



Security Directors' Guide: Selecting the Ideal Access Control System

acresecurity.com

Security Directors' Guide: Selecting the Ideal Access Control System

Executive Summary

In the rapidly evolving realm of security technology, the need for organizations to deploy sophisticated and reliable access control systems is more crucial than ever. A top-notch access control system bolsters the physical security of a site and seamlessly integrates with other security protocols for a well-rounded security solution. Beyond physical security, ideal systems defend against cyber threats while providing scalability, centralized management, process automation, and user-friendly interfaces. Assessing systems based on these critical factors empowers decision makers to make well-informed choices that align with their security objectives, operational efficiency desires, and compliance needs.

Introduction

Security Directors encounter various factors when selecting an access control system. Beyond ensuring physical safety for personnel, visitors, assets, and property, they must tackle data, evaluating the effectiveness of access control systems that provide flexibility and scalability to address changing security needs. The objective is to implement a system that fulfills data security issues stemming from the ever-changing cybersecurity landscape. This requires a comprehensive strategy to safeguard sensitive operational needs and guarantees continuous monitoring and updates to effectively deal with emerging security risks.



Addressing Cybersecurity Issues Through Enhanced Access Control Systems

As technology evolves, so do the potential threats to your security system. That's why it's crucial for Security Directors to stay updated on the latest advancements in access control technology.

With features such as multi-factor authentication and encryption protocols, cloud-based access control systems provide sophisticated defense mechanisms against cyber attacks.



Data Encryption and Network Security

At the core of cloud-based access control systems is encryption, a powerful tool that transforms readable data into a coded format that can only be accessed with the correct decryption key. This ensures that, even in the event of data interception, the information remains secure and unreadable to unauthorized users.

Additionally, these systems employ robust network security measures, including firewalls, intrusion detection systems, and regular vulnerability assessments, to safeguard against potential cyber attacks. By creating a secure network environment, cloud-based access control systems prevent unauthorized access and ensure that communications between the devices and the cloud server are protected by the highest standards of security.

This combination of data encryption and network security offers a solid foundation upon which organizations can build a secure access control system that is ready to face the evolving cyber threats of the digital age.

Reliability and Redundancy

The reliability and redundancy of cloud-based access control systems are paramount for maintaining uninterrupted security operations. These systems are designed to operate seamlessly, ensuring that access control functionalities remain active even in the event of server downtime or network disruptions.

Redundancy is built into the infrastructure, with data and services replicated across multiple data centers. This design enables an automatic failover process, wherein if one server or component fails, another immediately takes its place without any noticeable impact on system performance or access control operations. Furthermore, the reliability of these systems is enhanced through rigorous testing and regular maintenance schedules, significantly reducing the probability of unexpected failures.

Data and Security Certification

Ensuring the highest standards of cybersecurity involves not only adopting state-of-the-art technologies but also adhering to rigorous data and security certifications. Compliance with international standards, such as ISO 27001, underlines an organization's commitment to managing and protecting data responsibly. This certification serves as a testament to an access control system's robustness and the organization's dedication to maintaining privacy, integrity, and availability of information.

Key Components of an Video Surveillance Access Control Solution

Integrated Security Solutions: Harness the Power of RESTful APIs

In today's dynamic digital landscape, the ability to adapt and integrate new technologies into existing systems is indispensable. Selecting an access control system that is equipped with a robust, developer-friendly Application Programming Interface (API) , empowers organizations to tailor functionalities, integrate third-party applications, and automate security workflows.

RESTful APIs offer several advantages that make them even more appealing for modern systems. They are known for their flexibility and simplicity in connecting and interacting with other web services, making them exceptionally beneficial for organizations looking to enhance their access control systems with additional functionalities or integrations with third-party services. The ease of use and implementation of RESTful APIs enables quicker development cycles and more dynamic adaptation to security needs, providing a clear advantage over more rigid and complex traditional APIs.

To maximize the benefits of an advanced access control solution, such as enhanced security, operational efficiencies, and environmental control, it is essential to ensure seamless integration with the following systems:



Video Surveillance

Integration with video surveillance allows for real-time monitoring and recorded footage associated with access events. This can help in verifying identity, investigating security incidents, and enhancing overall situational awareness.



