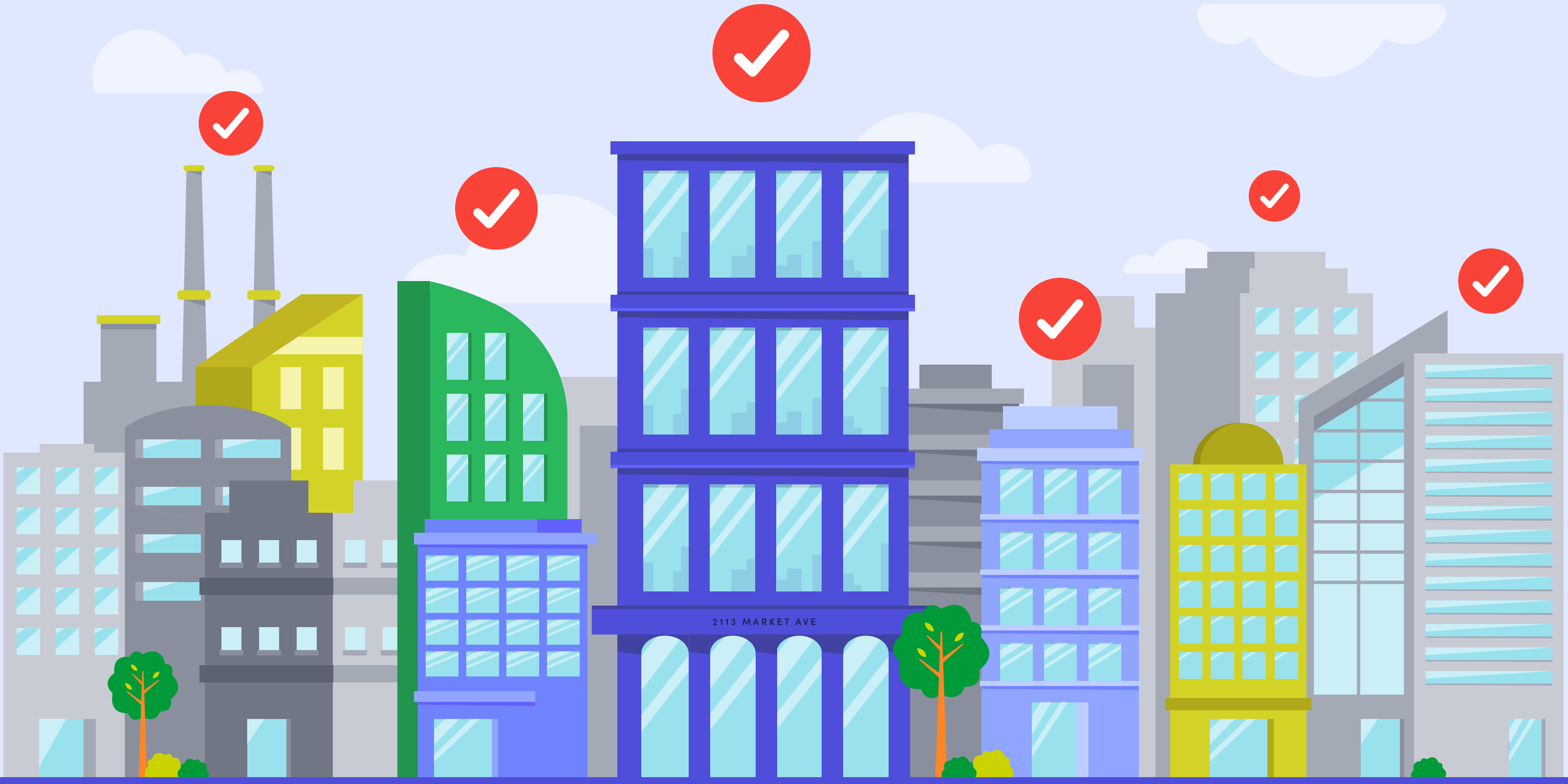
Envoy

EBOOK

The IT and physical security guide to new deployments

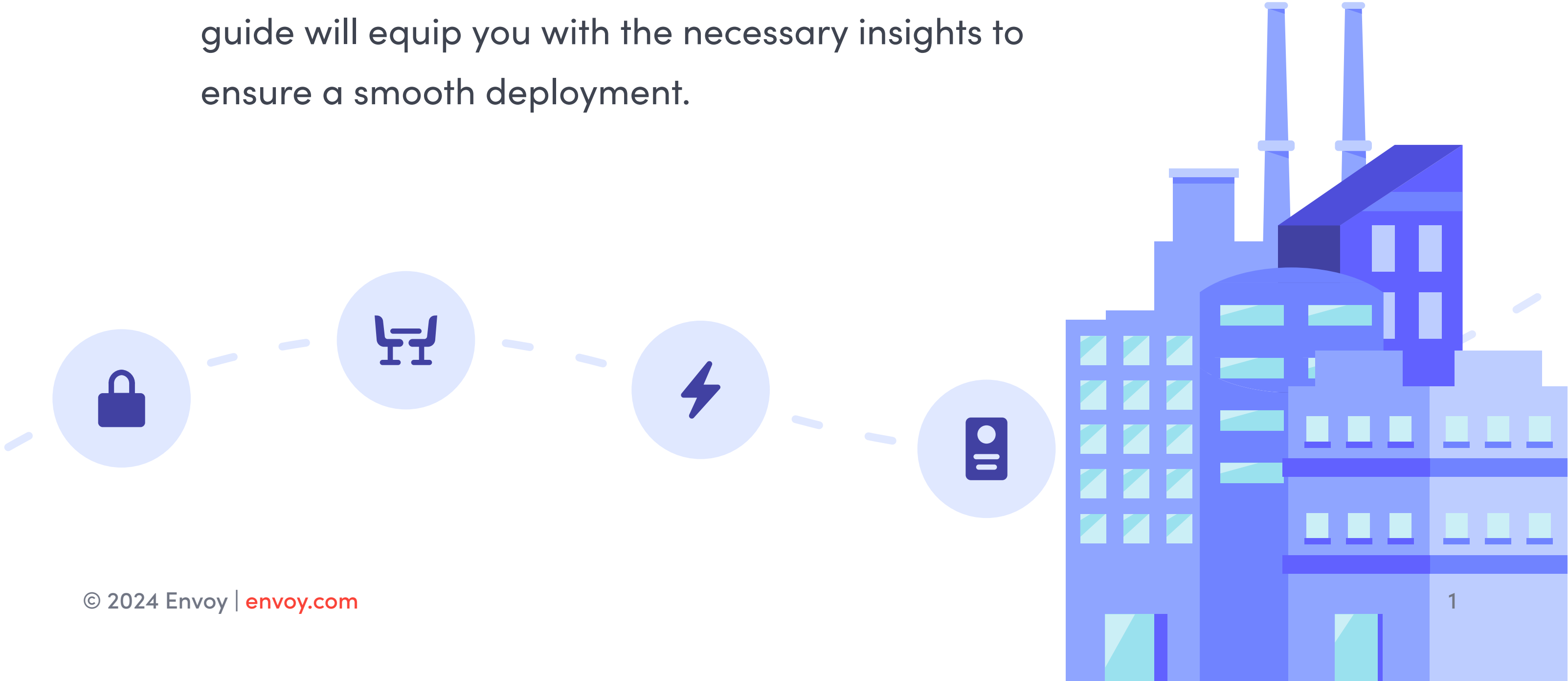


© 2024 Envoy | envoy.com

The nature of workplace security has become more complex in recent years. Security attacks are becoming more sophisticated. Data privacy concerns continue to inspire more laws and regulations. Adding to the confusion is the rise of distributed office models. Organizations now face an increasing demand to stay flexible, secure, and efficient amid these evolving threats and concerns.

Workplaces are multifaceted and require collaboration across a number of teams beyond just technology. This is especially true during new deployments, where constant coordination with stakeholders at every step is required. No matter if it’s integrating new and old workplace systems or tailoring security measures to specific site needs.

Successful deployments require careful planning, cross-departmental collaboration, and expert guidance. Whether you’re overseeing the move to a single new location or managing the security considerations of a global expansion, this guide will equip you with the necessary insights to ensure a smooth deployment.



© 2024 Envoy

Common challenges during deployments in new buildings

Setting up technology and security systems in a new building is a complicated job. This process involves various challenges that can vary greatly depending on the scale of operations, the diversity of the existing infrastructure, and any specific security needs. More specifically:

1. **Site-specific security requirements.** Customizing security measures to match the specific design and needs of a new building is crucial but can be complicated. This could include installing a virtual front desk, using biometric systems for access control, and setting up advanced visitor management systems. These systems should be able to track everyone coming in and out, work well with other security systems, and provide detailed reports for compliance checks and audits.

2. **Infrastructure compatibility.** It can be a significant hurdle to ensure that the new building's existing IT infrastructure is compatible with the new technology being installed. This involves checking things like network connections, data cables, power supply, and compatibility with existing hardware and software systems. For example, connecting old access control systems with a new building's entry points and door hardware might need careful planning and some upgrades.

