

Considerations and best practices for migrating to an access control system





Table of contents

Executive summary	3
Reasons to migrate	4
Goals for a migration	7
Overview of considerations	10
Steps in the migration process	13
The Genetec and Mercury advantage	17

Executive summary

Migrating from an existing legacy access control system (ACS) to an Internet Protocol (IP)-based ACS makes it easier for an organization to operate, expand, and customize its physical access control infrastructure.

A successful migration still requires planning and careful consideration. First, it is important to have a clear set of goals. Then, before beginning to plan a migration, an organization must evaluate its existing system to determine the costs and time required to complete the process.

Finally, alongside a systems integrator, it is important that an organization follow the key steps to realize a seamless integration.



Reasons to migrate

Migrating an existing centralized or distributed legacy access control system (ACS) to an IP-based ACS makes it easier for an organization to customize their system as their needs evolve, resulting in enhanced security and a greater return on investment.





An open, flexible IP-based ACS allows organizations to:

- 1 Leverage IP technology to standardize their access control infrastructure and replace proprietary equipment
- 2 Simplify future infrastructure expansion and modification to lower the total cost of ownership (TCO)
- 3 Integrate all security, access control, and video surveillance into a unified platform with a single interface
- 4 Obtain a greater return on investment through uses that go beyond locking and unlocking doors

With an IP-based solution, an organization can also take advantage of newer functionalities that are not available with traditional systems. For this reason, it is important to consider how to leverage new ACS capabilities offered by IP-based solutions, including:

- 1 Improving multi-site management and monitoring
- 2 Scaling to greater door counts over a network
- 3 Enhancing cybersecurity with end-to-end encryption and advanced authentication
- 4 Using global cardholder management to move to a single card across all sites

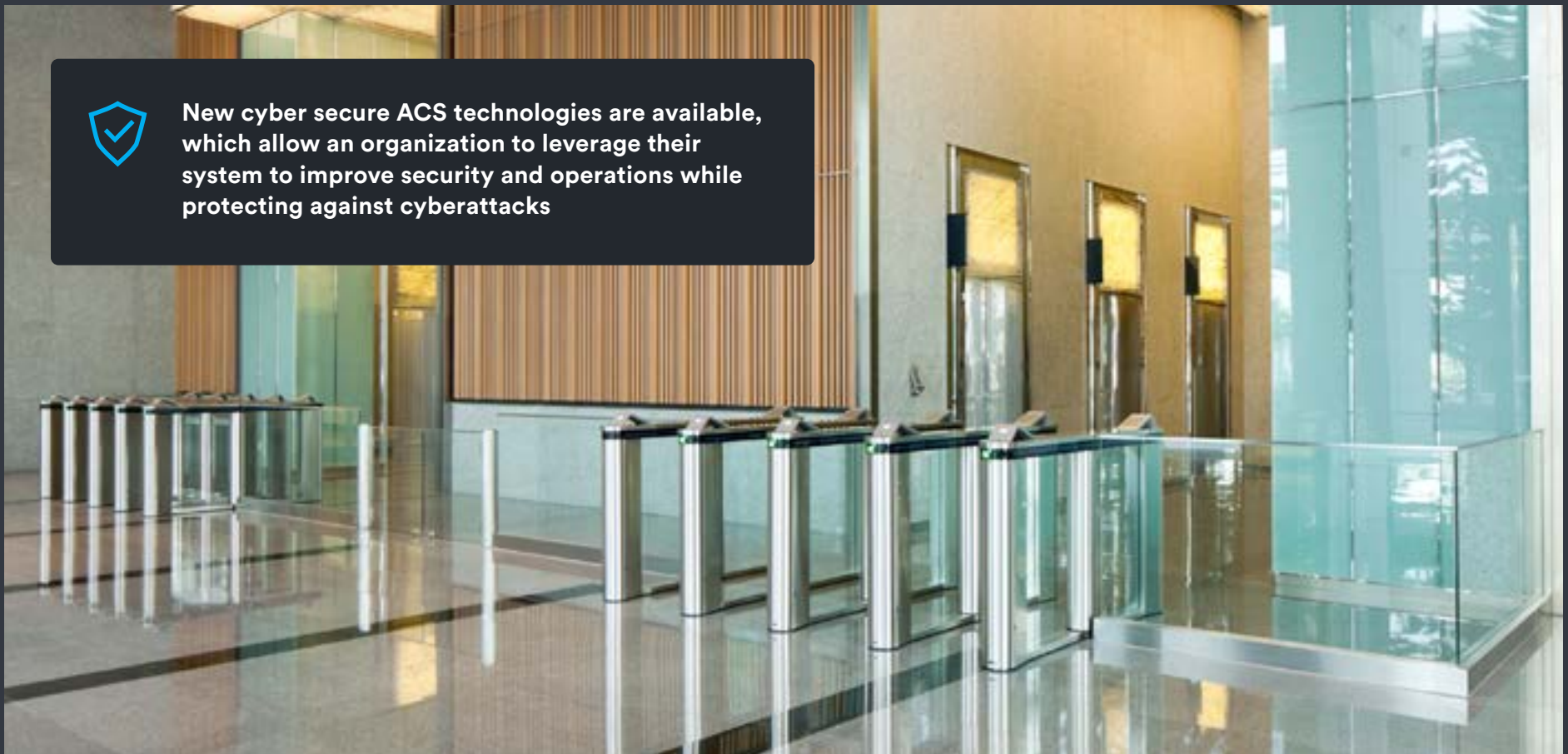
Traditional physical ACSs are also becoming increasingly expensive to maintain. When legacy ACS components reach the end of their service, the costs associated with maintaining such systems or finding replacement parts increase.

