Building a Mobile Access Program

10 Tips for Making Your Project a Success
## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Introduction to Mobile Access Control</td>
</tr>
<tr>
<td>07</td>
<td>Tip #1: Define Levels of Access Based on User Profile and Role</td>
</tr>
<tr>
<td>09</td>
<td>Tip #2: Balance Ease of Access with Security Needs</td>
</tr>
<tr>
<td>12</td>
<td>Tip #3: Assess the Internet Connectivity at Your Access Points</td>
</tr>
<tr>
<td>15</td>
<td>Tip #4: Choose a Pricing Model That Works for You</td>
</tr>
<tr>
<td>18</td>
<td>Tip #5: Stick with Open Standard Access Control Protocols</td>
</tr>
<tr>
<td>20</td>
<td>Tip #6: Consider Keeping Your Existing Access Control Software</td>
</tr>
<tr>
<td>23</td>
<td>Tip #7: Plan for Hardware You’ll Need at the Door</td>
</tr>
<tr>
<td>28</td>
<td>Tip #8: Add People Sensing to Detect Tailgating</td>
</tr>
<tr>
<td>31</td>
<td>Tip #9: Explore Your Options for Visitor Access</td>
</tr>
<tr>
<td>34</td>
<td>Tip #10: Go Beyond Access to Create Richer Workplace Experiences</td>
</tr>
<tr>
<td>37</td>
<td>Take the Next Step</td>
</tr>
</tbody>
</table>
Introduction to Mobile Access Control
Introduction to Mobile Access Control

Until recently, the gold standard in physical security was providing each employee an access key card or fob they carried with them to open secure doors, elevators, and other access points around the building. More broadly, employees might also use those cards and fobs to access office equipment like shared printers, copiers, and vending machines. Mobile access replaces cards and fobs (and in some cases, metal keys) with an app running on the smartphone or smartwatch most employees already carry with them everywhere they go.

In the security world, convenience and security usually have an inverse relationship—that is, if something increases convenience, it usually reduces the robustness of security; and vice versa. But mobile access control is a rare exception to this common tradeoff. Whether you're using metal keys today or electronic key cards and fobs, upgrading to mobile access increases both ease of use for your people and improves the security of your workplace and buildings. It’s a win-win for employees and the company!

The most common drivers for mobile access projects are:

- Eliminating the cost and complexity of cards/fobs
- Providing a better end user experience
- Improve building safety and security
Key cards and fobs that use RFID technology have been common since the 1980s and the user experience hasn’t changed much since then. In a recent survey of office workers, end users reported frustration with needing to carry multiple cards and fobs (23.2% of respondents) and always having to remember to carry the card(s)/fob(s) around with them (45.4% of respondents).

Lost key cards represent a big cost for companies today—both buying replacement cards and also the overhead of ordering a replacement, adding it to the access control system, and getting the card to the end user. Among workers who use an access card or fob, 17.3% report that they’ve lost at least one in the last year. Since some people lose more than one card/fob, the average company loses 2.6 cards/fobs for every 10 employees every year. It takes an administrator 12.2 minutes on average to replace a lost card, adding up to a lot of work.

By contrast, people are much less likely to leave their phone at home, in their car, or at their desk. They’re also far less likely to lose their phone and need to replace it.

Most access cards and fobs also aren’t very secure. Using readily available technology that anyone can buy online today, a technology-savvy thief can scan an employee’s key card in seconds standing a few feet away and clone their credentials to a new card, giving them the same level of access. No wonder 52.2% of physical security personnel see card cloning as a serious security threat to their organization. It can be even easier for a pickpocket to get a user’s access card and walk right into the building with it.
Unlike RFID cards and fobs, mobile access credentials are not transferable. There’s no way to clone access credentials off someone’s mobile device. Typically, people notice they’ve lost their phone much sooner than when they lose a key card, and access can be remotely revoked for that device. Taking security a step further, enterprise-grade mobile access solutions provide biometric options that leverage a phone’s fingerprint or facial recognition features, making it even harder for a third party to gain access to secure areas with someone else’s phone.

Contactless payment technology has been available in smartphones for several years and Bluetooth technology has been in phones even longer, predating the iPhone by about a decade. But until now, making mobile access easy to use and secure had been challenging. Early solutions were cumbersome. They only worked if your phone was connected to Wi-Fi, or made you contort yourself or wave the phone in a very specific way to unlock a door. In short, they weren’t very user friendly, they weren’t always secure, and they weren’t very reliable either.