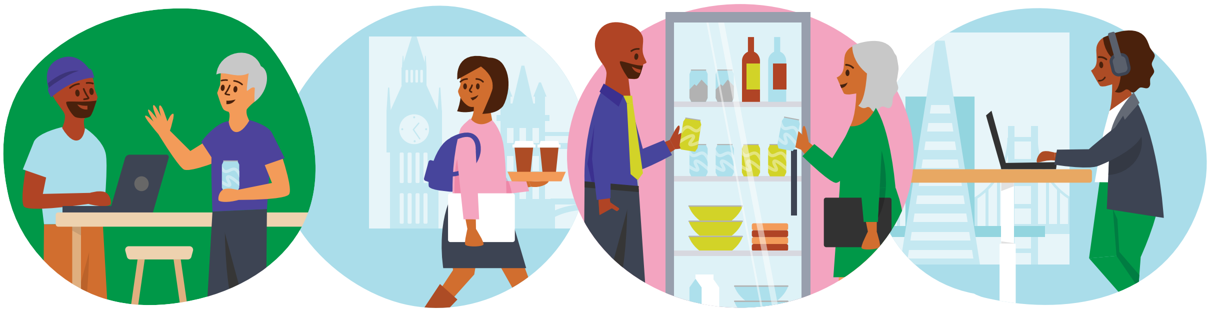
3. **Issues with compliance.** Compliance with local, national, and international regulations presents another layer of complexity. For example, Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) demand strict handling of data and privacy protection. Additionally, physical security measures must align with industry standards and possibly even specific insurance requirements.

4. **Vendor management.** Coordinating with multiple vendors for the procurement, installation, and maintenance processes can be tedious and headache-inducing. For deployment teams, tasks may include scheduling installation appointments, ensuring compatibility between different components, and overseeing the installation process.

5. **Budget constraints.** Tighter budgets may limit the resources available during deployment. IT and security teams need to carefully decide where to spend based on what's most critical for risk and business needs, all while staying within their budget.

First steps: Cover your bases

Setting up security and visitor management policies in a new building involves several important steps. These range from assessing the new building's security infrastructure to establishing a visitor management policy. But, IT and physical security teams still have to deal with various technical, operational, and regulatory roadblocks. These challenges might seem daunting, but with the right approach, they can be managed successfully. Careful planning and collaboration across departments can help you successfully navigate this process.



1 Establish a deployment tiger team

Forming a "tiger team" is a crucial first step for ensuring a successful rollout. Your tiger team should include representatives from various departments and disciplines to ensure comprehensive coverage and expertise. Some key departments to include are:

- □ **Information technology (IT).** At the center of most deployments is, of course, the IT department. They play a key role in integrating new systems with your existing tech and handle all aspects of network setup and data security. Including IT leaders is essential because they make sure the technology deployment aligns with the broader IT strategy and complies with cybersecurity policies.

- □ **Physical security.** This team handles the setup of security systems like access control, video surveillance cameras, and alarms. They have a deep understanding of security risks and how to manage them, which helps ensure the measures are effective and meet industry standards and regulations.

- □ **Workplace and facilities.** Their role is crucial for handling the logistics for installations and confirming that the new security features work smoothly with other building services. This is the team responsible for coordinating the installation of the physical components of security systems.

- □ **Human resources (HR).** The HR team works closely with other departments, such as IT, legal, and physical security, to ensure that all aspects of the deployment are compliant. This cross-functional collaboration is vital to identifying potential compliance issues early in the deployment process and addressing them proactively.

- □ **Legal.** The legal department ensures the deployment process complies with relevant laws, regulations, and industry standards. They review contracts, agreements, and permits related to the new location to ensure legal compliance and mitigate regulatory risks. Their involvement ensures the deployment process proceeds smoothly and legally, minimizing potential legal liabilities and risks.

- □ **Marketing.** The marketing department helps ensure that the branding on badges, check-in kiosks, and other materials align with the company's guidelines. Consistent branding reinforces the organization's identity and values, promoting a cohesive and consistent experience.

2 Settle on your software and hardware needs

Deployments at a new location require a well-planned mix of both software and hardware. The specific needs can vary greatly depending on the nature of the business, the industry regulations, and the scale of operations. Your choices should focus on specific business requirements, ability to scale, security considerations, and compliance requirements.

Here's a brief overview of the common types of software and hardware needed during these setups:

- □ **Access control.** These systems regulate entry to the premises by managing electronic locks, access cards, and biometric authentication (e.g., facial recognition). Access control hardware is used to secure entry points and manage access permissions onsite.

- □ **Networking equipment.** The hardware needed includes routers, switches, modems, firewalls, and wireless access points. These devices establish and maintain connectivity within your network infrastructure. In short, they enable devices to securely communicate and share data with each other.

- □ **Servers and data storage devices.** This hardware is used to host and manage enterprise software applications, databases, and digital files. They provide the necessary computing power and storage space needed for day-to-day business operations.

- □ **Physical security solutions.** Deploying physical security systems in new locations involves a combination of sophisticated hardware and software. These can include video surveillance cameras, alarm systems, motion sensors, and emergency notification systems, to name a few.

- □ **Visitor management system (VMS).** These platforms help you track and manage visitor access to your facilities, including registration, check-in/check-out flows, and badge issuance. Modern solutions come with features that enhance workplace safety and efficiency (e.g., integration capabilities, real-time tracking, emergency notifications, and robust data protection). Additionally, visitor management systems have hardware requirements. For example, Envoy supports various iPad models and Brother printers and badges.

