity-market-192605963.html
[2] Omdia, Mobile credentials are finally becoming mainstream but they won't replace their physical counterparts, https://omdia.tech.informa.com/OM004537/Mobile-credentials-are-finally-becoming-mainstream-but-they-wont-replace-their-physical-counterparts
[3] IFSEC Global, The Wireless Access Control Report 2018, https://www.ifsecglobal.com/global/exclusive-download-the-wireless-access-control-report-2018/

The move towards a 'wireless' world has also been a consequence of the growing call for buildings to become more integrated, smart and connected than ever before. Open architecture is a vital component, with the ultimate goal of convenience for all stakeholders.

Throughout this report, we will discuss much of the above, and more, thanks to the results of a survey undertaken in October 2020. With hundreds of respondents, including over 250 end-users, the findings here represent the views of security professionals involved in the procurement, operation, deployment, specification and maintenance of access control systems. We cover key trends in the sector, including the move to mobile access and the growth of open architecture and integration, as well as gathering opinions on the cloud and development of Access Control as a Service (ACaaS).

Finally, we set out to understand the importance of sustainability in the purchasing decisions and requirements of the security sector. As a topic, sustainability is playing an increasingly important role in our everyday purchasing decisions – and rightly so, may we add. Whether it's the UK Government's decision to ban the sales of new petrol and diesel cars from 2030, or an individual basing their weekly shopping decisions on those products that have less of an environmental impact, the issue is affecting our lives in myriad ways. We therefore felt it was important to cover the topic, and explore how wireless access solutions can play their part in achieving the sustainability goals of businesses.

ASSA ABLOY Opening Solutions, a global expert and provider in door opening solutions, has once again sponsored the IFSEC Global Wireless Access Control Report for this year. In doing so, the team provides valuable contributions throughout, supporting the interpretation of results, offering technical insight and challenging any misconceptions – as ASSA ABLOY views them – that may emerge about wireless access technology.

The report also includes comments and data contributed by Omdia's Access Control Intelligence Service. The global research business has a dedicated analysis team covering biometrics, software, physical identity, access management solutions, and more, so we thank the team for its valued contributions and market insight.

A deeper insight into the respondents can be found at the end of the report, where we provide further detail into the types of professionals who offered their opinions. We'd like to thank all those who took part in the survey and found the time in what has been a challenging year for many.

About ASSA ABLOY Opening Solutions

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Their offering includes doors, door and window hardware, locks, access control and service.

About the author

James has been Editor of IFSEC Global since November 2019, commissioning, organising, writing and publishing content to help inform and educate security and fire safety professionals. Prior to this role, James worked in B2B magazine publishing for three years.

James can be reached at james.moore@informa.com

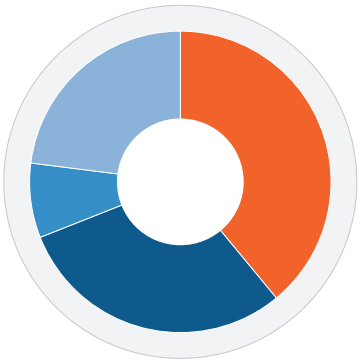
Electronic access control and the move to mobile

One clear conclusion is that the move to electronic access control systems continues to gather momentum. Only 23% of end-users currently do not operate an electronic system. Though there isn't a major difference here compared to the 2018 report, it is important to note that the overwhelming majority of those who aren't operating an electronic access system are from smaller companies: 68% were from businesses with fewer than 50 employees, and another 11% had between 51–250, so it would be reasonable to suggest that such organisations may not require the features a modern electronic access control system can provide – particularly those with only a handful of employees to keep track of.

Following on from this, 38% of end-user organisations are now operating some form of wireless system as part of their access control solution. Again, this is not a vast difference from previous findings, but the technology is certainly well established, with reliability and cost-effectiveness available from vendors continuing to improve. It is now not unusual for an entire building to utilise electronic systems, especially in larger organisations which may hold high value assets that only authorised individuals are given access to.

Those operating fully wireless systems has climbed from 6% to 8% since the 2018 report. This is a marginal increase, though demonstrates growth all the same. And, with so many offices and organisations facing logistical challenges this year due to the pandemic – in April 2020 it was estimated nearly 50% of the UK's workforce was working from home – and projects placed on hold due to financial constraints, perhaps this number would have been higher had the pandemic not hit? [4]

There are certainly clear intentions to replace and upgrade existing systems – in particular to mobile. For instance, when asking end-users if they intended to replace traditional credentials (cards, keys, tags, etc.), with mobile credentials or virtual keys stored on a smartphone, 39% answered they were likely to implement this within two years. Another 26% said they already offered mobile credentials – a significant increase on estimates cited in the 2018 report, where Gartner predicted "less than 5% of organisations enabled the use of smartphones for access to offices or other premises".[5]



Does your organisation already operate an electronic access control system?