End users want and demand simplicity. They’ve come to expect experiences with their mobile devices to be effortless. To meet that high bar while also ensuring your building exceeds current security standards, we’ve summarized ten tips to make your mobile access project a success.

“The average company loses 2.6 cards/fobs for every 10 employees every year.”
Tip #1

Define Levels of Access Based on User Profile and Role
Define Levels of Access Based on User Profile and Role

You could give all your employees, visitors, and contractors the same access permissions. This would be very easy to manage but it wouldn’t be very secure. Visitors only need access for maybe a few hours or a few days, cleaning staff only require access for specific hours on weekdays, sales staff only need access to the office but never the server room. It’s safer to provision access based on a user’s role, the space they’re accessing, the time of day/week, and also expire some access permissions after a defined period of time.

Before you set out to configure these permissions in your mobile access software, you may need to get input from stakeholders such as IT, physical security, and leadership. First, audit all the individuals that need access and group them logically based on their role (this is a good opportunity to audit your system to ensure only current users are active). Next, map the different parts of the building and assign user groups to each area based on their need to access. Armed with this information, you’re ready to have a conversation with stakeholders about what access policies are right for your organization.
Tip #2

Balance Ease of Access with Security Needs
Balance Ease of Access with Security Needs

The most popular access modes for mobile devices include:

• Standard tap-in mode — works similar to cards, just tap the device near the reader
• Hands-free mode — works at a greater distance so you can leave a device in your pocket
• Biometric mode — requires fingerprint or facial recognition to unlock the door

Replacing access cards and fobs with smartphones and smartwatches doesn’t just give you the same door-unlocking functionality in a new package. Mobile access opens up a new world of access experiences, and you’ll need to tailor them according to your security requirements.

Hands-free mode makes it very easy for end users to unlock doors, but since it works from a few feet away you may want to limit its use to less secure areas of the building where you want to give more streamlined access, such as a door that gives access to a break room that’s already behind several layers of locked doors.
Hands-free mode may not be ideal for exterior doors and lobby turnstiles, because it’s possible for a user to inadvertently stand too close to the reader and unlock the door for someone else who’s not authorized.

On the other hand, biometric mode introduces some additional friction to the access experience because, unlike tap-in mode and hands-free mode, it requires more than the mere presence of the phone in proximity to the reader to unlock the door. With biometric mode, end users have to authenticate at the door using the fingerprint or facial recognition capabilities of their smartphone, adding an additional layer of security that prevents someone carrying another person’s device from gaining access to high-security areas.

Mobile access gives security teams a new set of options when managing security levels for employees, tenants, visitors, and contractors—you can now better balance convenience with security, instead of choosing one over the other.
Tip #3

Assess the Internet Connectivity at Your Access Points
Assess the Internet Connectivity at Your Access Points

Most older card readers don’t support mobile access, so you’ll need to upgrade them to new readers that do support mobile. Access control vendors have taken different technology approaches when designing mobile access readers, and some of them require the reader to have an internet connection and/or the user’s smartphone or wearable device to have an internet connection.

The internet connection could come from the Wi-Fi installed in the building, a cellular network, or from cables wired through the wall to the reader.

There are two main reasons readers can sometimes require internet:

1. To update the reader’s firmware
2. To authenticate the user

User devices can also require access when the user is near the door. In this case, the user presses a button in an app and the app sends the unlock request over the internet.

The controller then unlocks the door they’re standing next to. This is different from how most mobile access solutions work—where the phone directly connects to the nearby reader using Bluetooth.

If the reader and/or the user’s mobile device requires internet at the time of access, the user would not be able to unlock the door if for some reason the internet connection is lost.

There are often areas around a building where a Wi-Fi or a cellular connection isn’t available, especially...
in areas with poor reception such as parking garages and building cores that are built with concrete—e.g. stairwells, utility closets, service elevators. Of course, this problem could also happen at your front door if the Wi-Fi router needs to be reset.

