AVIGILON™

THE ULTIMATE GUIDE TO ACCESS CONTROL SYSTEMS

What access control is and why it's important to security

MOTOROLA SOLUTIONS

THE ULTIMATE GUIDE TO ACCESS CONTROL

Access control systems are an important and integral element of security systems to protect property, people and resources. Door access control systems determine who is authorized to enter a property or a restricted area within a property and provide various techniques to manage and control access.

Access control security is used in many different types of building, including campuses, office blocks, commercial buildings, multi-tenant apartment buildings, industrial complexes, condos, gated communities, schools and colleges, airports, stadiums and government buildings.

This article explains what access control is and why it's important to security. You'll also learn about the benefits and use cases for access control, as well as access control policies and the components of an access control system.

Access control definition

The role of access control security, or the true access control security meaning, is to regulate who can enter a building or a space. Its aim is to minimize risk to a business or organization.

To secure facilities, organizations deploy electronic access control systems that incorporate user credentials, access control readers, auditing and reports to manage and track access to restricted locations. They may also deploy alarms and lockdown capabilities to prevent unauthorized access or control operations in restricted areas.

Electronic access control has replaced traditional lock and key systems as a more secure and convenient method of controlling access, overcoming the problems of lost or stolen keys, retooling locks and the inability to view access activity.

Another subset of access controls, information security can include ways to limit who has access to computer systems or networks. Also known as cybersecurity access control, these types of methods are used both on the premises and in cloud-based platforms to help ensure data and information remains protected. When combined with physical security methods, it's often referred to as security convergence, a growing trend in the security industry.

Why access control security is important

In short, replacing traditional locks and keys with electronic security and access control strengthens security. Traditional locks have many drawbacks, including management challenges, lack of audit trails and the fact that metal keys are easily lost, stolen and copied.

Electronic credentials are more difficult to steal or copy, and they require validation before an individual can gain access, which gives security teams greater ability to control access. Electronic access control systems can be programmed with different levels of access for individual users and groups, which enables security teams to impose the strongest levels of security where they are needed most.

Flexibility and control are important because, compared to single-family residential properties, commercial buildings must provide convenient, secure access to large numbers of occupants and their visitors, who might include friends or family, business visitors, couriers delivering mail, packages or food, contractors or tradespeople carrying out maintenance work.

A commercial access control system is important at building entrances, where the system provides convenient access for employees, residents or other occupants, while preventing intruders or unauthorized individuals from entering.

Within a building, access security protects areas where entry must be restricted by only allowing users with the right credentials to enter. In an office block, this might apply to server rooms or spaces where confidential data is stored. In a multifamily residential complex, the access security system might limit access to resident-only facilities such as gyms or mail rooms.

A door access control system also provides security teams with important information on all entry activities. This can provide useful evidence in the event of an incident or suspicious activity.

How access control security works

A user who is authorized to enter a building or secure area presents credentials to an access control reader positioned at the entrance or door. The reader transmits the credentials' data to software which validates the credentials against a database of authorized users.

If the credentials are valid, the software initiates a door release signal which opens an electronic lock to grant access. If the credentials are invalid, or the user does not have permissions for that door or time, the door will remain locked.

An access control panel is the backbone for the access control system; access control panels or controller boards determine the basic functions of the system, including the entry decisions. The system also records and retains all access requests for analysis, audit or evidence.

In the case of visitors requesting security access, they will either need temporary credentials, such as a visitor badge or digital guest pass. If the occupant or front desk has the ability to operate the access control mechanism, either via a button or app, they can issue a door release signal to grant access.

What is an access control policy?

To impose the right level of security and access at entrances to restricted areas, security professionals or property managers must enforce access control policies. These fall into five main categories:

- **Discretionary access control (DAC):** The owner or administrator of the property sets the access control policy defining who is authorized to access the building or a specific area. This type of access control provides minimal levels of security.
- **Mandatory access control (MAC):** Security professionals grant and manage access rights based on multiple levels of security. Access is granted or denied based on the user's security clearance level. This category is used to protect highly secure areas.
- **Attribute-based access control (ABAC):** This approach provides access to users based on who they are, rather than what they do. Access permissions can be based on the user's type, location, department and duties, mirroring the organizational structure of the business.
- **Role-based access control (RBAC):** Access is based on defined business functions rather than the individual user's identity. The aim is to provide users with access only to areas that are deemed necessary for their roles within the organization.
- **Rule-based access control:** An administrator defines rules that govern access to an area. These rules may be based on conditions, such as time of day and location.