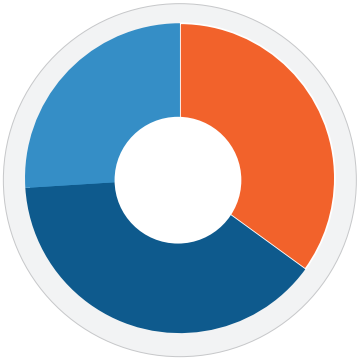
- **39%** Yes, a traditional wired system
- **30%** Yes, a combined wired and wireless access system
- **8%** Yes, a fully wireless access control system
- **23%** No

[4] Office for National Statistics (ONS), Coronavirus and homeworking in the UK: April 2020, https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020

[5] IFSEC Global, The Wireless Access Control Report 2018, https://www.ifsecglobal.com/global/exclusive-download-the-wireless-access-control-report-2018/

As already discussed, this growth is in line with other industry reports from the likes of Omdia. Annual downloads of mobile credentials grew by more than 220% from 2018 to 2019, increasing from 4 million to 9.3 million downloads, as the capabilities of smartphones combines with ever-increasing user comfort levels to enable greater reliance on the devices.[6] In addition, major access control vendors have released improved and compelling line-ups of mobile access solutions, encouraging take-up from end-users.

Sectors that are most likely to engage with mobile credentials are predicted to be hotels, offices, and education facilities, where access needs to be flexibly updated and managed quickly. However, 35% answered 'mobile credentials will not be the right solution for my organisation', with 44% of this group hailing from companies of 50 employees or fewer – once more suggesting that small companies might not have the need for an upgraded access control solution.



Do you intend to implement mobile credentials or virtual keys?

- **35%** Mobile credentials aren't right for my organisation
- **39%** We are likely to implement mobile credentials within 2 years
- **26%** We already offer mobile credentials

Why the growth in mobile access credentials?

There are several potential reasons behind the uptake of mobile credentials. Unsurprisingly, convenience is key, with 46% of professionals placing this in their top two answers for the 'main advantages of mobile credentials'. The user benefits are widely accepted, with 60% of respondents agreeing that 'using a mobile phone instead of a separate access card is more convenient'. Employees or visitors would no longer need to carry around separate access cards or tags, for instance, and the idea of carrying your phone with you while on the move has become the 'norm'. Certainly this is the case across much of EMEA. Omdia also highlights tremendous economic growth in China and India, which "has led to an especially dramatic acceleration of the technology's growth rate in Asia Pacific".[7]

Russell Wagstaff, EMEA Platform Director at ASSA ABLOY

"In line with market trends, ASSA ABLOY Opening Solutions has seen a significant uptick in the adoption of mobile access credentials. Our flagship wireless locks accept mobile credentials, including via BLE and NFC, seamlessly via their RFID readers – no hardware changes required. Offices, co-working spaces and universities have been enthusiastic adopters to date."

Nearly half (47%) agree that mobile is more flexible than hard credentials, and 36% believe that mobile credentials make it easier to upgrade employee access rights at any time. Improved convenience is not simply limited to those requiring access, but also for those giving and managing access, such as security and facilities managers. The software – be it proprietary or open access – that is part of a mobile access ecosystem often allows for scalable and flexible access management, with managers able to issue or revoke access to users via a single, centrally managed platform.

Security professionals are therefore relatively aware of the improved convenience mobile access offers, but what about the security benefits? Only 23% of respondents felt they were more secure than alternatives, while 30% believed that they were a potential security risk. This is somewhat surprising when access cards, keys or fobs can be easily lost, misplaced or stolen. Whether it's a hotel, university or workplace environment, it is customary to have a policy of access card replacement – demonstrating

[6] Omdia, Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual

[7] Omdia, Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual

such instances are a regular occurrence. Employees and visitors however, are far more likely to look after their mobile phone, which now houses so much of their personal and valuable data.

Perhaps the move to a mobile solution raises issues of cyber security? In 2016, another access control report from IFSEC Global found 80% of security professionals agreed that using smartphones, tablets or wearable tech to gain access increases an organisation's vulnerability to cyber hacks.[8] There is much concern over cyber security threats, which has only been stimulated by the pandemic – the UK's National Cyber Security Centre removed more than 15,000 coronavirus-related campaigns during 2020 – and those organisations that operate BYOD (Bring Your Own Device) policies may be anxious about providing mobile access to their employees.

Russell Wagstaff, EMEA Platform Director at ASSA ABLOY, offers his thoughts on mobile access security: "Mobile credentials offer layers of extra security. The first of course is the cyber security offered by both device manufacturer and mobile network. These are global companies with multi-billion dollar reputations to protect. Next is the credential itself, which is housed within the device's secure element. Seos® credentials, for example, offer advanced cryptography and privacy protection.

"Next is device security: fingerprint, face ID and other biometrics, plus password security, are part of most people's daily routine. On top, you can mandate this extra authentication factor in your credential app design. Finally, there is behavioural protection: we would all spot our phone missing long before a plastic card. These all add up to a formidable, multi-layer protection advantage for mobile."

Interestingly, security also scored well on the major advantages of mobile credentials. We gave two separate options here: 'Security (unable to clone)' and 'Security (less likely to share with an unauthorised person or colleague)'. Both scored higher on average than the alternative options: 21% of people selected both these options in their top 3 (out of 8). Those security professionals who did were clearly confident that security was a major advantage for mobile access solutions.

Top 5 advantages mobile credentials are perceived to offer	
1	Convenience
2	Security
3	Cost
4	Easy issuing/revoking of credentials
5	Contact-free solution

Yet, returning to the cyber security concerns, it is interesting to note that very few IT/cyber professionals are included in that 21%. One respondent raised their concerns that "smart phones can still be hacked". Information security professionals are likely to be more cautious whenever new software or technology is integrated within a network, though perhaps there are some misconceptions on the cyber security support presented by vendors?

