SecurAccess v8.1

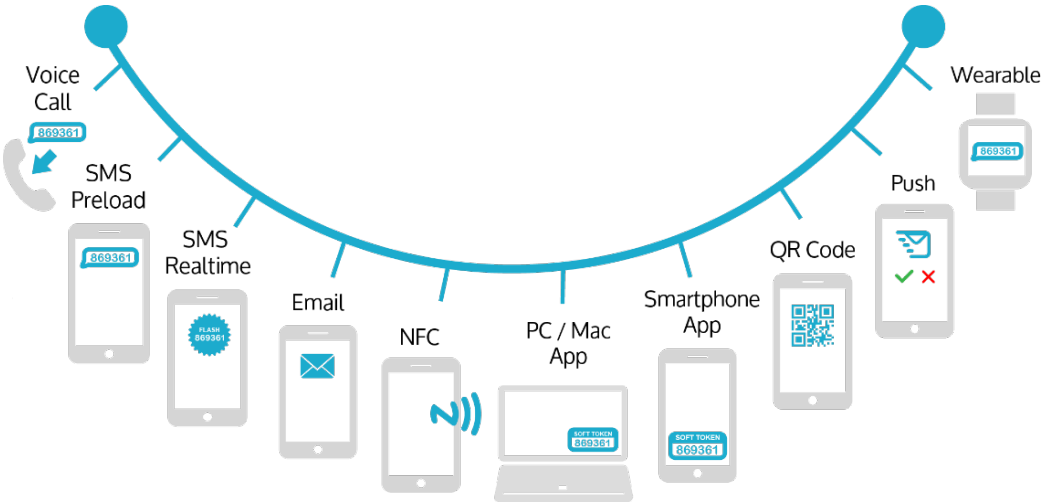
Mobile device-based tokenless® Two-Factor Authentication for VPN, SSL, Remote Desktop, Wi-Fi, Web and Laptop Encryption.

SecurAccess allows users to leverage their existing personal devices to authenticate. Users with multiple devices are free to move their identity between devices as often as they like.

In addition to patented Tokenless® methods such as SMS, voice and soft apps, SecurEnvoy consistently develop, ready for tomorrows technology. Embracing mobile advancements SecurAccess supports NFC 'tap and go', biometric finger print logon, wearables and QR scanning; all of the latest technologies of tomorrow, available today!

Similar to ApplePay and SamsungPay, SecurEnvoy have patented the Authentication equivalent of the 'tap and go' using NFC and Bluetooth technologies embracing phablets, mobiles and wearables; **Two Factor Authentication is now quicker and easier than the traditional password!**

Authentication Options



Features

Passwords alone are not sufficient to protect your organization's data from the three billion users online. Two-Factor Authentication is required to provide robust security and, by leveraging users' existing mobile devices, can be deployed seamlessly and cost-effectively.

SecurAccess can be implemented as an on-premise software solution or hosted as part of a managed service or in the Cloud. The simple 2FA logon experience leverages the user's device of choice as the authenticator, delivering a solution at a fraction of the cost of traditional alternatives. With SecurEnvoy; any mobile device can be used as the authenticator.

SecurAccess can be deployed rapidly and scaled to 25 users per second (1,500 per minute). Users can be automatically deployed via LDAP group membership, utilizing existing infrastructure, costs and deployment is simple.

SecurAccess utilizes your current LDAP server as its database and integrates seamlessly with Microsoft Active Directory, Novel eDirectory, SunDirectory Server and Open LDAP without the need for additional databases or hardware; delivering multiple server support across multiple domains. It's also deployed rapidly and can scale to 25 new users per second (1,500 per minute).

SecurAccess is available at a fixed annual cost, payable on a per-user basis, with no hidden extras.

Benefits

- Re-utilize existing LDAP User Repository – no requirement for additional databases
- Users do not need to remember additional passwords as they can use their existing LDAP password
- Doesn't require an additional PIN, unlike other two-authentication systems (PIN support available if required)
- Utilize existing devices - users do not need to carry an additional authentication device; use what's in your pocket!
- No resynchronization or PIN resets, reducing management time
- Deploy to thousands of users in minutes, saving time and money

Putting the user in control

We believe users should be able to choose any personal device to be their authentication token, whether it's their mobile phone, tablet, laptop or even their desk phone. Users should be able to seamlessly move their single identity between these devices without leaving their identity behind.

A world without hardware tokens

Hardware tokens, first seen over 30 years ago, are preventing the mass uptake of two factor authentication as they are expensive to deploy and run and do not scale easily. Users cannot be expected to carry a different hardware token for every business they log on to – office, bank etc. Clearly, using an existing personal device such as a mobile phone is the answer.

As the original inventors of tokenless authentication, our goal is to continue to design innovative solutions that take advantage of users' personal devices and resolve issues that have prevented adoption such as SMS delays, no phone signal or synchronization problems.

Elegantly Simple

We believe the logon process should be as simple as possible; that thousands of users can be deployed at the click of a button whilst maintaining strong security. Our designs leverage existing infrastructure, such as Active Directory as the central database, to create simple, elegant solutions.