3 Get all your technical ducks in a row

Setting up the technical framework is a foundational step for IT and physical security teams. This process requires careful planning and precise execution to make sure your tech stack is effective, scalable, and adaptable to each location's unique needs. Some recommended steps:

- □ **Choose system admins and assign roles.** Begin by identifying and appointing system administrators who will oversee the deployment and ongoing management of your security systems. These individuals need a strong grasp of the technical details and how these systems operate day-to-day. Assign roles based on expertise: network security, physical security, software management, and compliance are all areas that require dedicated oversight.

- □ **Set up your employee directory.** Make sure your employee directory is up-to-date and includes everyone working at the new location. Include important details like employee IDs, access permissions, and contact information. This directory should be integrated into your security and visitor management systems to enable automatic updates and easier management. This will help facilitate smoother onboarding and offboarding processes, keep access rights up-to-date, and reduce security risks from outdated information.

- □ **Create a default deployment template.** Put together a template that documents best practices and standard procedures for your organization. This template should cover configurations for hardware and software settings, standard operating procedures for security incidents, and baseline visitor management protocols. What's the benefit of creating a deployment template? It provides a consistent approach to security across all locations, simplifying the process across the board.

- □ **Customize the template to your new location's needs.** While a default template provides a good starting point, you do have to tailor it to meet the specific needs and risks of each new building. Factors such as local regulatory requirements, weather and environmental conditions, architectural layout, and operational needs should influence how you adapt your security measures. For example, a building in a high-risk area may require more stringent access controls than one in another neighborhood.

Expert advice

Dana Stocking, Envoy’s Head of Workplace Technology

Question: When opening a new location, what steps do you take to ensure all compliance regulations are met?

Dana: When opening a new location, the first step is understanding the specific compliance requirements of the state where the new office will be. Since different states have different regulations, it’s crucial to start with thorough research to determine exactly what’s needed in terms of regulatory compliance for that particular location.

Besides state-specific requirements, there are also universal compliance standards that apply everywhere, regardless of location. For example, SOC 2 compliance often requires monitoring systems that record who enters and exits our buildings. Ensuring compliance both at a state level and with these overarching standards is essential for every new office.

To manage this process effectively, I recommend assembling a dedicated tiger team comprising members from key departments. This team should meet regularly, ideally through weekly updates, to ensure that every aspect of compliance is being addressed.

Next steps: Set the ground rules

After laying down the technical foundation, the next step is to create clear and actionable policies and procedures. This phase is pivotal in ensuring your security infrastructure functions effectively and complies with relevant laws and regulations.

4 Develop compliance policies and processes

Start by understanding the legal requirements and work closely with your Legal and HR departments. Your policies should address all areas of physical security, data protection, and visitor management, ensuring they meet industry and legal standards. Set up processes for regular audits to stay on top of compliance. Also, include clear steps in your policies for what to do if there's a security breach to mitigate damage and quickly inform everyone who needs to know.

5 Determine your employee check-in workflow

This is the process employees use to register their presence when they enter your facility or specific areas within it. Employee registration flows help organizations track and manage employee movements when onsite. You will have to tailor the check-in steps for your new location to meet local health and safety requirements. For example, you can include automatic check-ins, pre-check-in questionnaires, waivers, or safety videos in your check-in process.

6 Set capacity limits for your facility and sensitive areas

Establish how many people can be in the facility and specific areas like server rooms or research labs. Based on the size and safety regulations of the new location, you should set clear capacity limits to ensure evacuation routes and safety measures are adequate during emergencies. Access to these areas should be restricted to authorized personnel only and monitored closely.

Pro tip: Use real-time monitoring tools to alert security when capacity limits are close to being reached or exceeded.

7 Create a visitor policy

A good visitor policy keeps people and assets safe and makes guests feel welcome. Here's how to put your plan into motion:

- □ **Decide if your front desk will be staffed.** The decision on whether to staff your front desk impacts how visitors will interact with your security and VMS. A staffed front desk can provide a personal touch and handle complex visitor issues more effectively. On the flip side, an unstaffed front desk might rely more on automated systems such as Envoy's virtual front desk, which can include static QR codes and self-service kiosks. These systems can make check-ins more efficient and consistent while reducing staffing costs. Consider your volume of visitors and your specific security needs when making this decision.

- □ **Identify your visitor types.** Figure out the different kinds of visitors your facility may have, like contractors, vendors, job candidates, or customers. The information you capture and access levels you provide may vary based on each guest's reason for visiting. Knowing these differences helps you tailor security measures and make the check-in process smoother.

- □ **Set up pre-visit communication.** Clear communication before a visit improves the visitor experience and speeds up check-ins. Share important information like parking details, check-in steps, which ID to bring, and contact points upon arrival. This helps visitors come prepared and understand the security procedures.