Advantages that respondents were least concerned with included 'contact-free solutions' – perhaps unsurprising when many card-based systems could already be considered 'contact-free' – and 'modern image'. While 49% selected 'modern image' as the advantage they were least concerned with, the 7% that selected it as their first option were almost all made up of installers/integrators and consultants, rather than end-users.

Challenges of the move to mobile

What challenges do security professionals believe may be affecting the move to mobile? Perhaps a few years ago, problems such as battery life and reliability of smartphones may have caused concern. With only 12% of the industry concerned about the access application's power requirement draining battery, this demonstrates how far technology has come in a relatively short space of time.

Other barriers remain, however. Much like any upgrade or implementation of a new solution, logistical concerns dominated the responses. The 'need to replace existing readers' and the 'need to replace existing locks' were cited by 45% and 35% of professionals respectively.

[8] IFSEC Global, 80% of security industry says mobile access control increases vulnerability to cyber attacks, https://www.ifsecglobal.com/access-control/80-say-mobile-access-control-increases-vulnerability-to-cyber-attacks/

For the 23% who don't already operate an electronic access control system, the implementation of a mobile access system would inevitably come with logistical challenges. Yet, this would also be the case with any access solution upgrade. For those who already operate electronic systems, the move to mobile may not require in any wholesale changes to their current lock and reader systems. A software upgrade may suffice.

'Ensuring implementation on the employee's own smartphone' was considered the third biggest challenge. This is perhaps linked to some of the security concerns respondents have, with BYOD policies potentially creating an operational challenge. Policy makers may experience friction or resistance from employees if the latter feel there is potential encroachment on their personal devices, for instance.

It is interesting to note that only 22% of respondents cited cost as a potential barrier. Expense is traditionally the most common barrier to entry for new solutions – in IFSEC Global's Physical Access Control 2020 Report, 86% of end-users cited 'cost' being among the top three obstacles to upgrading their access solutions.[9]

This response falls in line with the responses to our earlier question over the statements regarding mobile credentials/virtual keys, where 33% agreed that 'mobile credentials are more cost-efficient than hard credentials'. And, with reference to wireless solutions in general, 45% of professionals believe that wireless locks are either less expensive, or similarly priced when factoring in the lifetime TCO (Total Cost of Ownership) as their wired counterparts.

One respondent added to this argument, highlighting there was also "no cost for issuing and printing of credentials". Again, this speaks to the lifetime TCO, with no expense necessary on printer purchasing or maintenance, ink and card supplies.

According to Omdia, wireless locks are, on average around 15% more expensive on initial purchase, though prices are falling at an accelerating rate.[10] It would also appear security and facilities professionals are becoming aware of the TCO benefits that wireless locks provide. For instance, installation prices are often lower with no cabling and invasive building work to factor in to the job, energy savings can be made where solutions essentially 'go to sleep' when not in use, and scalability is considered to be a much easier process. Typical savings on an office relocation or expansion can reach around 30%, according to some reports.[11]

Top 3 challenges when moving to mobile access	
1	The need to replace existing readers/locks
2	Ensuring implementation on employee phones
3	They will be expensive

Russel Wagstaff, Platform Director ASSA ABLOY, adds: "We recently undertook a cost benchmarking study, based on internal research. It identifies major savings from choosing wireless versus wired locking.[12] At installation stage, we estimate cost savings from going for wireless rather than wired door security could be around 80%, based on person-hours and travel costs required at a typical 100-door installation. During operation, energy use savings should be around 70%: battery power is much cheaper than mains electricity, and wired locks use a surprising amount of energy – often a hidden cost, because it's probably not charged to the security cost centre in a large organisation."