Also, traditional ACSs lack the ability to withstand an evolving number of cyberattacks. Legacy ACSs use outdated technology that leaves them vulnerable to cyber threats. New cyber secure ACS technologies are available, which allow an organization to leverage their system to improve security and business operations while protecting against cyberattacks.

Lastly, because legacy systems typically operate by delivering separate power to each card reader and lock, they are more expensive than an open, flexible IP-based ACS that supports Power over Ethernet (PoE) to connect and power all IP-based door controllers, readers, and door locks.



New cyber secure ACS technologies are available, which allow an organization to leverage their system to improve security and operations while protecting against cyberattacks



Goals for a migration

After deciding to migrate from an older legacy system to an open, flexible IP-based ACS, an organization should consider the following goals when searching for a solutions provider.



Buying a system with a long life span

When trying to determine the life span of an ACS, there are numerous factors to consider:

Is the solution non-proprietary and open architecture?

An open architecture, non-proprietary ACS makes it easier to expand and modify the system in the future.

Does the solution provider have a developed ecosystem of partners?

Choosing a solution provider with technology partners in areas such as asset management, human resources, and visitor management ensures greater flexibility and more options during migration and future modification.

Does the solution provider offer an off-the-shelf software development kit (SDK)?

An off-the-shelf SDK allows for custom integration and scripting and makes it possible to develop plug-ins to the IP-based ACS in the future.

Reusing existing equipment

Migrating to an open, flexible IP-based ACS can enhance and protect an organization's long-term investment in their current security infrastructure by extending the life of existing components and by leveraging new system features and applications.



Migration to an IP ACS can enhance and protect an organization's long-term investment in their current security infrastructure by extending the life of existing components and by leveraging new system features and applications.



In addition to analyzing features, an organization should also look at their current access control workflow to ensure that the solutions provider will be able to at least maintain, if not improve the workflow in the new system.

