jamf

# How to be Passwordless and Secure

## Passwords, P@sswords1, P@$$word$1234!

The password has long served as the barrier that keeps out those who shouldn't have access and let in those who should. They are the bouncer at the door of your device and data. They have stood admirably at the entrance of your devices and defended them with all the power eight minimum characters, a number, and a special character can muster.

As our digital footprint continues to boom and the device ecosystem grows, the needs of on-the-go users are expanding, which has made the value and ease of the password less and less effective. Individual users now interact with more devices and apps, more often than ever before in any given day, each presenting an opportunity for a security break should that password become compromised.

Every IT admin has seen the dreaded list of most used passwords — and it is dreaded — because nearly every interaction end users have with their devices, and the data on those devices, involves having to prove they are who they say they are.

**Top 10 most used passwords**[1]

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

1. According to Cybernews.com

**In this paper, we'll discuss:**

- Heightened security vs. ease of use
- What passwordless means
- Why organizations should care about passwordless workflows
- Jamf's answer to password woes

## Heightened security vs. ease of use

The number one security problem for organizations today? ***Stolen login credentials.*** Surprised? What about the fact that **80% of all data breaches involve stolen or weak passwords**? Even with the enforcement of stronger password policies, server breaches can expose passwords and thus, corporate and employee information. Additionally, InfoSec adversaries are becoming more sophisticated in their methodology and types of attacks. Phishing attacks, push notifications and account takeover fraud are all aimed directly at susceptible users, attempting to gain direct access to devices and vital data.

Over time, the need for heightened security led to IT requiring greater password complexity and password rotation as a solution. While these added measures helped and should be considered "best practices", they also became points of friction in the user experience. Many users simply reduced their burden by creating weaker passwords, by making note of the password on paper or digitally, and even squirreling them away below their keyboard for all to find. Those that did create and use complex passwords had their own setbacks — increased help desk tickets due to forgetting those random strings of letters, numbers and characters.

While a password reset may not be the most complex of help desk tickets to resolve, they become tedious for any IT admin hired to work on loftier IT goals than password management aid. To go a step further, having your IT team spend their precious time resolving menial tickets costs you money. **A single password reset costs companies an average of $70**. And when you add up all the time spent on these tickets, it's a shockingly large amount of money for some enterprise organizations. For the end user, forgetting a password and having to wait for it to get reset stalls work and productivity. Still, these time and monetary costs aren't always enough for passwords to get the attention from security teams or users they deserve.

The uptick in security needs to prevent attacks against companies and protect company and customer data has seen enterprise security budgets increase. Yet the breaches increase as well and the allocation of funds going toward preventing compromised password breaches isn't proportionate to the problem they pose. In fact, **less than 10% is spent on eliminating compromised credentials but is where greater than 80% of all breaches originate**. This is where passwordless workflows step in to help.

## So, what does passwordless mean?

By 2022, **Gartner predicts 60% of large and global enterprises, and 90% of mid-sized enterprises, will implement passwordless methods in more than 50% of use cases**.

Why? Because by its nature, a passwordless workflow for authenticating users eliminates the problem of weak passwords, eases users' password fatigue, and means organizations don't need to store passwords that could become exposed and compromised. In other words, it alleviates almost every pain point of physical passwords mentioned in the beginning of this paper.

To successfully introduce passwordless workflows, an organization must offer their users a way to authenticate, or prove their identity, during the sign in process to the resources, data or software they have been authorized to access and use by IT. Security and identity and access management (IAM) leaders should be familiar with authentication and authorization concepts as a crux of identity management.

One example of an authentication method is a smart card system. A smart card is a physical card, resembling a credit card that houses cryptographic keys tied directly to a user and is used as a secure method to authenticate. The problem is, these systems are time consuming to implement, very expensive and an additional piece of hardware an end user must manage. Unless your organization is a high-risk use case, the cost and potential of end users losing or breaking the smart card often outweighs the potential threat making that level of security unnecessarily excessive.