Any time you have trouble with Wi-Fi access or getting a cellular signal inside the building, keep in mind that employees would not be able to unlock nearby doors if your mobile access solution requires a constant internet connection. So, before you embark on a mobile access project, it's important to assess what your internet requirements are and to test Wi-Fi and cellular reception throughout your property. Otherwise, it's best to standardize on a mobile access architecture that doesn't require internet for access or for updating readers.
Tip #4

Choose a Pricing Model That Works for You
There are several different pricing models available in the mobile access market that cover four separate components of a mobile access system:

1. **Hardware** — upgraded readers and controllers
2. **Cloud service** — needed for access policies, authenticating devices, etc.
3. **User credentials** — for each end user or device to gain access
4. **Installation** — wiring up and mounting your new access reader

### Hardware costs

Most customers buy hardware up front at the time of installation, but in some cases, you may want to roll the hardware into a subscription license fee. Pay close attention to what hardware is needed for a mobile access project. Sometimes you need to replace door access readers, and in other cases you may be required to replace the access controllers (and cabling), which tend to be far more expensive than the readers, as well. If you license the hardware with a subscription, you’re effectively leasing it similar to leasing an automobile, in which case you’d need to return the hardware once you cancel your account, but this model can be advantageous because it offers lower initial setup costs.

### Cloud service costs

Mobile access companies usually price their cloud service subscription based on the number of door readers or by the number of end users who need mobile access, or in some cases both. Landlords and others with a comparatively small number of readers and high number of end users (such as a building owner with a door reader to enter a multi-tenant property) typically find that pricing based on the number of door readers to be the most cost-effective option because they don’t pay per-user pricing. Also, companies that want to give mobile access to visitors and contractors also may prefer to not pay per-user pricing for their mobile access subscription.
Choose a Pricing Model That Works for You

**User credentials**

Finally, you may find that some vendors charge for mobile credentials using a model similar to the credential model used with plastic key cards and key fobs. If this is the case, you pay for a credential that is associated with an end user’s mobile device, despite the fact there is no physical card associated with the credential. You may not be able to transfer that credential to a new mobile device when the user upgrades the phone, requiring you to pay for a new credential. In other cases, you pay a flat rate for the number of active users, regardless of how many devices those users have. Other companies offer an unlimited number of end users, something that can make it less expensive to provide mobile access to all employees, tenants, visitors, and contractors, etc.

**Installation costs**

Depending on your existing door hardware, location of a power supply, and the materials your walls and doors are made of, installation can cost more than the reader hardware itself, but these costs are often offset over time by lower operating costs for mobile access as compared to key card and fob access. Install costs for door access readers generally range from $500 per door to over $2,000 per door. Your install costs will generally be lower if you already have electronic door hardware (see tip #7), you already have electrical power near where the reader you’re installing, and you’re installing the reader on drywall in a newer building. Your install costs tend to climb if you need to electronic door hardware, need to run a power supply through the wall or ceiling from far away, or install a reader on a brick or concrete wall.
Tip #5

Stick with Open Standard Access Control Protocols
If you already have an access control system that uses key cards or fobs, you likely have panels with access controllers in a utility or IT room.

If you’re not familiar with these systems, access controller panels connect to door readers with cables, and communicate using one of two industry standard protocols—Wiegand or OSDP. In most setups today, the controllers connect to your electronic door locks and the controller is what actually triggers the lock to unlock after the controller authenticates the credential from the access card or fob sent to the controller by the reader.

Usually, organizations will want to allow employees to continue using their existing card or fob while they make the transition to mobile access. In this case, when you upgrade your door readers to support mobile access, it’s important that you keep your existing controller because the controller is what authenticates the user’s card/fob and unlocks the door. When planning a system upgrade with new readers and existing controllers, you should plan to use Wiegand or OSDP protocols as most existing controllers use these to communicate. Depending on your situation, you may decide to update your controllers at the same time you upgrade your readers as part of a mobile access project. When deciding on a new access control system, it’s important to use the industry-standard Wiegand and OSDP protocols. Why? Because using a proprietary vendor protocol locks you in to their ecosystem and makes it harder to make modular changes to your access control system in the future without replacing everything at once, making any future upgrades more expensive and logistically challenging.
Tip #6

Consider Keeping Your Existing Access Control Software
Consider Keeping Your Existing Access Control Software

If you’re like many companies with an existing card-based access control system, you’ve likely built robust processes and workflows around your access control software. Don’t assume that in moving to mobile access you’ll be forced to scrap your existing software! With the right integration, you can continue leveraging your existing software.