- □ **Maintain a detailed log of all visitor entries and exits.** Determine the information you need to collect from visitors for auditing purposes, such as their name, contact details, purpose of visit, areas accessed, and duration of stay. Detailed records are crucial for checking security measures and proving compliance with safety standards.

- □ **Determine necessary legal documents for signing.** Depending on the nature of the visit, visitors may need to sign legal documents such as non-disclosure agreements (NDAs), safety waivers, or data privacy consent forms. Automate the distribution and signing of these documents as part of the check-in process to ensure compliance and minimize paperwork.

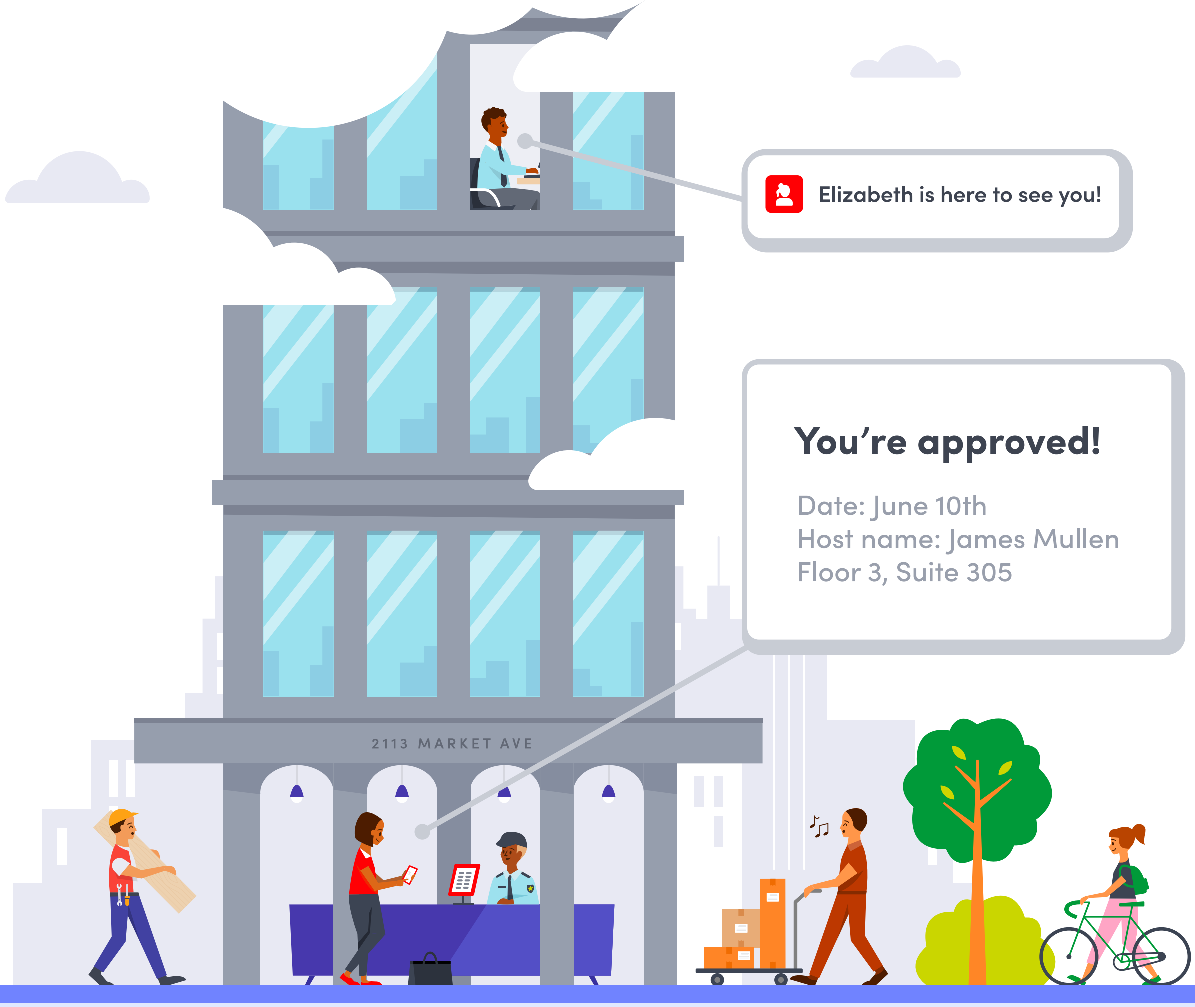
- □ **Establish procedures for identity verification.** This could include checking a government-issued ID or performing background checks. Many visitor management systems can connect with identity screening software like Visual Compliance to make this process smoother. Some modern solutions even come with photo capture and facial recognition capabilities, which can further streamline identity checks.

- □ **Develop a process for creating and printing visitor badges.** Choose what details to print on badges, such as visitor names, host names, sign-in times, and custom messages, which can include Wi-Fi credentials.

Visitor management systems let you customize badges for different types of visitors and include options to add logos, photos, and barcodes.

