



Reasons for adopting Passwordless authentication

Deploy passwordless strong authentication for all access points with seamless user experience:

- PC
- Tablets
- Mobile web access
- Mobile apps

Strong authentication is meant to secure access to all your digital assets, not just one channel.

Most of Passwordless authentication solutions are focused on desktop access. Other access channels will then use other methods or solutions making it cumbersome to end users.

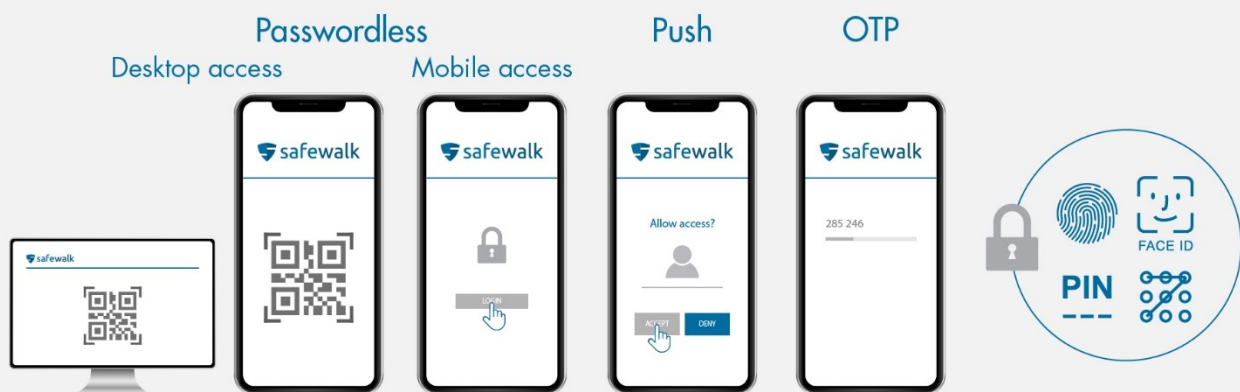
The challenge is to secure Mobile web access apps or native Mobile apps (home developed or third party apps such as SAP Fiori) with a single solution and user experience together with desktop access.

Then how to improve security of all access points, while streamlining infrastructure and maximizing simplicity of use for end users?

That's where the *Safewalk Fast Auth* passwordless solution shines - as it provides:

- A unique platform to easily deploy multi-factor authentication on all channels
- Strong authentication to access applications from any device minimizing user interactions
- A secure and streamlined on boarding process to install and register Fast Auth mobile
- A seamless, frustration free user experience
- All kinds of mobile apps can be secured with MFA without any development
- Fast Auth also provides a wide range of other methods that can be deployed from the same platform to meet the needs of other specific use cases where the passwordless method is less relevant

Fast auth mobile app is **seamless to register** and offer different authentication methods that can adapted for each user/group profile and use cases:





Why is passwordless strong authentication better than other methods?

1. Easy deployment of strong authentication for desktop & mobile access

- *Safewalk Fast Auth* mobile passwordless strong authentication method can be easily deployed in most frequent use cases, such as access to applications or web portals from a desktop or smartphone. It enables access to all types of native or web access mobile apps
- It provides secure access to consumer portals, with a large number of users, by providing the easiest authentication method in order to significantly reduce help desk involvement.

2. Streamlined user experience

- Users no longer have to devise and remember complex passwords or type them each time they log on
- They no longer have to renew or change passwords
- Access is straight forward, utilizing biometric recognition or pattern entry, providing a seamless and intuitive user experience
- When accessing portals or mobile apps from a smartphone, strong authentication is done with one or two user interactions

3. Improved security

With the many credentials a typical user has to remember today, remembering usernames and/or passwords can be problematic and frustrating. This inevitably leads to passwords being reused and eventually security being compromised.

Obviously, users' passwords are vulnerable to many traditional attack vectors. But, with passwordless authentication, the users' authentication data is not stored within the system, as a password would be. This gives a Passwordless solution a significant security advantage, as it eliminates the existence of attack vectors that are inherent to traditional passwords.

4. IT cost reduction

- A passwordless method greatly reduces the associated costs of password management operations such as storage and protection.
- Help desks will no longer be clogged up with endless users' demands for changing or resetting forgotten passwords - this is particularly helpful for strong authentication of high user volumes.