**What is multi-factor authentication (MFA)?**

Multi-factor Authentication (MFA) is an authentication process that requires the user to provide two or more verification factors to gain access to a resource. This could be a PIN on a user's phone, **Face ID**, fingerprint verification, or a few other options.

The most common example people are familiar with when it comes to passwordless is the use of biometrics. Face ID and Touch ID are examples that every Apple user will know. Biometrics allows a user to authenticate without inputting a password, or requiring a knowledge-based secret or challenge question which can be stolen or guessed. Your face is your face, and your thumb is your thumb — hard to steal. Add in a rotating PIN requirement and it's double the security effectiveness.

We've talked about how passwords are no longer the most secure way for organizations to allow users to access their devices and resources, nor are they the best experience for workers that have to enter passwords many times a day. And with the changing landscape to remote and hybrid work environments, organizations now must consider better security measures that take into account the end user experience. Let's look at how digital transformation is driving the need for organizations to implement passwordless workflows.

**What is passwordless authentication?**

Passwordless authentication is an authentication method in which a user can log in to a computer system without the entering a password or any other knowledge-based secret

**What is certificate-based authentication?**

Certificate-based authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc.

## Why should organizations care about passwordless?

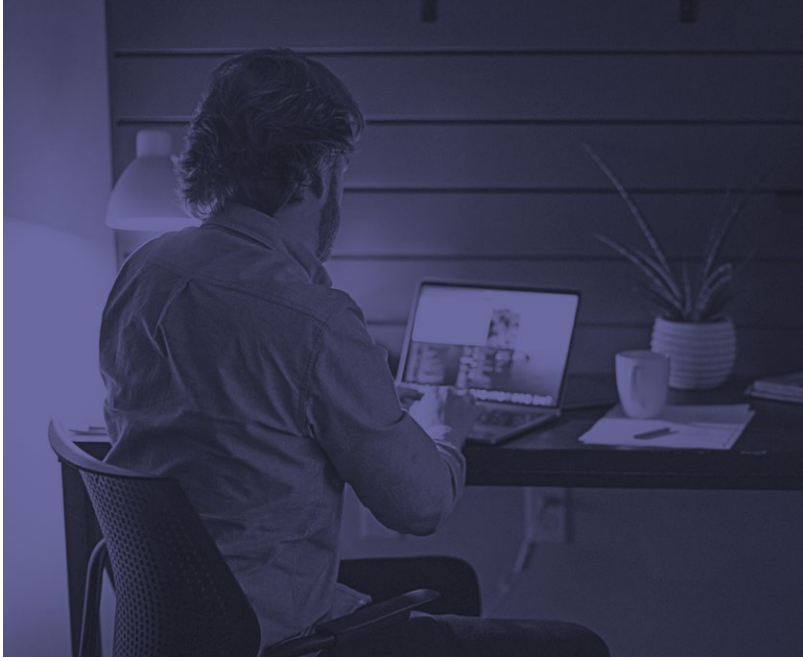
If the security vulnerabilities associated with passwords briefly outlined in the opening of this paper wasn't enough to convince you to join the movement toward passwordless workflows, let's dive into digital transformation and the effect on passwords a little bit deeper.

### Remote workers

The shift to remote and hybrid work has accelerated the urgency for passwordless authentication as extra emphasis is being put on providing an excellent user experience and remote security. A large component of that is end users logging in remotely. Users can go anywhere – home, the office, a coffee shop, the park – to access their devices and resources which is flexible and convenient but also comes with the added risk of being outside the corporate perimeter. Users can be on unsecured networks which pokes holes in the security layer and makes attacks more likely. One easy way to reduce threat risks is a clean and reliable passwordless workflow to access everything a user needs. No more entering passwords to steal and less help desk tickets – security meets eliminating password fatigue.