> **Pro tip:** Badges should be color-coded or marked to quickly identify different types of visitors.

- □ **Implement host notifications.** In your visitor management system, you can customize notification settings for each host. This can involve choosing how they'll receive notifications—via email, SMS, or app notifications—and tailoring the content in the message. You can also adjust settings to ensure notifications are sent only during specific times, based on visitor type, or for denied entries (e.g., a visitor matches a block list).



Expert advice

Nicole Persaud, Samsara’s Head of Global Safety and Security

Question: If you were moving into a new building, what would be your three top tips?

Nicole: If you’re at the stage where you can influence the design—particularly during tenant improvements or if it’s a completely new building—here are my top three tips:

1. Integrate security into the building’s design. One of the most effective ways to enhance security is to incorporate it directly into the building’s design. For example, consider the layout of elevator vestibules. Typically, emergency exits are separate from the main vestibule area, but integrating an emergency exit into the vestibule itself can reduce security risks. By placing a push-to-exit button inside the vestibule, you comply with safety regulations while also simplifying the structure and minimizing the need for additional security hardware and monitoring. This approach not only enhances security but also reduces costs and complexity.

2. Get involved early in the design process. It’s essential to participate in the design process from the beginning. This allows you to address security concerns right from the start, rather than trying to retrofit solutions later. By engaging early, you can ensure that the building’s architecture itself contributes to security, which is often overlooked by architects and designers who may not view building features through a security lens.

3. Define your security building standards. Determine and document your security standards based on whether you’re in a leased space or a serviced office. These standards should outline what is mandatory and what is optional, tailored to the specific risks and uses of your space. From there, you can decide which security solutions to implement based on a thorough risk assessment and available budget.

By following these tips, you ensure that your new building is not only aesthetically pleasing and functional but also secure and compliant with safety regulations. This proactive approach to security in the design phase can save time and expense down the road.

Groundwork: Hardware and software installation

At this stage of the process, it's time to start laying the proper groundwork with careful hardware and software installation. Successful installations are key because they directly affect how well everything works in a new location. They ensure that systems function properly, are secure, meet compliance standards, and operate efficiently.

8 Source trusted integration partners

Having trustworthy and knowledgeable integration partners is critical. Issues during installations can delay deployments and increase costs in the long run. Evaluate potential integration partners based on their expertise, experience, and reputation. Review their case studies, customer testimonials, and certifications to ensure they meet your requirements.

Pro tip: Choose partners who are familiar with your security systems.

9 Pair and connect your hardware

The next step is to pair and connect your hardware to your network infrastructure, including access control, surveillance cameras, and visitor kiosks. Proper configuration is crucial to avoid gaps in security coverage and ensure that all components communicate effectively with one another. Also, be sure to test the hardware to check that everything works smoothly together.

10 Integrate your essential workplace systems

Integrating workplace systems with your security setup is crucial for better operational efficiency and security management. Here are some systems you might need to integrate with your visitor management system:

□ **Wi-Fi.** Ensure that your Wi-Fi infrastructure is robust and secure, as it will be the backbone for wireless security devices and mobile-based access controls. Implement strong encryption and secure authentication methods to protect against unauthorized access.

□ **SAML/SSO and SCIM.** Use Single Sign-On (SSO) and System for Cross-domain Identity Management (SCIM) to make user authentication and authorization secure and straightforward across all platforms. This improves security by minimizing potential risks and enhancing user experience by reducing the need for multiple passwords.

□ **Access control.** Integrate your access control systems with your VMS to enable centralized management of entry points and user permissions. This integration allows for real-time updates and automated responses to security incidents.

□ **Workplace ticketing.** Integrations with your workplace ticketing systems (e.g., Jira, ServiceNow) can help you better manage IT requests, facility issues, and more. As a result, every incident will be logged, tracked, and resolved.

□ **Communication tools.** Link your communication tools (e.g., Microsoft Teams, Slack) to enable instant notifications and alerts about security events to the relevant personnel. This can enhance the speed and efficiency of your security response.

□ **Calendar.** Connect your visitor management system with your organization’s calendar system to automate appointment scheduling and management. This will help you prepare for visitor arrivals in advance and enhance the visitor experience.

□ **Custom tools.** If your organization uses custom-built tools, ensure these are integrated into your security ecosystem. These might include specialized software for data analysis, project management, or customer relationship management (CRM). This may require custom API integrations or the development of bespoke interfaces by your IT team or external partners.

Expert advice

Lee Odess, Access Control Leader

Question: What should security leaders prioritize in 2024?

Lee: In considering what security leaders should prioritize in 2024, we need to take a broad view, especially regarding access control systems. Historically, the primary focus of these systems has been to keep unauthorized individuals out—essentially safeguarding against potential threats.

However, the role of access control is evolving. Now, it's about efficiently letting the right people in, enhancing operational efficiencies, and potentially increasing revenue. This shift is about leveraging the utility of these systems beyond traditional security measures.