Access control functions

Access security has five main functions:

- **Authorization:** The access control system administrator specifies individual users' access rights to areas or resources. For example, employees are authorized to enter a building, but only authorized to enter restricted areas relevant to their grade or job function.
- **Authentication:** The system or an individual validates an entry request such as the identity of a person or the credentials they present. For example, a resident checks a video image of a visitor before granting access, or the system validates credentials against a database of authorized users.
- **Access:** When the system has authenticated a request, it grants access by opening a locked door.
- **Management:** Security administrators manage the access control database by adding or removing authorized users so that the access control devices only validate requests based on current information.
- **Audit and review:** Regular reviews and audits minimize the risk of users retaining access rights they no longer require. Audits also provide essential records for compliance.

Reporting is also an important function. Each time a user requests access, the system generates data that provides important management information. The system records all access requests with details of location, user identity and type of credential used. Notifications also provide insight into potential security issues, such as tailgating, doors left open or access requests from unidentified users.

The data from door access control helps security professionals monitor the performance of the systems through reports such as:

- Door activity history recording who opened a specific door and at what time
- Invalid access attempts where users attempt to use their credentials at an unauthorized access point
- Door openings, door forced open or door left open too long

Access security configuration

System administrators use the information from the authorization process to configure access levels for users and access locations. They rank locations based on the level of security and authority required to gain access. They can then configure the credentials issued to individual users.

Access control software can also configure user credentials to automatically expire by specific dates, based on the completion of a project, for example, or the date when a resident leaves their tenancy. The software can also configure temporary credentials for a one-time event, for example, where attendees will only require access for emergency maintenance or a vendor visit.

Building owners may wish to restrict general access to a building at certain times, such as evenings or weekends. Software can configure all credentials to be invalid at those times. It's also important to put emergency measures in place so that access control systems can automatically operate in lockdown mode in the event of a fire or other emergency.

Security access locations

Security access control examples are found in many internal and external areas of a building or campus that need to be secured and controlled. Here are a few examples of common areas for access control security to be installed:

- **Main entrance:** This might be a reception area where check-in is automated and employees and visitors must present credentials. There may be multiple entrances to a building, so it is essential that they are all covered by access control techniques.
- **Turnstiles:** These might be located close to the main entrance as a means of access control where there is public lobby access, but restricted access to the rest of the building. They may also be located on other floors or zones that need to be secured.
- **Car lot or parking garage entrance:** Entry may be secured by a gate or other form of barrier that limits access to authorized vehicles and visitors.
- **Elevators:** Access control systems may be used to manage numbers of occupants or to control access to certain floors.
- **Server rooms:** All entrances must be secured, allowing only authorized users.
- **Perimeter:** In a building or campus with a large perimeter, security access can be installed at gates, barriers or other entrance points to manage the flow of visitors and vehicles.

It's also essential to identify other areas that are vulnerable to intrusion, represent a security risk, or where it's important to manage movement:

- **Vulnerable areas:** These include emergency exits, windows or unsecured exterior doors where intruders could gain access without detection.
- **Areas with a security risk:** In commercial buildings these include certain offices, storage areas or meeting rooms where confidential information is held. In multi-occupant residential buildings, these might include storage rooms or resident-only facilities such as gyms or recreation areas.
- **Areas to manage movement:** These include lobbies, stairways and passages where it's essential to avoid overcrowding.