### Work is in the cloud

Cloud computing has changed the world, and embracing it is undoubtedly a key component in most modern IT infrastructure. Because the on-premises corporate perimeter is falling and organizations are shifting to the cloud, their identity management strategy should follow suit. Apps and resources are everywhere in the cloud. IT needs to find a secure way to give their workers access and keep them productive and passwordless can help provide secure and seamless access in the cloud and all of the apps in it.



### Lowering costs of password management

According to **World Economic Forum**, employees around the world spend an average of 11 hours each year entering or resetting passwords. Multiply that by the number of employees you have within your organization and it's a massive chunk of time wasted on password management. While implementing a new solution has a cost, it pales in comparison to the waste from hours of tedious password resets and an unfocused workforce.

### Promotes increased productivity

Less time spent managing passwords leads to an employee and workforce spending more time on their tasks, with uninhibited access to the resources they are authorized to use, and a more productive workday. Not only are costs lowered with less password management, and security-related headaches associated with the risks of passwords, but improved employee productivity also leads to increased revenues.

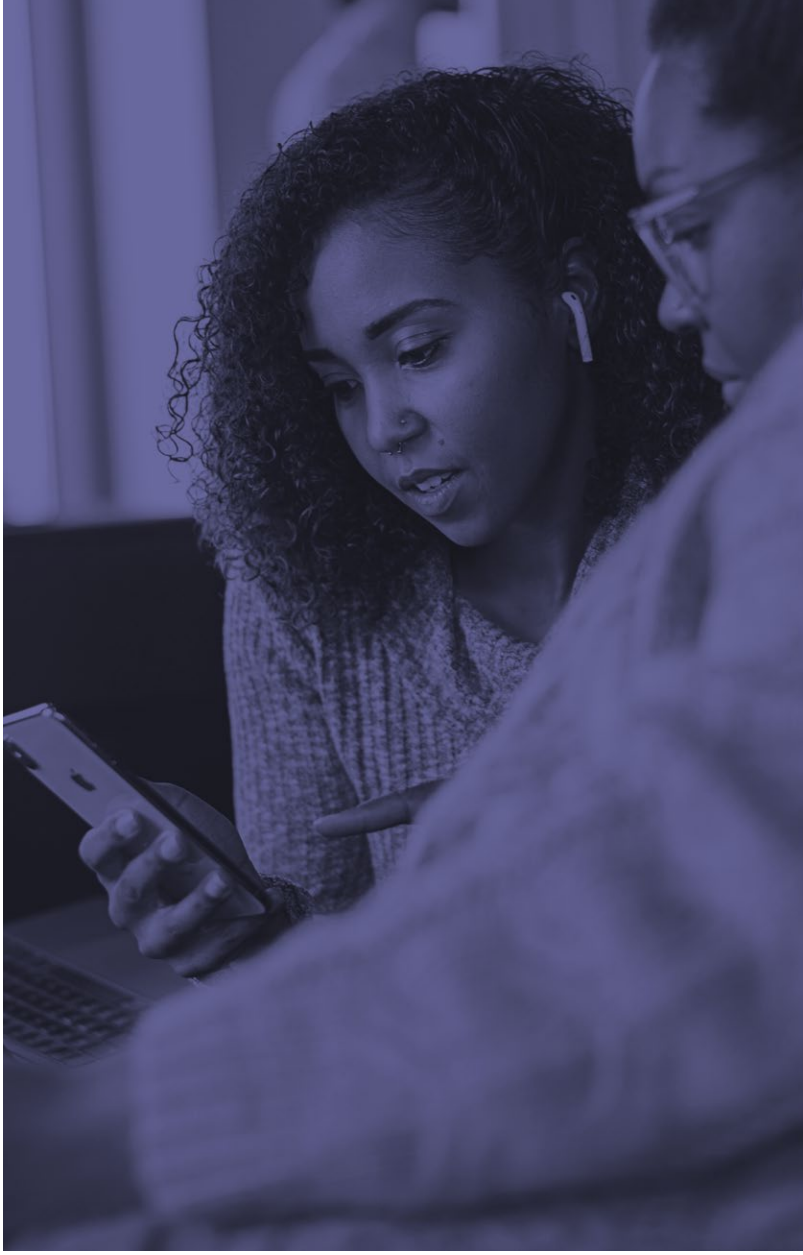
These are just a few additional examples of how something like passwords, an aspect that many have spent years overlooking or accepting as "good enough" can be fine-tuned, and improved to aid in the company's overall security strategy, bottom line and financial wellbeing. It's not hard to see why many view passwordless workflows as a key component to their digital transformation plans.