Visitor Management

Integrating visitor management systems with access control provides streamlined entry and exit processes for guests, contractors, and temporary employees, ensuring access permissions are appropriately granted and revoked in real-time.



Intrusion Detection

By linking access control with intrusion detection, alerts can be automatically generated when unauthorized access attempts correlate with detected security breaches, facilitating swift response to potential threats.



Fire and Life Safety

Integration with fire and life safety systems can ensure that in the event of an emergency, doors automatically unlock, or specific protocols are initiated to facilitate evacuation procedures and ensure the safety of all occupants.



Heating, Ventilation, and Air Conditioning (HVAC)

Connecting access control to HVAC systems can result in energy savings and enhanced comfort by adjusting temperatures based on occupancy detected through access control data.



Lighting Control

Similar to HVAC integration, linking access control with lighting systems can enable automated lighting adjustments that reflect room or building occupancy, promoting energy efficiency and cost savings.

Centralized Management

A centralized security management system offers many benefits, most notably the ability to remotely access and manage various security components from a single interface. This centralized approach simplifies the oversight of complex security infrastructures, allowing administrators to efficiently update policies, manage user permissions, and review security events and logs. Furthermore, it enables quick responses to incidents and anomalies by providing real-time access to all connected systems, regardless of the administrator's physical location.

The integration of cloud technology further enhances these benefits, offering scalable storage solutions and advanced analytics capabilities, which can be leveraged to identify trends and patterns in access data, improving overall security strategy and proactive threat detection.

From managing access permissions and user credentials to generating reports and configuring system settings, a centralized management platform streamlines security operations, saving time and resources while increasing overall effectiveness.

Scalability and Flexibility

Scaling in an access control system refers to the ability to adapt the size and complexity of the system to meet changing security demands. This flexibility allows for the addition of new users, doors, and even sites to the system without compromising performance or security integrity. An effective scalable access control system is designed to grow with an organization, accommodating both small-scale enhancements and large-scale expansions seamlessly. Scalability ensures that an access control system is a long-term investment, capable of adjusting to future growth, technological advancements, and shifting security landscapes.

Auto scaling stands as a pivotal feature in modern access control systems, offering unmatched benefits in terms of operational efficiency and cost management. By dynamically adjusting the capacity of the system to meet real-time usage demands, organizations can ensure optimal performance during peak periods without incurring the high costs associated with maintaining excess capacity during off-peak times.

This not only leads to significant cost savings but also enhances the system's responsiveness and reliability. Furthermore, auto scaling contributes to a sustainable operational model by precisely aligning resource usage with actual needs, thereby minimizing wasted resources and supporting an organization's efforts toward environmental responsibility.



Visitor Management

Visitor management is an integral component of a comprehensive access control system, serving as the first line of defense in securing a facility's premises. Implementing a sophisticated visitor management system ensures detailed screening and tracking of everyone who enters and exits, providing a clear audit trail and enhancing overall security posture. It not only streamlines the process of guest identification and authorization but also integrates seamlessly with other elements of access control to enforce security policies consistently.

By employing advanced technologies such as biometric verification, digital ID scanning, and pre registration capabilities, visitor management systems can effectively mitigate potential security risks posed by unauthorized access.

This layer of oversight is crucial for maintaining controlled access to sensitive areas, ensuring that only verified individuals can gain entry. The incorporation of visitor management within the access control architecture fortifies the security framework, safeguarding against breaches and reinforcing the organization's commitment to a secure operational environment.



A recent survey conducted among 200 enterprises revealed that while visitor management systems were once considered a nice-to-have feature, 66% of respondents now view Visitor Management as critical to an organization's security and operational capabilities.

User Friendly Interface

A user-friendly interface significantly enhances the efficiency and effectiveness of security operations. It ensures that even individuals with minimal technical knowledge can operate the system efficiently, thereby reducing the likelihood of errors and increasing the system's overall reliability. An intuitive interface allows for quick and easy navigation, facilitating rapid response to security incidents and streamlined management of access permissions.

The streamlined user experience not only reduces staff training time, but also proves cost-effective for organizations. Moreover, a user-friendly interface promotes consistent system utilization and monitoring, bolstering a proactive security stance. Emphasizing user-friendliness in access control systems enhances usability across the organization, making security a shared focus rather than solely the duty of IT staff.