ACCESS CONTROL COMPONENTS

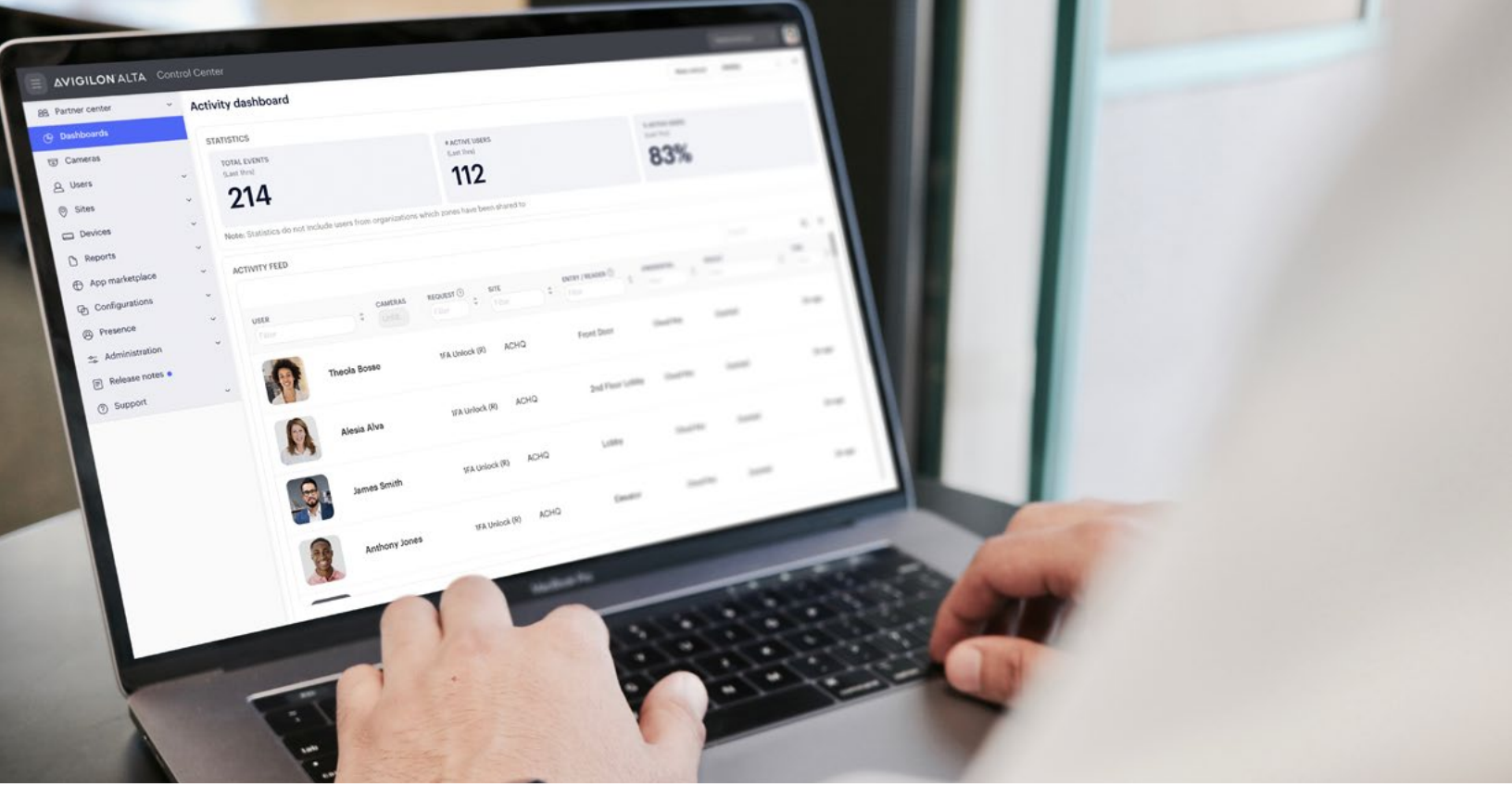
Door access control systems have a number of basic components, each with its own importance for a fully functioning system. It's important to understand how access control components influence the convenience and security of the system in order to deploy a solution that fits your needs.