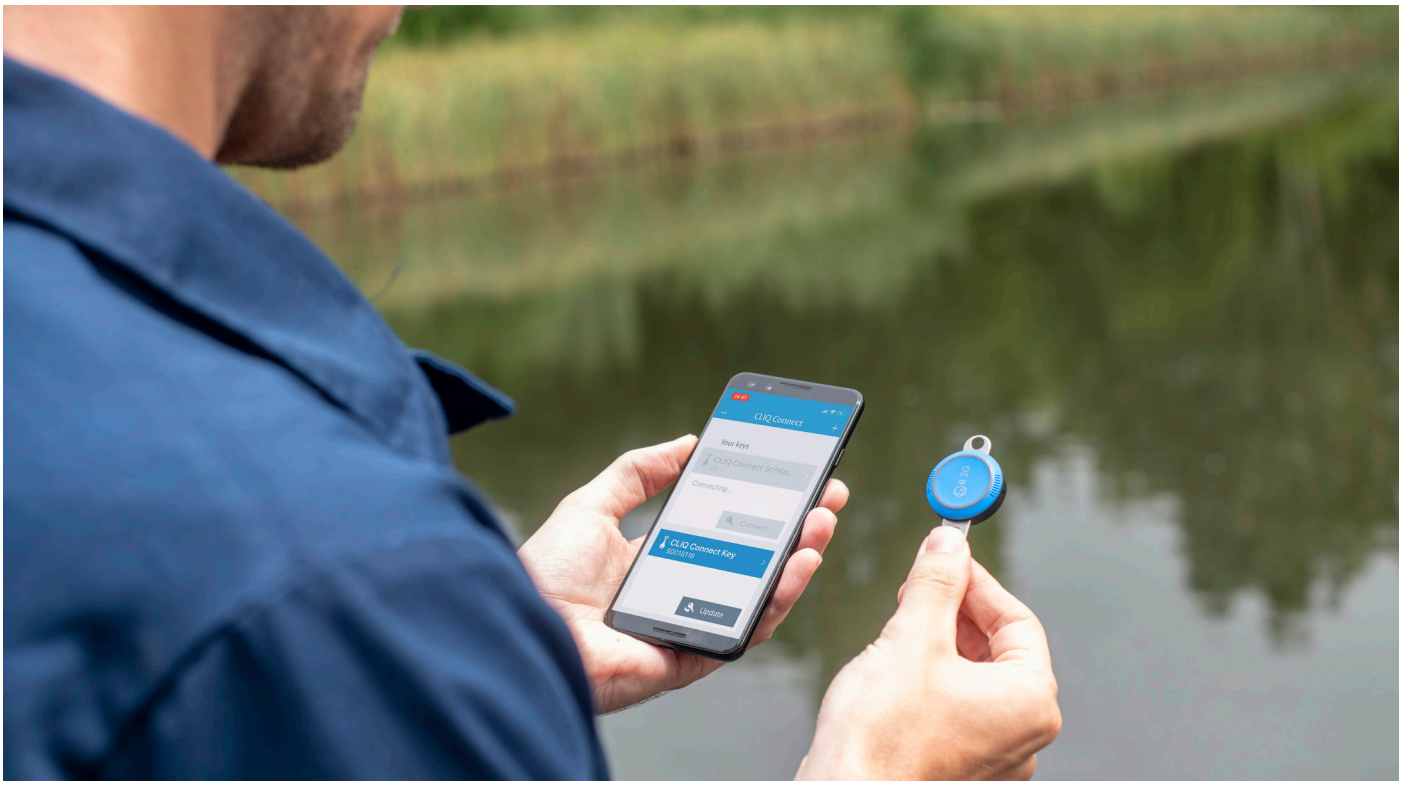
[9] IFSEC Global, The State of Physical Access Control in EMEA Businesses – 2020 Report, https://www.ifsecglobal.com/resources/state-of-physical-access-control-2020-report/
[10] Omdia Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual
[11] IFSEC Global, The benefits of wireless electronic locks, https://www.ifsecglobal.com/security/the-benefits-of-electronic-locks/
[12] You can download the calculations at https://campaigns.assaabloyopeningsolutions.eu/aperio-cost-savings

"Overall, TCO savings for a typical business over the lifetime of an access system could run into many thousands of euros."

The uptake of wireless access control, and in particular a 'move to mobile' is clear from these responses. The growing appreciation of the convenience and cost benefits such solutions can bring, combined with much greater accessibility as vendor offerings grow and prices drop, are two factors driving this trend.

A wholesale move has not yet happened, however. And it was interesting to note that specific environments had challenges that mobile may not be able to overcome so easily – for example, an end-user in the healthcare sector highlighted that "not all staff carry phones – especially in clinical environments – so ID badges remain crucial for us".

While many expect to welcome mobile credentials to their businesses in the next couple of years, Bryan Montany, Research Analyst at Omdia's Access Control Intelligence Service, believes they will not completely substitute physical credentials. He explains: "Mobile credentials are not expected to replace physical credentials in most access control systems. Instead, mobile credentials will increasingly supplement physical credentials in hybrid access control architectures where both mobile and physical credentials can be relied upon." A few survey respondents backed this argument up, noting that card access was still useful to them as a back-up solution in case a mobile phone breaks or the battery is drained, for instance.



The growth of open architecture and integration

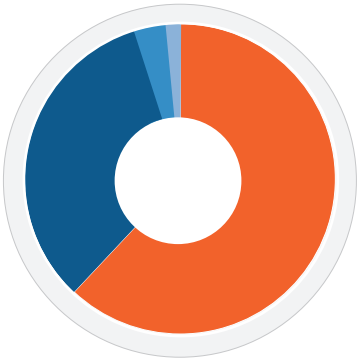
"Systems integration is a recurring theme in marketing materials for physical security products and in conversations among security professionals." This quote from our 2018 Wireless Access Control Report is worth repeating, as the continued evolution of 'smart' systems and open architecture plays a role in building infrastructure. Integration is a useful and, in many ways, inevitable by-product of this.

Clearly it continues to be of utmost importance to the industry: 92% of security and building management professionals consider open architecture, designed for interoperability with similar technologies and products, to be either 'somewhat' or 'very' important – the latter being representative of 62% of the respondents. In addition, when referring to access control specifically, 95% cited system integration with other building/security management functions to be 'somewhat' or 'very' important.

Integration of access control with other security functions creates a more streamlined operations workflow. As Bryan Montany from Omdia explains: "The introduction of security integration platforms has led to further unification of security systems under a single comprehensive software application. The most significant advantage of connecting security domains through such a platform is the capability to manage each associated system through one centralised software hub with one user interface.

"Traditionally, security personnel had to monitor different access control, video surveillance, and intrusion alarm programs, but a security integration platform can aggregate and present data across all these domains, streamlining daily security operations. The use of integrated platforms benefits security managers because it is easier and less time-consuming to train new security personnel to become familiar with a single application. From a cyber security perspective, the integrations of disparate equipment types into a third-party platform can increase vulnerabilities, but it is less intrusive to update firmware for only one unified software application."