Work in parallel

To achieve a seamless ACS migration, pre-staging work should be done in parallel and offline to build the configuration of the new IP-based ACS into the software, including:

- 1 mapping the system
- 2 importing the inputs and outputs (IOs) from the system components
- 3 integrating the logic to control the components



Keep downtime to a minimum

When migrating an existing system, an organization must consider the impact that downtime will have on system users. During the selection stage it is important to determine:

- 1 the peak hours during which the ACS must be fully functional
- 2 whether or not the new IP-based ACS allows for pre-staging
- 3 if the new IP-based ACS can be connected to existing doors in parallel

Ensure that all crucial functionality remains available

It is important for an organization to review the hardware and software features currently being used in their legacy ACS to ensure that these features will also be available in the new system. Features that should be analyzed include:

- 1 the number of doors that can be supported
- 2 cardholder management
- 3 access rights management
- 4 badge design
- 5 web client needs
- 6 mobile app needs
- 7 visitor management
- 8 enrollment devices

In addition to analyzing features, an organization should also look at its current access control workflow to ensure that the solutions provider will be able to at least maintain, if not improve the workflow in the new system.



Overview of considerations

The following considerations are intended to help an organization evaluate its current legacy ACS.

The results of these evaluations have a direct impact on (1) the decision to conduct a migration with full replacement or partial replacement, (2) the cost of the migration, and (3) the time required for the migration.



Hardware considerations

Any migration from a legacy ACS to an open, flexible IP-based ACS must begin by evaluating the current system.

Migrating to an IP-based ACS is simplified if the existing system uses non-proprietary cards and readers. However, if the existing readers support proprietary communication, then a full replacement of legacy readers is likely required.

It is also important to determine if the existing intelligent controllers and downstream interface panels can be reused. If the existing controllers are open architecture, then it may be possible to incorporate them into the new ACS.



ACS migration requires the expertise of pre-sales engineers, technical specialists, field service engineers, and support engineers.



Software considerations

It is important to determine exactly what needs to be ported to the new system. Consideration must be given to the native data in the legacy credentials, the tools used to export that information from the current database, and any third-party components integrated into the configuration through the SDK.

Network considerations

The network needs of the new IP-based system must also be evaluated when considering migrating to a PoE access control solution.

In addition, an organization must also consider issues of latency and bandwidth regarding communication between sites when migrating a distributed system with both local and remote sites.

Wiring considerations

The wiring in a legacy ACS is another important consideration for any migration, since it may be possible to reuse some of the existing wiring in the new IP-based ACS. Prior to migration, it is important to compare the characteristics of the existing cabling against the requirements for the new IP-based ACS equipment. Additionally, if an organization is looking to expand its current ACS during migration, consideration must be given to the extra wiring that will be required.

Power considerations

Prior to migration, consideration must also be given to the type of power in place in the current ACS, specifically whether the system is 12V or 24V and DC or AC, and whether it can provide enough current for the new hardware components.

Training considerations

Any successful migration to an open, flexible IP-based system requires comprehensive training on how to use the new software. Therefore, consideration should be given to the type of training required for the various ACS users, based on their tasks and the client applications they will use with the new ACS.

Support during the migration and later

For a successful migration, it is important to take into account the level of support provided by the integrator installing the new ACS, as well as by the manufacturers and solutions providers whose components will make up the new system. ACS migration requires the expertise of pre-sales engineers, technical specialists, field services engineers, and support engineers.



Steps in the migration process

There are multiple steps involved in a successful migration. First, the customer works with a systems integrator and possibly manufacturers and solutions providers to build a quote and a migration plan. As the plan is being implemented, technical support and field engineers will design and configure the new IP-based system.



Get the facts

The first step for the systems integrator is to create the configuration of the current ACS, including details such as the location of electrical and telecom closets, wiring, and the type of power currently in place. It is also important to develop a complete list of the hardware components, servers, and networking equipment currently being used in the system, as well as provide details about current software features that will be required.

Understand the requirements of the new system

To develop a successful migration plan, the following requirements of the new open, flexible IP-based ACS must be recognized and confirmed:

- 1 hardware components
- 2 software components
- 3 network configuration
- 4 wiring
- 5 power

Understanding these requirements is critical for designing the architecture of the new system.