Door access control credentials

Credentials are what users will present to a door reader when they want to enter the building. There are six main types of credentials that offer different levels of security and convenience:

- **PIN codes:** PIN codes are convenient, but require users to remember their codes. General codes can be used in low-risk areas, with individual codes issued for higher-security entrances.
- **Swipe cards:** These badges feature codes on a magnetic strip. Users swipe the cards through a reader to request access. While they are convenient, they can present a security risk if users swap or lose cards that can be used by intruders.
- **Proximity key cards and key fobs:** Proximity solutions use RFID technology to provide contactless access. Users present RFID-enabled key cards or key fobs when they are close to a reader. This makes them a simple, convenient form of access for high-traffic areas.
- **Smart cards or smart fobs:** These advanced cards and fobs contain a computer chip that can store additional, unique credential information, which increases security while retaining convenience.
- **Mobile solutions:** Users download an app to their smartphone or other mobile device. Depending on the access control system, they scan the smartphone at the reader or use an unlock feature in the app to gain access. Mobile credentials support regular use for authorized users, or temporary access to specific areas for visitors, contractors or service staff.
- **Biometric solutions:** Biometric door locks combine strong security with convenience for authorized users. The most widely used solutions include fingerprint door locks, facial ID and eye scan door locks for retinas or irises. Biometric solutions overcome the problems of lost or stolen credentials because they are extremely difficult to copy.

The systems to capture biometric credentials and the scanners required to read them are expensive, and this initially limited their use to protecting highly secure areas. However, if budgets allow, they can also be used as a fast, convenient method of access in high-traffic areas.



Door readers

Door readers can be installed inside and outside of the building to provide security for areas with different levels of vulnerability. There are different types of security door readers for use with corresponding credentials. They include:

- **Keypad readers:** Users key in a general or unique PIN using the keypad. Although this type of reader is simple and convenient to use, PINs can be shared, guessed or used by intruders with stolen credentials, especially when buttons wear over time. Capacitive touch keypads and longer-digit unique PINs help combat these challenges.
- **Key card swipe readers:** Users swipe their key cards through the reader. Although these readers are secure, they may require frequent maintenance if they are used in areas of heavy traffic.
- **RFID key card or key fob readers:** This type of contactless reader is more suitable for heavy traffic areas. Readers simply present their credentials when they are within range of the reader.
- **Biometric readers:** Users present one of their approved biometric attributes, which are scanned for validation against a biometric database. For even higher levels of security, biometric solutions can be used as part of two-factor authentication with other credentials.
- **Smart door lock readers:** These readers are designed to operate with different types of credentials. They can also be programmed for two-factor authentication using a combination of credentials to increase security levels.
- **Video door readers:** Video door readers have a camera embedded into the access control device, giving security teams visual evidence of identity and any security issues.
- **Intercom readers:** This type of access control device combines reader technology with two-way audio, and is commonly used on front doors to help verify visitors prior to granting entry.

Controllers and access control boards

These are the "brains" of the access control system, acting as a link between the door reader and the user database. These units are usually installed behind restricted doors, as they contain vital data and information that should be protected.

Access control software and data storage

The software for access control systems is a vital tool for managing the database of authorized users. The database holds the details of the network of access controlled doors and authorized users together with their access levels.

To maintain security, it's essential to keep the database up to date by adding new users and removing users who have left or who no longer have permissions to access specific areas.

There are two options for hosting access control software: on-site in servers or hosted in the cloud accessible via the Internet.

Access control devices can produce high volumes of data, particularly if the system incorporates video or biometric credentials which create very large file sizes. If data volumes grow, additional servers may be required for an on-site system. Cloud storage is more scalable; if capacity requirements increase, additional capacity is available on demand for a

higher subscription. In some cases, a hybrid option may be available, which is particularly useful for businesses with multiple locations.

Another key differentiator in these system options is that on-site servers have to be maintained and updated by an internal IT team. All maintenance and updating of cloud-based systems is usually handled by the hosting company as part of the subscription.

Cloud storage for access control devices offers the additional benefit of remote access. Security teams are no longer restricted to reviewing data on-site. If data is stored in the cloud, security teams can also access the data from any location using an Internet-connected fixed or mobile device. This increases flexibility, allowing teams to remotely monitor and operate keyless locking systems outside of normal business hours.

Electronic locks for door access control

Electronic door entry systems remain closed until a user's credentials are validated and a 'release' signal unlocks them. There are two types of electronic door locks for commercial keyless entry:

Electric strike locks are fitted to the inside of a door frame where they replace conventional lock strike plates. A small motor on the strike is connected to a power supply and the current holds the strike plate in the locked position. When an access controller submits a 'release' signal, the motor releases the strike plate allowing an authorized user to open the door.