From my experience working with numerous companies, there's a growing need for a deeper curiosity about what our security systems can do. It's about not just installing systems and letting them run on autopilot for decades. While preventing incidents is crucial, we now see a need to push these systems further, to truly maximize their potential.

This involves rethinking and possibly redefining our relationships with technology providers and forming new partnerships. It's about seeing these systems as dynamic tools that can provide exponential value, not just static measures that only respond when threats are detected.

So, for 2024, the top priorities for security leaders should be driven by curiosity and a willingness to expand our expectations of what our security systems are capable of achieving. We need to explore new possibilities for using these systems to enhance our operational capabilities and contribute more significantly to our organizations.

Last steps: Finishing touches

As you near the final stages of deploying a security and visitor management policy in your new building, it's crucial to focus on the finishing touches to ensure comprehensive protection and preparedness. Here are the key steps to follow:

11 Double-check your security posture

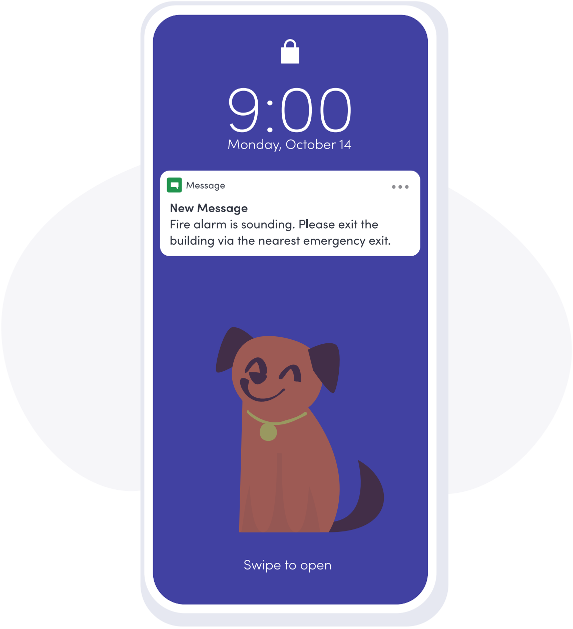
Before declaring the security system operational, perform a comprehensive review of all installed systems and protocols. This includes:

- □ **System testing.** Perform stress tests and simulate different security scenarios to ensure systems respond as expected. Check alarm triggers, access control responses, system integrations, and any of your other security technology.
- □ **Vulnerability assessments.** Have security experts perform vulnerability scans and penetration testing on your networks and systems to identify and address any potential security gaps.
- □ **Review integration points.** Ensure that all systems are correctly integrated. This means verifying that your visitor management system communicates seamlessly with access control and that all data flows are secure and without any gaps.
- □ **Physical inspection.** Walk through the facility to ensure that all entry points are properly secured with functional access controls.

12 Establish emergency protocols

Having robust emergency protocols in place is crucial for the safety of everyone in the building. Set clear procedures for various potential emergencies, including fires, natural disasters, and security breaches. Key elements to include are:

- □ **Evacuation routes and procedures.** Clearly define and mark evacuation routes. Regularly review these routes to ensure they remain unobstructed and clearly visible.



New Message
Fire alarm is sounding. Please exit the building via the nearest emergency exit.

- □ **Communication plans.** Set up and test communication systems that will be used during an emergency. This includes internal communication among security staff and communication with external emergency services.

- □ **Emergency response team.** Designate a team responsible for initiating and managing emergency protocols. Train them in specific roles, including first aid, crisis communication, and technical support for security systems.

13 Conduct employee and admin training

The effectiveness of your security and visitor management systems greatly depends on how well employees understand and adhere to established protocols. A few things to consider:

- □ **Employee training.** Conduct training sessions to familiarize employees with the new systems. Include practical demonstrations on how to use security badges, sign in and out of visitor management systems, and whom to contact in case of security concerns.

- □ **Admin training.** Provide specialized training for system administrators and security personnel. This should cover system monitoring, managing visitor access, responding to security alerts, and troubleshooting common issues. Ensure that admins are also trained on regulatory compliance aspects and data privacy concerns.

- □ **Security awareness.** Foster a security-conscious culture by educating employees about potential security threats and how to prevent them. Encourage them to report suspicious activities and understand the importance of following security protocols.

- □ **Refresher courses.** Implement an ongoing training schedule that includes periodic refresher courses to keep everyone updated on new security features, changes in protocols, or emerging threats.

