OLOID

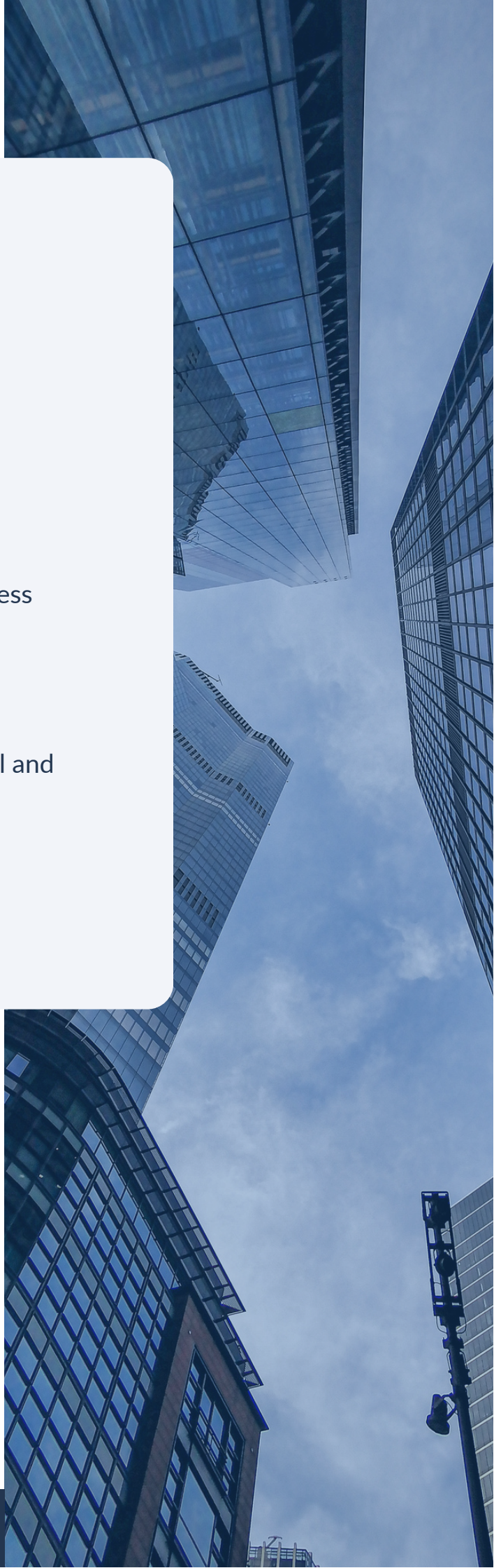
www.oloid.ai

Mobile Access Control

A Comprehensive Guide

Learn how mobile access control is transforming traditional access control systems with greater convenience and flexibility.

Table of Contents



Introduction

The world as we knew it before 2020 has changed drastically because of the COVID-19 pandemic. However, it is getting back on its feet with new tricks, techniques and technologies. Workplace access management technologies have emerged as a key component in not only preparing for any future adversity but also playing a critical role in solving various workplace access challenges. In a study conducted by Marketsandmarkets, the global identity and access management market is projected to grow from an estimated USD 13.4 billion in 2022 to USD 25.6 billion by 2027.

With contactless access solutions and hybrid work models gaining popularity, physical access management in its conventional format where most of the administrative tasks are done manually and on-premise pose certain challenges to the organizations, such as admin staff may or may not be in the office 24X7 to issue access cards to employees and visitors, or some new employees may not have been received their access badges, etc. This is in addition to the cards existing employees may have lost or forgotten during the pandemic lockdown.

As a result, mobile access control has emerged as a simple and powerful solution to tackle workplace access challenges and has now become increasingly popular. It provides contactless physical access, digital access, enterprise-grade security, cloud-based access control, remote administration and other benefits.

What is mobile access control?