Magnetic strikes incorporate an electromagnet attached to the door frame, which bonds to a metal plate on the door. The door remains locked while an electric current is flowing through the electromagnet. When a user's credentials are validated, the access controller sends a signal which cuts the power, breaking the magnetic bond and allowing the user to open the door.

Commercial security doors

Electronic locks for access control are generally used in conjunction with commercial security doors, which have the strength and durability to resist threats. These doors can cope with high traffic volumes and continuous use by larger numbers of users with minimal maintenance. They also have the performance to withstand different internal and external environmental conditions, such as extreme weather conditions.

Data networks and cabling

Dedicated cabling has traditionally been used to connect security access components. However, cabling can be expensive to install and maintain, with additional installation costs if the system changes or expands.

Data networks offer a more flexible alternative for IP-based systems. Access control components, such as readers and control units, can be connected to existing networks wirelessly or using Power over Ethernet (PoE), reducing installation costs and offering simpler, faster scalability.

A fast, secure and reliable data network is essential for efficient access control operations. The networks must be able to transmit signals securely between controllers, readers and electronic locks.

Data networks must be capable of transmitting high volumes of data at high speed to minimize the risk of slow response times. To maintain performance, the network should provide high bandwidth availability and functionality such as traffic prioritization to support bandwidth-hungry traffic such as video images or data from biometric devices.

Power supply

An access control system requires power for door readers, controllers and electronic door locks. Power can be connected using conventional cabling to each component or supplied via a data network using PoE technology. This simplifies installation and reduces costs because no separate cabling is required.

As part of your access control best practices, it is recommended that each component also have a backup power supply, so that doors can still be functional in the event of an Internet or power outage.

INTEGRATING DOOR ACCESS CONTROL SYSTEMS WITH OTHER SECURITY SOLUTIONS

Access control systems provide an essential first line of defense against unauthorized access. However, integrating access control devices with other security system components can strengthen protection even further and provide security professionals with a single 360-degree view of activity throughout a building.