## Jamf's Answer to Password Woes: Jamf Unlock

Instead of relying on unmanaged, costly hardware, like smart cards, Jamf Unlock — a built-in feature of Jamf Connect — provides a passwordless workflow on the device users always have — their iPhone — to securely unlock their Mac and provide a more secure log in and authentication process with a seamless end user experience. The Jamf Unlock workflow satisfies Mac system authentication needs with an authenticator running on a user's iOS device instead of password entry on their Mac.

1. Users open the Jamf Unlock iOS app on their iPhone and sign in the first time with their cloud-based identity credentials.
2. Users then pair their iPhone with their Mac via a QR code.
3. On the Mac, users will enter their local password when prompted to allow the device pairing.
4. Once pairing is complete, the user can start using the app to securely unlock their Mac with method required by IT: biometrics with or without a rotating PIN.

Jamf Unlock leverages Apple's Multipeer Connectivity, CryptoTokenKit and Core Bluetooth frameworks to perform wireless certificate-based authentication between a user's mobile device and their Mac.



Passwordless workflows are undoubtedly going to evolve but should only be one component of a modern identity and security strategy. Jamf Unlock is a component of Jamf Connect for Mac which gives organizations just-in-time account provisioning, **identity management** capabilities and a single cloud identity to access the Mac and resources. By integrating with a cloud identity provider, Jamf Connect allows IT to remotely manage the data attached to each end user's identity and the software and resources authorized to their account. This not only increases security but streamlines account provisioning and enables users to open their new Mac, power it on and gain secure access to everything from the word 'go'.

Further your security and go one step further with Private Access: Unlock is only one part of securing data and resources. Jamf Private Access – a true Zero Trust Network Access platform – ensures that after a user authenticates into their device, business connections are secure.

**Learn more about Private Access**

## Become more secure today

It goes without saying that the work environment is constantly evolving, but that evolution comes with challenges and opportunities. Advancements like mobile and remote workforces may open the door for attackers and hackers to seek opportunities for nefarious actions, but they are also resulting in creative workflows and solutions for IT Admins, InfoSec and end users.

While InfoSec may always have a “security first” mindset, they will constantly be challenged to balance that priority with the wants and needs of their end users who are far more focused on their own experience interacting with their devices daily. End users don’t want laborious workflows or security measures that slow them down immensely and while most users will understand the importance of data security, that understanding only goes so far.

Jamf Unlock’s ease of integration with existing workflows benefits the end user and InfoSec/IT teams in this regard. And while nefarious actors will always try to breach your data, implementing a passwordless workflow using Jamf Unlock and Jamf Connect, is an easy win when it comes to providing an extra layer of security with a great end user experience that mitigates the risk imposters may carry.

Implementing a passwordless environment should be well thought-out process for any organization, as most security plans are, but it’s an enhancement that moves any organization forward and provides an opportunity to grow. The focus should be on streamlining your process and saving on overhead costs, not onboarding unnecessary hardware and adding further cost. That’s exactly what Jamf Unlock proves and precisely why it’s the best method for securing your organization’s Mac.

**Contact us**, or contact your Apple reseller, to put Jamf Connect’s identity management and passwordless capabilities to work in your organization.