Step-by-step deployment checklist

First steps:

Cover your bases

- ○ Establish a deployment tiger team
- ○ Settle on your software and hardware needs
- ○ Get all your technical ducks in a row
  - ○ Choose system admins and assign roles
  - ○ Set up your employee directory
  - ○ Create a default deployment template
  - ○ Customize the template to your new location's needs

Next steps:

Set the ground rules

- ○ Develop compliance policies and processes
- ○ Determine your employee check-in workflow
- ○ Set capacity limits for your facility and sensitive areas
- ○ Create a visitor policy

Groundwork:

Hardware and software installation

- ○ Source trusted integration partners
- ○ Pair and connect your hardware
- ○ Integrate your essential workplace systems

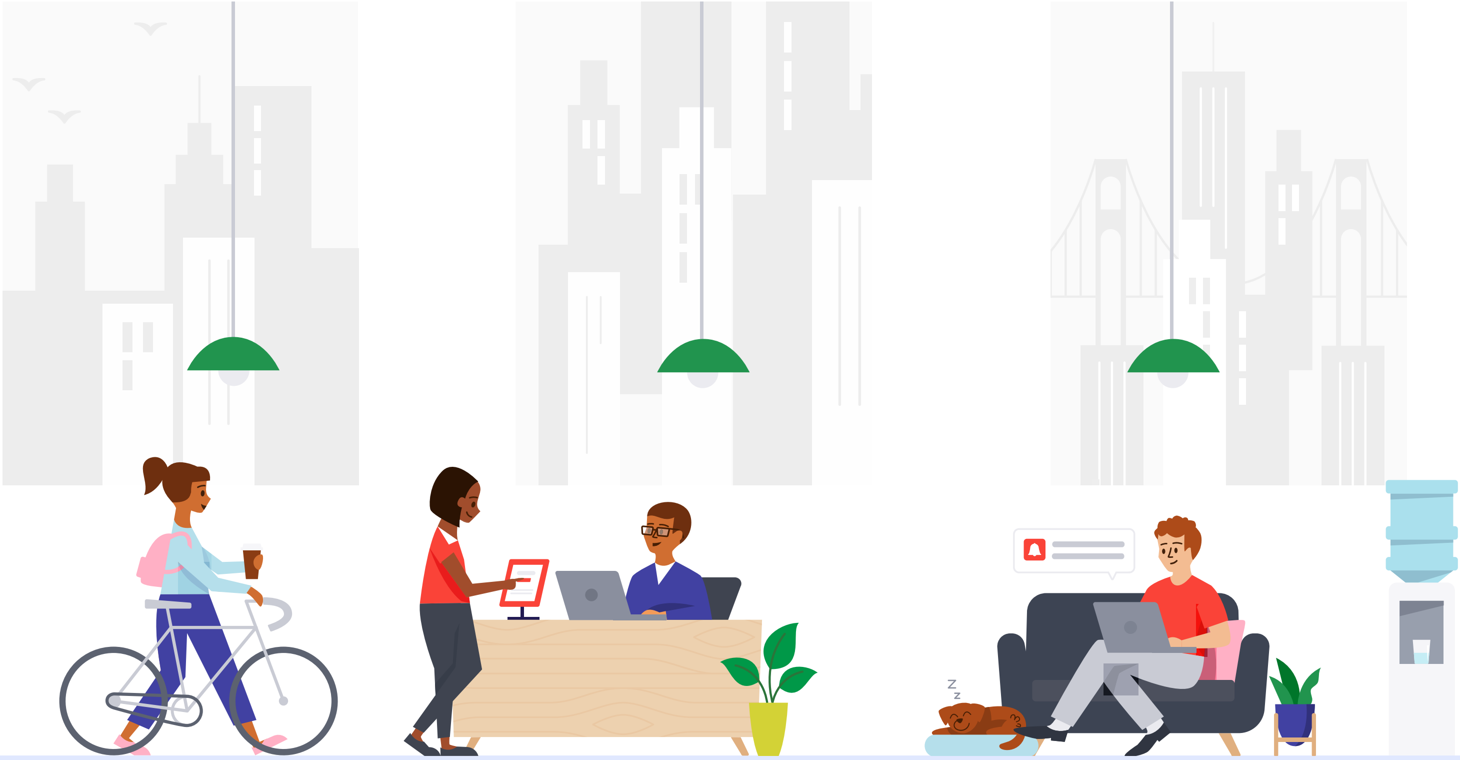
Last steps:

Finishing touches

- ○ Double-check your security posture
- ○ Establish emergency protocols
- ○ Conduct employee and admin training

Conclusion: Tying it together with Envoy's Visitor Management System

Since your business is constantly evolving, so should your approach to security and visitor management. Visitor management systems are crucial for dealing with increasing complexity, offering integrated solutions that connect smoothly across various platforms and devices. More than just an operational upgrade, a VMS is a strategic step towards a more streamlined, cost-effective, and efficient business ecosystem.



About Envoy

Envoy's workspace platform has redefined how companies manage modern workplaces. 16,000 workplaces and properties around the globe rely on Envoy's fully integrated solution to create an unrivaled first impression, keep spaces secure and compliant, and solve common and complex workplace challenges. From multi-tenant buildings and corporate headquarters, to labs, production sites, and factory floors, Envoy powers the places where people work best together.

© 2024 Envoy, Inc.

Envoy