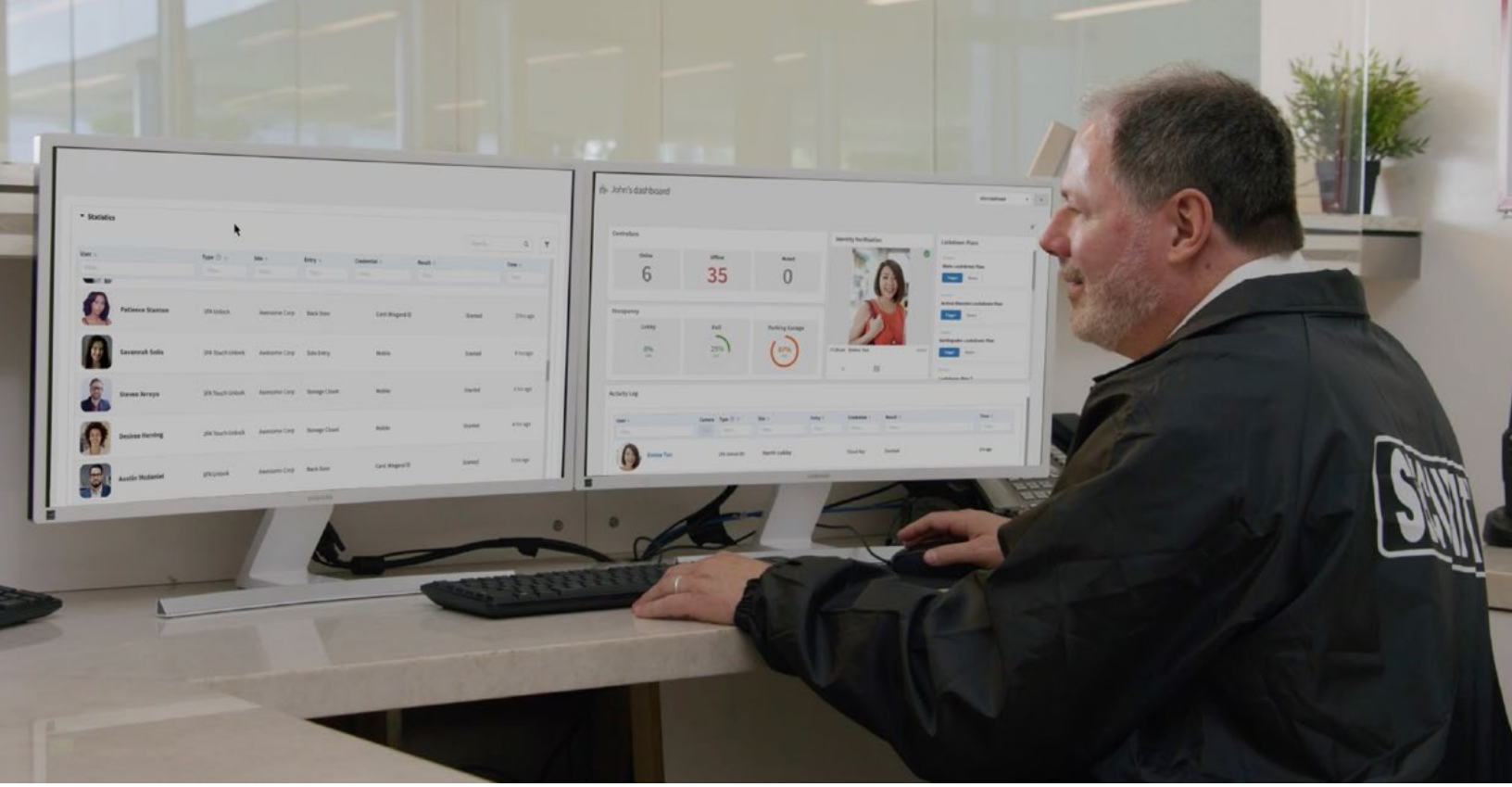
Security video cameras monitor vulnerable areas inside and outside commercial properties to identify and record incidents. By installing video cameras at restricted areas covered by access control systems, security professionals can monitor and analyze the camera feeds so that they can respond rapidly to any incidents.

Integrating security access data with video feeds enables security teams to identify suspects more easily in the event of an incident.

Fitting alarms and sensors to external doors and windows extends security coverage and ensures that security teams receive immediate notifications of any attempt to break into the building. When integrated with the access control system, this allows security teams to quickly identify a door forced or propped open, or remotely unlock a door if needed. Smoke and fire alarms can be integrated with security access to trigger local or building-wide lockdown in the event of an emergency.

Software applications can also be integrated with access control systems for more efficient management. For example, syncing identity platforms with access control ensures credential databases are always up-to-date, and connecting visitor management platforms gives security teams greater control and visibility over guest access within a property.

Video cameras, alarms, sensors, access control devices and electronic locking systems should be built to open standards so that they can be easily integrated into a comprehensive security system that provides the highest level of protection for people and property.



BENEFITS OF ACCESS CONTROL SYSTEMS

Investing in access control techniques can transform the security and convenience of building access and deliver important operational and financial benefits.

Stronger security

Replacing traditional locks and keys with electronic access control mechanisms strengthens security. It eliminates the problem of lost or stolen keys and replaces them with electronic credentials offering different levels of security. Electronic credentials are more difficult to copy and they require validation before a user can gain access, which gives security teams greater ability to control access.

Targeted security

Security professionals can deploy different types of door access control systems or program electronic credentials with different levels of access. This enables security teams to impose the strongest levels of security where they are needed most. For example, smart key cards can be programmed with unique codes to protect highly secure areas, or users can be assigned mobile access permissions based on their titles or work schedules. Mobile or RFID credentials can also be paired with other credentials, such as PIN codes or biometrics, to support two-factor authentication.

Greater convenience for users

Credentials for security access control systems are available in different forms, all offering users convenient access. Proximity solutions, for example, allow users to enter high-traffic areas quickly and easily, while biometric solutions eliminate the need for separate credentials. Mobile credentials can increase convenience even further by allowing users and visitors to identify themselves using a smartphone app. When choosing and developing an access control policy, make sure to provide staff training on how to use the new system.