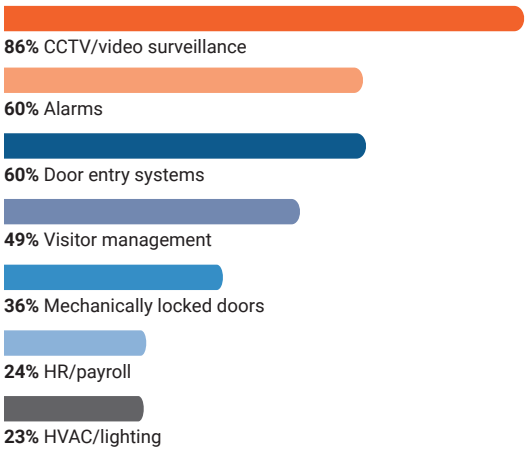
The benefits to such an approach are becoming clear to end-users, it would seem. When asked which third-party technologies they would prefer to be administered from a single environment alongside access control, security-related devices were deemed to be the most important. 86% selected CCTV/video surveillance, 60% alarms, 60% door entry systems and 49% visitor management. While this is unsurprising, given the audience of the survey, this demonstrates the value end-users place on integrating security systems going forward. The appetite for video surveillance and access integration in particular, is prominent, and Omdia analysis suggests that over 80% of all integrated access control systems are at least partially integrated with video surveillance systems.[13]



How important is open architecture when choosing a security system?

- **62%** Very important
- **30%** Somewhat important
- **6%** Fairly unimportant
- **2%** Not at all important

Which third-party functions would you prefer to control from a single integrated environment alongside access control?



[13] Omdia Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual

Russell Wagstaff, EMEA Platform Director at ASSA ABLOY

"Platforms developed to open standards can improve the power and security of an access solution. If integrators can upgrade technologies and systems quickly, it minimises any risk of software being out of date. An API makes customisation straightforward: installers no longer wrestle with incompatible systems, because seamless, secure integration is built in from day one."

"We specifically designed our Incedo platform to be an integration-led solution. Online and offline control, wired and wireless locks, all operate within a single electronic access control system. From the site user's perspective, one secure Seos credential operates every locking point."

Other proponents go a step further, arguing that cyber security processes should also be merged with the security operations system.[14] The 'converged' security approach brings in cyber security and physical security feeds and monitoring solutions, identifying everything from a traditional break-in attempt, through to network disruption due to hacking attempts.

So, if the benefits are so obvious, what is holding the industry back from implementing changes? After all, we found that only 6% of professionals don't feel held back in integrating further.

As is so often the case with upgrades or new solutions, cost was cited by the majority (59%). If no value was anticipated in a move to integration, you'd expect to see this followed by 'selling the ROI' – not the case here, with only 21% specifying this as an obstacle. One respondent added that their organisation had "separate budgets for security and access control". Perhaps a lack of internal operational cohesion could play a role in some instances?

A quarter (26%) of respondents highlighted a lack of knowledge/expertise – a response selected by those occupying several different job roles. Perhaps more education needs to be carried out across the supply chain on the solutions available in the market and how they can be best implemented?

Which factors are holding you back from integration?	
1	Cost
2	Complexity
3	Lack of agreed standards between technologies

The industry does, however, continue to be unsure about the inherent security of integrated systems – 27% cited it as being a factor in their reluctance to adopt such an approach.

The importance of open architecture

Due diligence when embarking on an integration process is advised. A comprehensive integration approach may be a logistical challenge if businesses are operating with proprietary technology, for instance: 27% of respondents noted that a 'lack of agreed standards between technologies' was a major factor holding them back from integration. Systems integrator specialists are increasingly available and on-hand to offer expert advice, however. Many installers of electronic security systems have viewed a move into this field as an excellent growth opportunity, as the integration market continues to expand.

Open standards are therefore key for the momentum behind the shift towards system integration. The migration from proprietary or closed technology to open architecture has likely come as a response to the demand for flexibility from end-users, consultants and systems integrators. Indeed, 64% of professionals believe that one of the most important advantages in open systems is their flexibility. This was followed by open standards providing more choice when upgrading (39%), and the ability to develop solutions from open APIs (28%).

There is also long-term investment gain to be had. With the flexible options which open systems provide, 30% of respondents agreed that they help to save money in the long

[14] James Willison & Sarb Sembhi for IFSEC Global, The growing significance of Converged Security, https://www.ifsecglobal.com/cyber-security/growing-significance-of-converged-security/

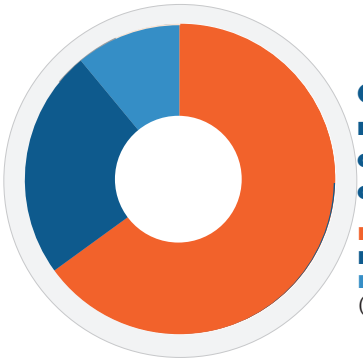
Top 3 challenges integrated security can solve	
1	It removes the need to keep multiple systems up-to-date
2	It will save my employees time
3	It makes compliance easier

run, while 23% cited open standards futureproofing security investments – particularly important for businesses expecting rapid growth in the years to come.

The cloud and Software as a Service in access control

It is no longer just the choice of access control device that security professionals and facilities managers need to consider, but also the model of management their system is based upon. In our 2020 Video Surveillance Report, we found a growing move towards the adoption of cloud-based applications for hosting surveillance storage and video analytics.[15] Is this also the case for access control?

