ENTERPRISE AUTHENTICATION WITH PAYCONFIRM FAM

GENERAL OVERVIEW

Required to memorize different passwords to access corporate resources, employees tend to simplify, duplicate, and write them down. All of this leads to password leaks and unauthorized access to company resources. This is why the implementation of Multi-factor Authentication (MFA) and Single Sign-on (SSO) are one of the top trends in enterprise security.

PayConfirm FAM provides an effective solution to employee problems regarding authentication in enterprise infrastructure. This is done by replacing outdated and insecure authentication methods, such as static passwords, SMS OTPs (one-time passwords), expensive USB/MAC-tokens, and smartcards. It doesn't matter whether your employees work from home or not, how deep their technical knowledge is, and so on. With PayConfirm FAM, your employees can connect to the majority of applications and in-house company systems
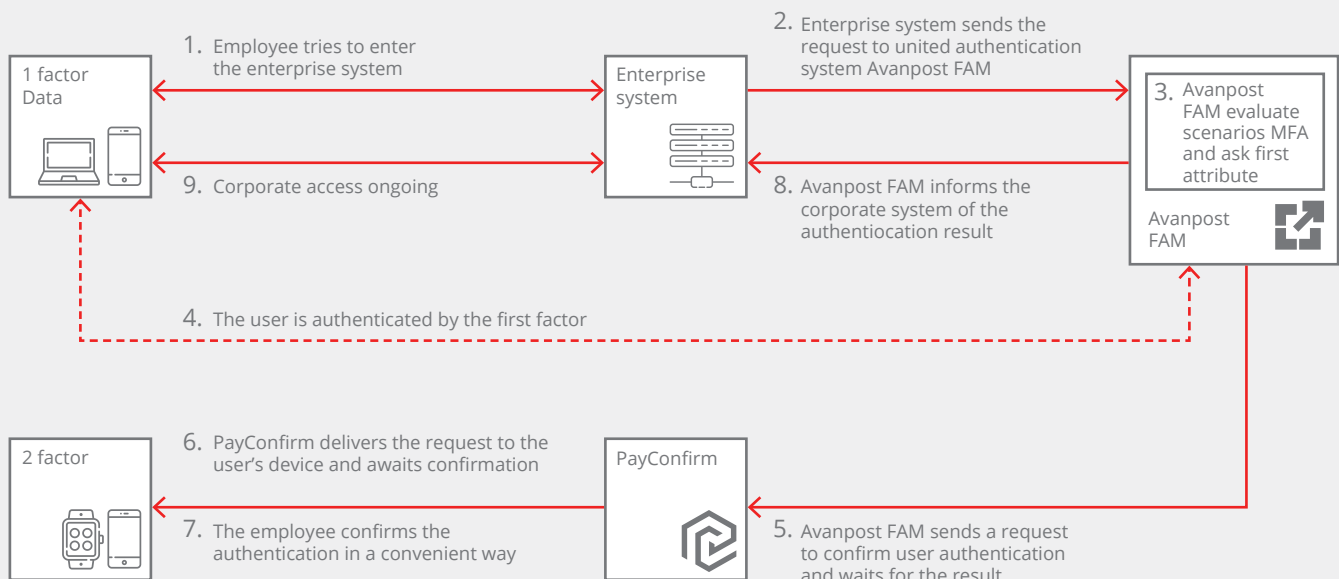
with a single tap on a smartphone screen.

The solution accommodates the technology of SSO with MFA for all types of corporate systems: mobile applications, APIs and micro services (OAuth), modern/legacy desktop and web applications (SAML, OIDC, ESSO, Reverse Proxy), VPN and VDI (RADIUS), Windows environment (Credential Provider), and Linux (PAM).

With PayConfirm FAM there is no need to authenticate in each corporate resource separately because an SSO allows authentication through one system. Unlike many other solutions, PayConfirm FAM makes it possible to simplify the authentication process itself–it does not require any hardware-based or OTP-based solution– log in operations can be confirmed with a tap on a smartphone screen.

HOW IT WORKS

In a basic scenario, while trying to access a corporate information system, the employee is requested to use passwords as the first factor (this can be configured). As soon as the first factor is passed, the user receives an authentication request to their mobile device as a second factor. The employee can authenticate into the system after a successful second-factor confirmation.

PayConfirm FAM also protects from loss of

credentials. If credentials are compromised and someone tries to use them to log in to the system, the employee will receive a notification on their mobile device concerning a login attempt and a request to confirm that operation. The only thing the employee will need to do is refuse this operation on their mobile device, while (in parallel) an attempt to receive unauthorized access will be recorded in the security event log.

Thus, with PayConfirm FAM there is no need for a user to waste time retyping random digits sent via SMS, or manually enter a code generated in an OTP generator, or even hold onto any USB-tokens or smartcards. To confirm the request for authentication, you need only two taps on a smartphone or even a smartwatch screen. Your smartphone is your token.

1 factor
Data

1. Employee tries to enter the enterprise system

Enterprise system

2. Enterprise system sends the request to united authentication system Avanpost FAM

3. Avanpost FAM evaluate scenarios MFA and ask first attribute

Avanpost FAM

9. Corporate access ongoing

8. Avanpost FAM informs the corporate system of the authentiocation result

4. The user is authenticated by the first factor

2 factor

6. PayConfirm delivers the request to the user's device and awaits confirmation

PayConfirm

7. The employee confirms the authentication in a convenient way

5. Avanpost FAM sends a request to confirm user authentication and waits for the result

USER EXPERIENCE

For employees:

- SSO for faster and easier access

- No need to memorize multiple logins and passwords

- Access from anywhere: it is not necessary to carry a USB-token, smartcard or wait for an SMS

For the IT department

- Cost reduction for administration of user credentials

- Reduced costs and management of corporate identifiers through usage of personal mobile devices

- No need to spend money for storage and logistics on hardware tokens, OTP generators, scratch-cards, etc.

- Seamless operation—stability during roaming or when you are out of a mobile operator's coverage

For the Security department

- Reducing risks for compromised passwords and interception of codes delivered via SMS messages and/or push notifications

- Two independent communication channels are used to activate the PayConfirm app in a user's smartphone

- Increased security by adding a second authentication factor

- A universal control point for authentication events

ABOUT US

Airome Technologies is a Singapore-based developer of cybersecurity solutions for digital banking and e-document management systems. The company provides a secure client-server software to confirm or digitally sign any type of operations, including bank transactions or e-documents, on a mobile device. Our solution lowers the risk of unauthorized transactions caused by man-in-the- middle, phishing, or social engineering attacks.

Our mission is to enable our customers to provide user-friendly, secure and cost-effective digital services.

GET IN TOUCH WITH US

airome.tech
info@airome.tech