Simpler user management

Security teams no longer have to issue, manage and replace large numbers of individual keys, which could prove expensive in a building with many different lockable doors and entrances. Adopting mobile credentials simplifies management even further. Teams do not have to issue key cards or key fobs; they simply send a link to smartphone apps programmed with individual access levels.

Modern access control system management software also allows teams to manage credentials online, handling moves, adds, changes and removals with just a few clicks. With cloud-based access control, security teams can manage user credentials from any location on any Internet-connected device.

More flexible property management

A cloud-connected security access system gives teams greater operational flexibility. They no longer have to be onsite outside normal business hours because they can manage access requests, open or lock doors and monitor alerts from any location with a secure Internet connection.

A remote door entry system can provide important security continuity in the event of a fire or other disaster that makes it impossible to provide onsite security management. Teams can continue to monitor and secure doors from a temporary location with Internet connectivity.

Reduced support burden

Electronic access security systems require less maintenance than traditional manual entry systems. IT staff do not have to manage and maintain connectivity and power supply because this is handled by the network team. If the system is cloud-enabled, the IT team doesn't have to manage servers or other infrastructure because this is handled by the cloud hosting provider.

Greater scalability

Networked access control security systems are easier to scale than conventional lock and key systems or access systems connected by dedicated cabling. A new door reader can be added to an existing data network with no need for the delay or disruption of installing dedicated cabling. In addition, adding new locations to the access control security network in the cloud is just as effortless, with all sites managed from a single dashboard.

Consistent security levels

Cloud-enabled security access systems provide an opportunity to centralize security operations and impose consistent security standards, particularly for organizations with multiple sites. A central security team can monitor and manage all access requests from a single location, or remotely via a secure web browser. Centralized management enables security teams to standardize permissions and access levels across all sites, which can strengthen overall security.

Detailed audit trails

Data from access control requests can be useful for analyzing real-time access activity as well as providing input for security audits, management reporting and compliance records. This type of information can also help security teams and property managers assess the efficiency of access control and refine best practices over time.

Streamlined interoperability

Access control devices designed and built to open standards can be integrated with other security components such as sensors, alarms, video security cameras, existing access control systems, fire and smoke alarms to create a comprehensive security solution that enables security professionals to monitor and manage all activity through a single pane of glass. These systems can also be integrated with compatible building management systems and environmental control platforms to improve overall protection and safety in the building.

ACCESS CONTROL AND SMART BUILDINGS

Access control systems play an essential role in protecting a building and its occupants against threats from intruders, but they can also make a wider contribution to building management and the evolution of smart buildings.

While the primary application of access control techniques is to monitor and control access to secured areas, data from the system can also provide greater insight into movement and use of facilities within buildings. That can provide valuable input into facilities planning to create safer and more efficient routing as well as optimizing space utilization. For example, analyzing traffic in spaces such as conference rooms or other busy spaces provides useful information on room availability and occupancy levels.

Access control devices can also be integrated with other elements of building management systems. For example, security access data on room occupancy can support more efficient use of heating, lighting, ventilation and other facilities by automating the allocation of resources in line with actual occupancy. This can improve resource efficiency and reduce overall operating costs.

SELECTING AN ACCESS CONTROL SECURITY SYSTEM

There are many factors to take into consideration when selecting a security access control solution for door access control:

Security

The most important factor is security. The system must ensure that only authorized users and approved visitors can enter a building. Door access security must restrict entry and provide adequate protection for areas of the building that contain sensitive information or resources and facilities that could harm the business if they were damaged by intruders.

Reliability

If a reader or access control unit is not reliable, it reduces the level of security. Downtime for repair or maintenance also increases risk and inconvenience for users. The equipment should have guaranteed levels of uptime and incorporate back-up or failover solutions for high-security areas.

Convenience

Although access control is designed to deter unwanted intruders, it should not prove inconvenient for authorized users who require access. The system and access control devices should be quick and easy to use and incorporate touchless technologies for added convenience.

Management

As well as convenience for users, the access control mechanisms and system should also be convenient to manage. Operation, configuration, management and maintenance should be straightforward with software that's intuitive to use and interoperable with other security tools. Selecting a cloud-enabled system simplifies management even further.