If the readers you use for mobile access support the Wiegand or OSDP protocols, they’ll work with almost any existing access control system. But now you have two systems—one for provisioning and managing physical credentials for cards and fobs and another one for managing mobile access. While Wiegand and OSDP allow a reader to pass a credential to a controller and unlock a door, they don’t sync all users between the backend software that maintains credentials and the policies for who can access what and when.

To do that, you could manually transfer users from your existing access control system to your new mobile access software, but for many organizations this isn’t a one-time event. If you plan on continuing to manage users and access policies within the access software you already use today (because it’s familiar and you already have workflows associated with it), those changes won’t take effect for mobile users until you manually transfer the data. Manual syncing might only
Consider Keeping Your Existing Access Control Software

happen every week or every month depending on your resources, during which time the two systems get out of sync or you might have to login to two screens to make every change.

To get around this potential issue, you’ll want to set up a backend integration between your existing access control software and your new mobile access software, so you can continue managing everything from one system. One thing to look for when beginning a mobile access project is a pre-built integration between the mobile access software and the system you’re using today. You may be able to build a custom integration if you have the resources available (and provided the mobile access software has a complete set of APIs) but it’s a lot easier to leverage a tried and tested integration between these business-critical systems.
Tip #7

Plan for Hardware You’ll Need at the Door
Plan for Hardware You’ll Need at the Door

Mobile access requires your door to have an electronic door lock such as:

1. Electrified strike
2. Electronic mortise lock
3. Electromagnetic lock

If you don’t already have a card-based access control system today and you’re using metal keys, or if you plan to add mobile access to doors in your property that currently aren’t wired for card access, you’ll need to plan for upgrading your door lock hardware. Mobile access readers are designed to be used with a variety of electronic locks including electrified strikes, electronic mortise locks, and electromagnetic locks. Your installer will be able to help you select the right brand, size, shape, and voltage to match each door, gate, or garage door.
Plan for Hardware You’ll Need at the Door

Electrified Strike

Electrified strikes are most commonly found on commercial steel and aluminum door frames. When a controller sends an electric current to the strike, it activates the strike that unlocks the door. While you could install a strike on a wooden door frame, generally these don’t last as long because the small changes in the shape of the wood as it subtly warps and bends can bring the strike out of alignment with the door, causing the strike to stop working and requiring a potentially costly visit from a locksmith to fix it.
Plan for Hardware You’ll Need at the Door

Electronic Mortise Lock (Electric Handset)

Electronic mortise locks work well in situations strikes don’t, such as wooden door frames. When a locksmith installs an electronic mortise lock, they generally have to drill a hole all the way from the door handle to the hinge of the door to run a low voltage electric cable, and so these types of locks tend to be easier to install on hollow doors than they do on solid doors. The electric cable is fed from the door to the frame using an electrified hinge that looks just like a standard door hinge, but it hides the cable within the hinge hardware.
Plan for Hardware You’ll Need at the Door

---

Electromagnetic (Mag) Lock

Electromagnetic locks use powerful electromagnets to “lock” doors where the first two types of locks won’t work. Architects and designers like glass doors because they are seen as modern and more aesthetically pleasing than a solid wood door. Mag locks require a constant power source to stay locked, and so in addition to the lock hardware, you’ll also need to plan for a backup power supply. Building code requires you to have a way to manually open the door from the inside in case of an emergency. Electromagnetic locks require additional hardware and permitting, so if you plan to electrify these doors, consult with a professional security installer.

Finally, in addition to an electronic lock, you’ll also need to plan for a power supply for the mobile reader itself. You’ll probably be able to use the power for the door reader as you do for the electronic lock. This form of low voltage power is safer and less expensive to install because it doesn’t require the same certifications electricians need when working with higher voltage power supplies used for some lighting and electrical outlets.
Tip #8

Add People Sensing to Detect Tailgating
Add People Sensing to Detect Tailgating

One of the weakest links with physical security right now is “tailgating”, where someone follows a user who has unlocked a door. It’s a problem that’s not unique to mobile access, but one that’s not necessarily solved simply by moving from a card-based system to mobile access.

A recent survey of office workers who use cards or fobs found that 39.5% of them see people tailgating at least once a day. It’s not uncommon following an incident of theft to discover that the criminal walked right into the building following someone else.

To some extent, tailgating can be reduced by user training. Many organizations train users to swipe their card or fob on the reader each time they enter, even if someone is holding the door open for them. However, this places the responsibility for detecting tailgaters on the person holding the door for the person behind them, and in reality it’s extremely difficult to get user badge-in rates to 100%.