Understanding Card Readers: A Comparison of OSDP and Wiegand Technologies

Central to the efficiency of any access control system is the technology interfacing directly with users — the card readers. Wiegand technology has long been the standard for card readers, utilizing a simple one-way data transfer. But lacking encryption and bidirectional communication, Wiegand readers are vulnerable to interception and unauthorized access.

With advancements in security protocols and capabilities, Open Supervised Device Protocol (OSDP) technology has emerged as a superior alternative. This forward-thinking protocol supports bi-directional communication between the reader and controller, enabling not just the transmission of cardholder data but also the reception of commands from the control system, such as firmware updates and reader LED control. It also provides more secure encryption methods to prevent hacking and cloning of cards.

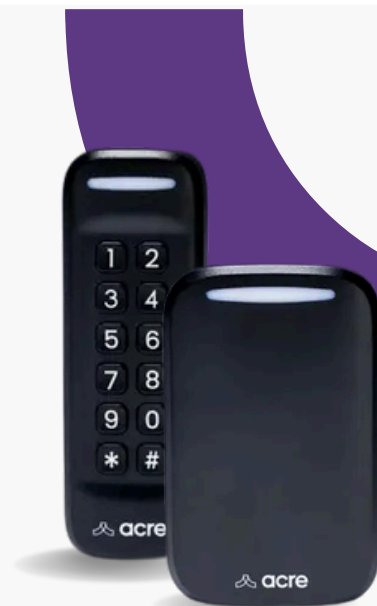
By implementing OSDP readers, organizations take advantage of its interoperability across various manufacturers, ensuring flexibility and a broader range of choices when designing their access control infrastructure. The use of OSDP readers underscores an organization's commitment to leveraging cutting-edge technology to fortify its security measures, demonstrating both innovation and an understanding of the scalability and adaptability demanded by the modern security landscape.

The Acre Commitment to Safeguarding Security

Acre is reshaping security with the convenience of one innovative, flexible, and secure solution. **Widgets and custom dashboards** make your Access Control user experience simple, easy, and customizable to the way you want it. Deployed in the **cloud, on-prem**, or a **combination**, you can engage your best software experience from anywhere with your choice of Windows, macOS, iOS, Android, or any modern browser.

Our **RESTful API** enables users to deploy an extensive range of technologies through a straightforward process for easy integrations between Acre Access Control and a multitude of systems:

- Single card solutions for photo ID badge, access control, time and attendance, payment, and other systems
- Blue light emergency phones to enhance safety
- Wireless locks to secure common spaces
- Mobile credentials for a convenient and modern access control experience
- Biometric readers for high-security areas
- Video cameras throughout the facility
- Visitor management systems
- Intrusion and fire systems
- Active directory connection to streamline HR operations



In conjunction with our open API, users gain unrealized operational efficiency with the unique Acre **FITS** (Functional Integration Toolkit Scripts) **process automation** capabilities. FIT Scripts combine programming, integrations, and workflows to deliver maximum efficiency daily, and reporting for event, system, and process analysis.

Acre Access Control leverages **redundancy and auto scaling** to further enhance the resilience and reliability of our cloud-based Access Control solution. This strategy ensures that the access control system remains operational and available, even in the face of unforeseen failures or spikes in demand.

Our company is proud to be **ISO 27001 certified** for our cloud-based access control and visitor management solutions, demonstrating our dedication to implementing robust Information Security Management Systems (ISMS) that meet the highest standards set by the International Organization for Standardization. This certification underscores our commitment to safeguarding data with utmost security and reliability.

Backed by 45 years as a physical security industry leader, Acre Security is a trusted name in safeguarding assets worldwide, known for our proficiency and our unwavering pledge to security excellence. Our state-of-the-art technology is scalable to worldwide enterprise levels and strikes the perfect balance between advanced security features and user-centric operability.



At Acre Security, our commitment to you is simple: We want to eliminate your risk.

We don't want you guessing if you're secure. We want you to know. And, we have the experience, expertise, and execution to do it, with 21% of our company resources focused on R&D. The technology we choose, driven by the end user experience we desire, impacts the software we develop, and adheres to our go-to-market strategy of being a disruptor. Reshape your security perspective, explore new possibilities for productivity, and find innovative ways to meet your strategic business goals by simply choosing Acre.





acresecurity.com