While the majority (65%) are using localised, internal servers to manage their systems, 35% of end-users have now moved to cloud-based software, according to our findings. Back in 2018, Gartner predicted that 20% of organisations will use cloud-based physical access control systems by 2020.[16] It would appear this move has happened, with even greater uptake than perhaps anticipated.



On which model of management are end-users operating their access control systems?

- **65%** Local internal servers
- **24%** Local, cloud-based management
- **11%** Third-party hosting software (ACaaS)

Breaking those numbers down a little more, we found that 24% were using local, cloud-based management, while 11% had moved to third-party hosted software. Often referred to as Software as a Service (SaaS) or more specifically, Access Control as a Service (ACaaS), such a solution involves management of an access control system using a software application operated by an external provider, which may or may not be the system provider. Omdia estimated that global revenues for ACaaS reached over $590 million in 2019.[17]

Options can be divided into hosted and managed access control solutions. A hosted model allows for users to retain full control over administrative procedures, but still using a remote data server, while a managed solution moves the administration and management responsibilities onto the third-party provider. The latter option is often based on a subscription-based payment model, where regular fees will be charged based on the size of the system to be managed. The ACaaS service provider also manages and stores the data in its own data centre, while delivering software updates remotely.

Thomas Akerberg, Business Unit Director EMEA – CLIQ and Pulse, says: "A SaaS solution makes budgeting more predictable for facility and security managers. It removes the need to hire additional in-house IT support and maintenance teams: you know ahead of time how much resource to allocate and can scale infrastructure up or down quickly. When they spend less on server hardware, less on staff and fewer hours ensuring software is up to date, ACaaS subscribers save time and money."

Russell Wagstaff, EMEA Platform Director at ASSA ABLOY, adds: "Survey data shows the way companies manage access control will continue to be a mixed picture, with both locally hosted and off-site cloud solutions. This is why, when we launched our Incedo access ecosystem, we gave users the choice: Incedo Lite as an embedded local solution and Incedo Business cloud management."

[15] IFSEC Global, The Video Surveillance Report 2020, https://www.ifsecglobal.com/resources/the-video-surveillance-report-2020/
[16] Gartner, Technology Insight for Physical Access Control Systems, https://www.gartner.com/en/documents/3451120
[17] Omdia Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual

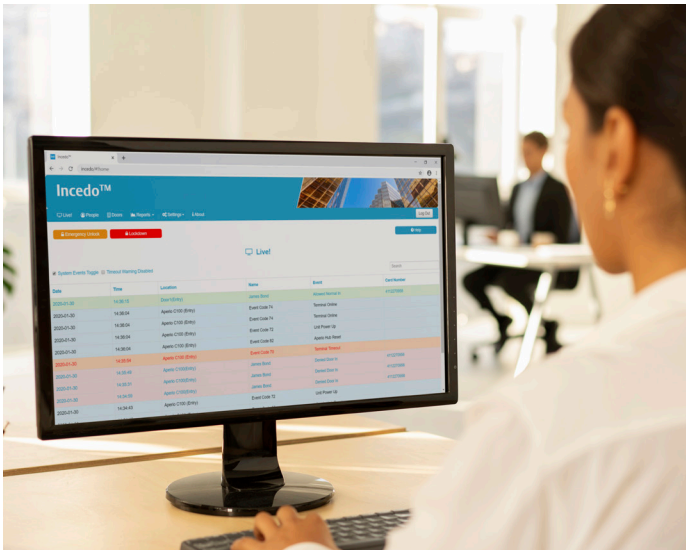
Most important features when choosing ACaaS	
1	Offers real-time access control functionality
2	Offered by a system/service provider I trust
3	Automated software updates and patches
4	Provider offers 24/7 customer support
5	Includes a subscription model that suits me

What are the expectations of ACaaS?

Proponents of ACaaS highlight several potential user benefits from adopting this management model. For instance, users no longer have to administer and host their data in local servers, which can be costly to run, maintain and protect, as well as taking up valuable space. Regular software updates are patched through by the provider, which can be carried out remotely and ensure systems are up to date and well protected. 34% of respondents selected 'automated software updates and patches' in their top three most important features of ACaaS.

Many continue to show reluctance in allowing a third-party provider to manage and administer their data. Indeed, cyber security (27%) and privacy and data protection (24%) were by far the most commonly-cited concerns from respondents when asked about their reservations over managing security in the cloud. Advocates, on the other hand, highlight the cyber security benefits. The regular software updates form a key part of this, but many also point to the fact cloud-based server companies will likely understand cyber security better than most, with dedicated teams to ensure the data they have on file is as secure as possible. Passwords, for instance, can be updated as often as every 30 minutes – a procedure that is not possible to do in-house for the vast majority of organisations.

But what did our respondents say? When asked what business goals they, or their customers, would aim to achieve from a cloud-based solution, 55% identified the ability to 'manage my security from any location at any time'. Once again, convenience for end-users is key. The ability to 'effectively manage IT infrastructure costs' also scored highly (50%), relating to the fact that many third-party solutions push customers towards a recurring subscription-based payment model – highlighted again with 38% of professionals observing ACaaS would allow for 'easier, more predictable security budgeting'.