Customization

System components should be customizable so that security professionals can configure them to meet specific requirements for different areas and individual users. Look for solutions that offer multiple permissions levels, door schedules and custom management dashboards to further streamline and control access throughout the property. The system should also be quick and easy to reconfigure if security requirements change.

Scalability

For growing businesses, it's important to have a system that can be easily scaled to cover more access points or support additional users. Organizations operating across multiple sites can improve operational efficiency if a system on one site can be scaled via the cloud to other sites. This will ensure consistent security across the organization and reduce overall costs.

Compliance

The security access control system should enable the business to comply with any customer security requirements, data protection requirements or industry-specific regulations. For example, customers may require data relating to their business to be secured by special measures as part of a contract. In some industries, compliance with an international security standard such as ISO 27001 is essential for doing business, while business in sectors such as healthcare or financial services require even higher levels of security compliance. In general, it's essential to provide security for personal data to comply with data protection regulations.

Cost of ownership

Cost is one of the most important factors in selecting an access control system, not just the initial costs, but the ongoing costs for operating, maintaining and managing access control systems. The upfront cost will be based on the number of access points to be covered as well as the type of components required. The ongoing costs will include installation and configuration, operation, monitoring and management, and the costs of maintenance, repair and upgrading. Costs may be more predictable with a cloud-based solution that includes maintenance and upgrading costs in a monthly subscription.

Access control features

As well as providing the essential security functions, it's important to select systems that include access control features that save time or improve efficiency. For example, automated notifications from the cloud ensure the security team has the latest information on potential incidents. A wide range of reports will enable security teams to provide different stakeholders with the specific information they need for their role. Remote management capability improves convenience and flexibility for the IT team, enabling them to manage systems and respond to incidents from any location.

GETTING THE BEST ACCESS CONTROL SYSTEM FOR YOUR BUILDING

To gain full benefit from security access control, it's important to plan the solution carefully by assessing vulnerabilities and access requirements throughout the building. A professional security system installer can provide advice and guidance on the most appropriate solution for different areas of the building and prepare detailed installation plans. Security specialists can also recommend integration opportunities to ensure the system forms part of a holistic solution for building security and management.

Here are a few questions to ask when determining which access control features and solutions are the best for your business:

How reliable is the access control system?

Security systems are only worth the investment if they work. Reliable door access control systems will have public downtime reports so you can compare. Also consider adding backup and fail-over security for your access controlled doors.

Is the system on-premise or cloud-based?

It's important to weigh the pros and cons of a cloud-based vs. on-premise access control system before investing in new technology. If you have an on-prem solution, some providers now offer remote capabilities and hybrid cloud deployments to make management more flexible.

How easy is it for employees to use the access control devices?

You don't want to make it harder for your staff to get into the building. Unlocking the door should be simple, fast and reliable. Touchless access control methods are a great way to keep traffic moving in your building, without compromising on security.

What does the installation process look like?

Before purchasing, know how long your access control system will take to install and what the installation project will involve. Do you need to run new cabling? Are there existing access control units or readers that you want to keep? Be sure to include installation costs in your access control plan.

What access control features are available with this system?

Be sure the system you invest in has a full feature set, with everything you need to maintain security in your buildings. Look for customizable user permissions, the ability to set door schedules, advanced reporting and audit tools, support for multi-factor authentication and automatic alerts. Other features you may want include lockdown capabilities, custom rule engines, digital guest passes and unification with video security systems.

Does the system integrate with my existing security and access control infrastructure?

Open architecture is an important consideration for access control, as it allows you to connect your access control devices to other security systems. For the best experience managing and maintaining your security, access control systems should be able to seamlessly integrate across your entire technology stack, including video systems, alarms and software tools.

How future-proof is this access control system?

A future-proof system is one that has all the access control features you need now, and will also work for any future security challenges the business might face. Factors like scalability, ease of integration and automatic updates all impact how future-proof a solution is. Consider what the process is for upgrading the software with the latest security, and how the company rolls out new features to determine the longevity of your access control system.

MOTOROLA SOLUTIONS

AVIGILON™

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**