The best way to detect and stop tailgating is through automation. You’ll need to pair your mobile access system, which knows whether the person going through the door is authorized, with a people counter that detects when people (authorized or not) pass through the entryway. When the people counter detects someone walking through the doorway and the mobile access system does not detect a signal from their mobile device authenticating them, an alert can be generated and then an incident response workflow can be triggered.
Add People Sensing to Detect Tailgating

Sending a security guard or alerting a security team to train their cameras on an entryway only works if the system reliably detects tailgaters without generating false positives.

There are several approaches to people counters:

1. One approach projects a laser beam across the door and counts each time the beam is broken, but they tend to mistake people pushing carts as two people.

2. Newer technology uses heat sensing to detect people passing through doorways and distinguish them from other things that don’t give off heat to accurately count them.

To sum it up, look for a people counter technology with open APIs that you can use to integrate to your mobile access solution, or even better look for a pre-existing integration between people counters and mobile access systems that works out-of-the-box.
Tip #9

Explore Your Options for Visitor Access
A major headache for physical security and facility management teams alike is visitor management. An employee visiting a company office in another city may need a separate card (if, say, the two offices use two different access control systems). To solve this, you could alternatively provide guest cards that visitors can check out when they sign in at the front desk, but these are hard to keep track of. Some companies print visitor badges with QR codes.
Explore Your Options for Visitor Access

that activate lobby turnstiles and elevator dispatches, but don’t work with the rest of the building’s access points. Perhaps due to these limitations, a survey of physical security managers found that the most common way for providing guest access (47.8%) is simply having a local employee escort the visitor throughout the building.

Requiring local employees to escort visitors around the building solves the biggest concern about guest access—namely, that there’s no way to track guests in the building. However, as visitors move from meeting to meeting or space to space, a single consistent visitor escort often become unviable.

Mobile access can open up new possibilities to reimagine access for employees visiting another office, contractors working at a site, or visitors who may need time-limited access. One example is giving a temporary mobile access guest card that allows access certain areas of the building like lobby turnstiles, one floor via the elevator, the hallway with the bathrooms, and the parking garage so they can navigate limited areas without an escort.

Mobile access readers can also detect when visitors stray too far away from where they’re supposed to be and alert their hosts (and monitoring teams). As part of your mobile access project, it’s worth exploring the possibilities for a more streamlined visitor experience.
Tip #10

Go Beyond Access to Create Richer Workplace Experiences
In moving to mobile access, which relies on mobile device software instead of plastic key cards and fobs, a world of new possibilities is opened up to reimage the workplace and create responsive environments. This aligns with the movement among leading enterprises and commercial real estate companies to offer hospitality-driven experiences that meet the increased expectations of younger workers and improve the performance and productivity of their workforce and tenants.
These are just some of the possibilities enterprises and commercial real estate owners are beginning to implement alongside mobile access:

- Welcoming office visitors by name when they enter the lobby and approach the desk
- Providing real-time conference room availability based on whether they're occupied
- Automatically booking available conference rooms when employees enter them
- Logging in and starting video conference software when attendees enter the room
- Optimizing smart building resources to meet current occupant levels
- Allowing employees to log in to their computer faster without a password
- Combined physical and logical access for high security environments

Even if you don't plan to implement smart workplace solutions right now, when planning a mobile access project make sure the project is architected in a way that you can have the flexibility to accommodate these future use cases.
Proxy has a team of experienced mobile access and identity experts, many of whom are former physical security and access management practitioners, that are available to help consult you as you embark on your mobile access project. Please reach out to our team if you have any questions or challenges we can help advise on.

Don’t be a stranger, shoot us an email

hello@proxy.com
+1 (415) 521-2323
About Proxy

Proxy is on a mission to empower every person on the planet with a unique identity signal they own and control. The signal, emitted from a smartphone, allows people to securely authenticate to any device or service, similar to a universal single-sign on for the physical world. Today, large enterprises like WeWork, Dropbox, and Hines enable their employees, contractors, visitors, and tenants to use their Proxy for frictionless access through secured doors, elevators, and turnstiles, and to create personalized experiences throughout the workplace. With Proxy, users own their identity and have complete control over their privacy and personal data. Learn more at www.proxy.com and follow us on Twitter @proxy.

Copyright © 2019 Proxy, Inc. All rights reserved.