Respondents also appeared to be aware of the flexibility ACaaS can potentially bring, with solution providers long exclaiming scalability efficiencies when adding new doors or credentials to the system: 29% cited 'fast scaling when needed', and 37% agreed it would allow them to 'deal with issues quickly'. In addition, 27% cited 'unlimited scalability' in one of the top three features they'd be looking for in a third-party service solution.

It is no surprise that trust plays a key role for security professionals: 37% specified that they would want their chosen ACaaS to be offered by a system/service provider that they trusted, while 29% agreed that the service provider would need to offer 24/7 customer support. With growing concerns over cyber security and data protection, particularly in regions with stricter legislative requirements such as the EU (GDPR), it is unsurprising that organisations want to ensure their access control data is well protected and supported by trusted providers.

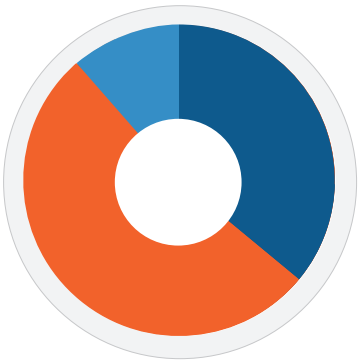
A more sustainable future?

Sustainability is higher on the agenda for governments, organisations and businesses than it has ever been before. In a recent article for *The Telegraph*, Sanda Ojiambo, Executive Director and CEO of the UN Global Compact, noted that: "Reducing carbon emissions and protecting biodiversity makes companies more resilient to shocks, more relevant to society and more valuable to investors." [18]

> ***"Reducing carbon emissions and protecting biodiversity makes companies more resilient to shocks, more relevant to society and more valuable to investors."***
>
> Sanda Ojiambo, Executive Director and CEO of the UN Global Compact

It would appear that the security industry, too, is following this trend. When asked how much respondents' choice of access control technology will be affected by sustainability concerns in the next five years, only 1 in 10 (11%) answered 'not at all'; 36% answered 'to a great extent, with the remaining 53% selecting 'to some degree'.

There are myriad ways organisations can contribute to sustainability goals, from pledging to improve recycling practices, through to commitments to planting trees and cutting waste from manufacturing processes. Energy efficiencies are another way to do so, particularly with the development of smart, integrated buildings, which increasingly incorporate intelligent energy saving processes.



How much will your choice of access control be affected by sustainability concerns?

- **36%** To a great extent
- **53%** To some degree
- **11%** Not at all

Could wireless access control solutions be one method, hitherto underutilised, among more sustainable practice by organisations? Certainly many in the security industry would agree, with just 8% citing that access control wouldn't have a role to play in their organisation's sustainability policy in the future.

But how can this goal be met? The most agreed upon way (54%) access control systems contribute to meeting sustainability goals is the implementation of wireless systems that reduce the need for cabling. Following a similar pattern, 40% selected 'reduced maintenance' and 31% 'minimally invasive installation'. As we've already discussed throughout this report, these are all points plainly associated with wireless electronic locks that don't require cabling or wires, and therefore have fewer components to install and service. In addition, as one respondent noted, a mobile access system doesn't require cards or ink to be used each time a new credential is processed.

We have also discussed the flexibility wireless electronic access control can provide – locks can be upgraded remotely via software patches, for instance, and reused when a company grows or relocates. Almost a third (32%) of security professionals believe upgradability and extended lifetime of access control solutions can promote resource efficiencies.

Those less sure about the economic and sustainability credentials of wireless locks may raise concerns over the life of batteries on which wireless electronic locks are required to run. In some instances, the average battery life for many of these locks can be less than two years, especially in heavily traversed entryways.[19]

According to the survey, 34% of professionals would be keen to see energy-harvesting solutions requiring no batteries in a more sustainable approach to access control. A fairly significant 40% are concerned to a 'great extent' about battery life when making the choice between wired versus battery-operated locks. Though there are

[18] The Telegraph, Why is it smart to invest in the planet, https://www.telegraph.co.uk/business/how-to-be-green/sustainable-development-goals/

[19] Omdia, Access Control Intelligence Service, https://omdia.tech.informa.com/products/access-control-intelligence-service---annual

energy-harvesting options now available in the market, and many wireless systems 'switch off' when not in use, perhaps this represents a development opportunity for vendors and manufacturers to investigate as we move towards a more sustainable future?

Thomas Akerberg, Business Unit Director EMEA – CLIQ and Pulse, adds: "While battery life in most wireless locks is very generous, ASSA ABLOY's new PULSE locking range addresses concerns about both this and energy use. PULSE locks are energy-harvested: their microelectronics are powered by kinetic energy generated from key insertion and turning. They offer secure, programmable key-based electronic access control without cables or batteries."

How may access control products contribute to meeting sustainability goals?	
1	Wireless systems which reduce the need for cabling
2	Energy efficiency during in-use phase
3	Reduced maintenance
4	Products made with recyclable components
5	Self-powered/no batteries

How tough are wireless locks?

A third of survey respondents believe wired locks are tougher than wireless locks. ASSA ABLOY's Russell Wagstaff responds to what he believes, is a misconception:

"It's quite possible to compare 'toughness' or durability across locking ranges, because standards and certifications are established for precisely this reason. For example, an Aperio wireless escutcheon complies with requirements for many types of buildings, including schools, stadiums and public institutions, where products must be certified (DIN 18273; EN 179, 1906). The Aperio L100 Lock meets EN 179 and EN 1125 standards and has a CE mark. It has a certified ingress protection rating of IP55. Locks within many wireless ranges are certified for use on security and/or fire doors. They are subjected to the same durability tests as wired locks. Plus, of course, if mains power is interrupted, battery-powered locking is not affected."