Site survey

The next step is a walk-through of the facility with the customer, systems integrator, and possibly with manufacturers, to ensure that no part of the existing system has been overlooked. The site survey can also be the first step in the overall process. The purpose of the site survey is to:

- 1 develop a clear picture of the existing architecture and layout of the existing system
- 2 determine where equipment is concentrated
- 3 measure the distances between access control panels, power sources, and readers



Determine components that can be reused

A complete picture concerning an organization's current ACS and the requirements for the new system is essential for determining what hardware, software, power, wiring, and networking components can be reused.



A complete picture concerning an organization's current ACS and the requirements for the new system is essential for determining what hardware, software, power, wiring, and networking components can be reused.



To ensure a seamless migration, the integrator should undertake a complete walkthrough of the new IP system before executing the migration.

Testing existing components

After determining what components of the existing system can be reused, the components should be tested to ensure compatibility.

Define new equipment needs

With a clear understanding of what can be reused from the existing legacy system and what is needed in the new system, the integrator must now determine the new network and access control needs.



Understand the existing databases and data

Determining how to import existing cardholder and credential data into the new IP-based ACS is the next step in the migration process. To leverage existing third-party software data, technical specialists or field engineers will need to export cardholder and credential data from the existing system into a usable file format.

Plan the migration

To keep downtime during migration to a minimum, the hardware migration must be carefully planned to ensure that as much software and hardware installation as possible is accomplished in parallel.

Test the new IP system

To ensure a seamless migration, the integrator should undertake a complete walk-through of the new IP system before executing the migration.

Execute the migration and acceptance testing

Following the schedule developed as part of the migration plan, the systems integrator and customer can now begin cutover from the old to the new ACS. At this point, it is important to have manufacturers on standby in case any problems arise with any of the new ACS components.



The Genetec and Mercury advantage

Modernization Simplified

With Genetec and Mercury open architecture solutions, customers have the power to upgrade to the latest supported technology at any time, or even unify their security and operations into one single platform.



The benefits are undeniable:



Open

Based on two open platforms, the Genetec and Mercury partnership delivers versatile access control solutions on the market. It enables organizations to easily adapt to changing technologies, industry standards, and network environments. By combining the Genetec software solutions with Mercury's advanced hardware, we empower organizations to proactively address dynamic system requirements. Together, we ensure seamless integration with smart building technologies, making your infrastructure smarter and more connected.



Secure

Genetec and Mercury both uphold stringent cybersecurity standards with their security-by-design methodologies. Our collaborative systems feature robust security, encryption, and advanced authentication methods to safeguard your assets, data, and people.



Connected

With open architecture at the core, the Genetec and Mercury partnership provides unmatched flexibility for third-party application integration. Supporting OSDP (secure channel), IIoT protocols (BACnet, MQTT, etc.) and networking protocols, ensuring seamless integration of building automation, elevator control, wireless locks, and more. By leveraging Genetec's IP-based systems alongside Mercury's API, organizations achieve the interoperability and freedom required to build a truly connected and future-ready access control infrastructure.

Looking for how to get started?

Established in 1997, Genetec is the global leader in unified security platforms, with a broad offering across a range of security specialties.

The partnership between Genetec and Mercury is strengthened by the extensive experience and longstanding reputation of both companies in the physical security sector. As a customer, you benefit from the combined knowledge and expertise of two leaders, spanning decades in the access control industry. This well-established collaboration ensures seamless integration, reliable performance and ongoing support for customers, backed by years of experience working together. By partnering with Genetec and Mercury, you gain access to cutting-edge products that form the foundation of a secure and efficient access control solution.

Video surveillance:

Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Operational decision support:

Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Access control:

Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Investigative case management:

Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Automatic license plate recognition:

Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Cloud services:

Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your organization to easily cope with rapidly changing security requirements and operate with greater efficiency.

Genetec[™]

 **Mercury**

Genetec Inc.
Genetec.com
info@genetec.com
@genetec