Mobile access control uses smartphones, tablets and other smart wearable devices such as smartwatches that stores digital credentials of the user to unlock doors and turnstiles in office buildings and other business premises. It eliminates the need to carry RFID badges and key fobs for authentication and authorization. Mobile access is a simple and secure way to regulate access in offices, commercial buildings and other facilities. Unlike access cards and fobs, which are susceptible to getting lost, stolen, damaged and duplicated, most of us carry our mobile phones at all times. Since mobile credentials are sent directly to a user's device using the cloud, they are away from prying eyes, and well-protected on the device, making mobile access a more secure way to manage access.

Here are some interesting stats to highlight the future of mobile access:

66.6%

In a survey conducted by ASSA ABLOY, by the mid-2020s approximately two-thirds of access systems will make use of mobile phones and other smart devices.

47%

In the same survey, 47% of the respondents agreed that mobile credentials are more flexible than physical credentials

36%

36% believe that mobile credentials make it easier to upgrade employee access rights at any time

93%

93% of the U.S. population uses a smartphone, and most of them carry their phones with them all the time. Interestingly, key cards are the second most forgotten item.

15%

According to an IPVM report, the usage of Mobile Access Credentials has grown from 8.5% in 2020 to 15% in 2022.

70%

According to Gartner, Inc., by the end of 2022, 70% of organizations adopting biometric authentication for workplace access will execute it through mobile.

However, like with any upcoming technology, there are many questions about mobile access control. Let's take a look and try to answer some of them!

Most common questions about mobile access

Is mobile access secure?

Mobile access is one of the most secure access methods. Most of us carry our smartphones with us all the time and almost everywhere. We can take the security a notch up if we enable password or biometric authentication on the phones, e.g. facial recognition.

Is my data safe on mobile devices?

Most mobile access providers have a very stringent privacy policy. Some employees might have apprehension about installing the app with location services activated. While the organization must ensure the mobile access provider is compliant with local data privacy regulations, they must also explain to their employees why it's important to keep their Bluetooth and location services active. With the right steps taken, one can be assured of data privacy protection.

Will I lose my mobile credentials if I lose my phone?

In case an employee's mobile phone is lost, he/she can notify the administration immediately to restrict/revoke the employee's access credentials to protect against any unauthorized access attempts. The access credentials can be re-provisioned as soon as the employee has a new device or has found the lost device.

Is it costlier than the RFID access control systems?

The mobile access control is more cost-effective than the RFID access control systems. There is no need to issue access cards or fobs, which need to be re-issued or replaced at regular intervals due to multiple reasons. Most employees bring their own mobile devices to work. Also, since most mobile access control systems support automated administration along with remote management, it saves a lot of time and manual effort and consequently brings down the cost.
And if the mobile access solution is a retrofit one, such as OLOID, the cost gets reduced even further as one doesn't need to remove existing badge readers and access control systems.

Will the access management app affect my smartphone's performance?

Mobile access technology does not drain a smartphone's battery or performance abilities. The Mobile access systems use NFC (Near Field Communications) or BLE (Bluetooth Low Energy) technologies to communicate with badge readers and smartphones. These technologies and the access control app use very little battery, storage or processing power.

Benefits of mobile access

If anything, mobile access comes with a plethora of benefits for both employers and employees. In a 2019 study conducted by HID, 54% of businesses had either upgraded to or wanted to upgrade to a mobile access control solution over the next three years.

Let's take a look at some of the benefits:

Easy to use:

Mobile access brings the convenience of use and management. The mobile devices powered by BLE or NFC technologies communicate with the badge readers to unlock a door. Mobile access technology also integrates seamlessly with other workplace applications and software to provide a range of capabilities.

Cost-effective:

According to Ackerman security and other reports, the cost of an access control system can range from $500 to $1,200. In addition, there is a cost of $5 to $10 per keyfob or access card. The cost goes up to $2000-$8000 if one opts for a biometric access control system. In comparison, mobile access control is an affordable option. The Bluetooth or BLE-powered mobile access solution can be installed on the inside and doesn't need a premise-wide network resulting in significant cost savings. However, if you opt for retrofit mobile access solution, such as OLOID's M-Tag, you can save up to $3200 per door annually.