About the survey respondents

With over 400 respondents to the majority of the survey, and 270 end-users answering the end-user focused questions, this report is built on an extensive set of data.

Demographics

Respondents hail from a wide range of geographical regions. UK respondents make up just over half (51%), while most others come from a spread of countries across the EMEA region, as well as India and a smattering from the Americas. For those looking to understand more about the market in the Oceania and Southeast Asia region, Omdia recently released its Access Control Report 2020 for the region, covering trends and data from Australia, New Zealand, Malaysia and Thailand.[20]

Job roles were also varied, with several options to choose from. When discussing end-users in the report, we are referring to those who often work in-house, or have a high level of influence over purchasing decisions at an organisation. These include security, facility or building managers (14% of respondents), security directors (8%), business owners (9%) [21], and in-house IT professionals or CISOs (7%).

There was a wide spread of vertical sectors where end-users worked, including government and public sector, cyber security, industrial/engineering, construction, education, healthcare, retail, banking and finance, logistics, residential, critical infrastructure, and more.

Business of various sizes were represented: 42% came from companies with fewer than 50 employees, 30% from medium-sized enterprises, and 28% from larger corporations of more than 1,000 employees.

There were also high response numbers from the installer/integrator audience (18%), and security consultants (13%), both of whose day-to-day work involves installing or advising on security access control systems. They have high-level insight into current trends. We did not require these respondents to detail the sectors they were involved in, as they often work across several areas, dependent on the project requirements at any given time.

Context

The survey was conducted during October 2020, a time where much of the world was in the midst of a second wave of COVID-19 infections. While there remained some uncertainty at the time, many governments and businesses had a better assessment of what the future may hold for their security operations and requirements moving into 2021 than they had earlier in the year – a time where we were very much in the unknown.

As a result, the answers provided to build this report provide valuable insight into current market trends and attitudes towards wireless access control.

[20] Omdia, Access Control Report – Oceania & Southeast Asia -2020, https://omdia.tech.informa.com/OM012111/Access-Control-Report--Oceania--Southeast-Asia--2020
[21] This figure does not include installer or integrator-based business owners.

Wireless access control solutions from ASSA ABLOY

Incedo™

Released in 2020, Incedo systems have been designed to provide the usability, flexibility and updatability demanded in today's always-on world. Easily expandable and endlessly scalable, it is quick to install, quick to upgrade and quick to provide results. It's also agile enough to adapt to the latest technological changes, intuitively combining secure, connected access points with intelligent identification technologies, for a solution that is both future thinking and future-proofed. Incedo Business has been designed to provide seamless integration with all Incedo-enabled hardware, which we test thoroughly prior to connection, for easier, more reliable third-party integrations.

Aperio®

Aperio devices enable access control providers to cost-effectively integrate non-wired doors with mechanical locks into new or existing access control systems. Doors merely need to be fitted with battery-powered, RFID-equipped Aperio locks, cylinders, escutcheons or handles. Server rack locks (KS100) are also available. All Aperio devices are then linked to the access control system via a communications hub for online integration, or via update on card for offline integration. As a result, security and facility managers have greater control, can easily respond to organisational changes and only need to monitor a single security system; users carry a single RFID access card.

SMARTair®

SMARTair is an access control system that offers an intelligent, yet simple, step up from physical keys. SMARTair wireless locks are more cost-effective to fit and to operate than standard wired access control doors — and can be installed offline or online. Replacing a lost card is much cheaper and faster than replacing a key. SMARTair access control doors are reprogrammed, with no need to replace locks or cylinders. For users, SMARTair offers smart-card and fob credentials, as well as the new Openow mobile app to open doors securely with a mobile phone.

CLIQ®

Award winning CLIQ locking technology is built around high-end, secure microelectronics and programmable keys. It combines mechanical and electronic protection to meet different security and flexible access needs. Power is supplied to the lock by a battery inside every CLIQ key. In this wire-free system, each key may be programmed and updated individually to allow access to specific areas at specific times and dates, accommodating changing access requirements and ensuring continued maximum security. CLIQ incorporates flexible access and key management solutions for all kinds of locking application.

PULSE

ASSA ABLOY PULSE is a digital locking technology incorporated in self-powered cylinders, padlocks and reusable electronic keys. Quick to install and easy to operate, PULSE is an intelligence of electronic access control with no need for batteries, wires or any external power supply. Users carry a single, programmable key to open every door they need. The insertion of their key powers the encrypted electronic security inside every PULSE lock. The PULSE hardware is part of the Incedo solutions and utilises Incedo cloud as the software for easy management and programming.

Learn more by visiting: https://campaigns.assaabloyopeningsolutions.eu/wac

IFSEC GLOBAL

www.ifsecglobal.com

THE NUMBER ONE SOURCE OF ONLINE CONTENT FOR SECURITY AND FIRE SAFETY PROFESSIONALS

IFSEC Global is the leading provider of news, exclusive reports, industry thought leadership, webinars, whitepapers and more.

Join the IFSEC Global Newsletter community and receive weekly industry news and updates to keep you at the forefront of the industry.

informa markets