Secure:

Conventional access means such as access cards and key cards can be lost, stolen, damaged and cloned easily. Mobile access not only eliminates such risks, it also protects against malpractices such as buddy punching, and unauthorized access to restricted areas - both physical and digital.

Better user experience:

A user does not need to carry the badges anymore. Their mobile device communicates with the badge reader as soon as it is in the access range to unlock the door, providing a seamless, user-friendly experience.

Integration capabilities:

Mobile access control systems can integrate into HR systems and single sign-on systems to automate various operational events. When an employee is added or removed from the HR database, access rights are automatically granted or revoked.

Cloud-based remote administration:

Mobile access management is primarily cloud-based, which gives administrators the flexibility to manage access events remotely. They can grant or revoke access rights from anywhere, anytime.

Differences between mobile access control and legacy physcial access control systems

Feature	Mobile Access Control	Traditional Access Control Systems
Authentication method	Uses smartphones, tablets, and smart wearables to store digital credentials	Uses RFID badges, key fobs, or magnetic stripe cards
Security	Mobile credentials are sent directly to a user's device using the cloud and are well-protected on the device	Traditional credentials are susceptible to getting lost, stolen, or duplicated
Physical access	Offers contactless physical access	May require physical contact with a reader or card swipe
Administration	Offers remote administration and management through cloud-based systems	Typically requires on-site administration and management
Cost	May require less infrastructure and hardware costs since it utilizes existing mobile devices	May require significant infrastructure and hardware costs for readers, cards, and management systems
Scalability	Can be easily scaled up or down by adding or removing users	May require significant effort and resources to scale up or down

Technologies driving mobile access control

Mobile access control technology typically involves a combination of hardware and software components, as well as cloud-based services for credential management and access control. Here are some of the key technologies involved:

Mobile devices:

Mobile access control relies on smartphones, tablets, and other smart wearable devices to store and transmit digital credentials for authentication and authorization.

Near-field communication (NFC):

NFC is a wireless communication protocol that enables contactless data exchange between a mobile device and an NFC-enabled reader. NFC is often used for mobile access control because of its short-range communication capabilities and ability to transmit data securely.

Bluetooth Low Energy (BLE):

BLE is a wireless communication technology that uses low-power radio waves to connect devices over short distances. BLE is often used in mobile access control to enable communication between a mobile device and a reader or door lock.

Cloud-based credential management:

BLE is a wireless communication technology that uses low-power radio waves to connect devices over short distances. BLE is often used in mobile access control to enable communication between a mobile device and a reader or door lock.

Mobile access control apps:

Mobile access control apps allow users to access secure areas using their mobile devices. These apps typically provide a user-friendly interface for managing credentials, sending signals to readers, and monitoring access events.

Biometric authentication:

Some mobile access control systems use biometric authentication, such as fingerprint or facial recognition, to further enhance security and prevent unauthorized access. Biometric data is typically stored securely on the mobile device and used to authenticate the user's identity during access requests.

The COVID-19 pandemic has brought significant changes in the workplace access management technologies, and mobile access control has emerged as a key solution to tackle various workplace access challenges. As a simple and powerful solution, it provides contactless physical access, digital access, enterprise-grade security, cloud-based access control, remote administration, and other benefits. With the increasing popularity of mobile access control, statistics suggest that by the mid-2020s, approximately two-thirds of access systems will make use of mobile phones and other smart devices. Despite concerns about the security and cost of mobile access control, it is one of the most secure and cost-effective access methods. It also comes with a plethora of benefits for both employers and employees, including easy management, enhanced security, and streamlined administration.

Contact us

to know more about our products and solutions.

18007119123

info@oloid.ai

www.oloid.ai