

SecurAccess MFA

Introduction

Passwords alone aren't strong enough to protect your business-critical data and Multi-factor authentication provides the strength of security in leveraging the process of verifying that a person is who they claim to be, with something the user knows (Password/PIN), something they have (Software/Hardware Token) and in some instances, something they are (Biometric/Facial Recognition).

Multi-factor authentication is best practice for securing user data and is seen as a need for the enterprise today, but increasing security does not need to be at the sacrifice of user experience.

SecurAccess from SecurEnvoy delivers a seamless, cost effective solution for increased security utilising Multi-Factor authentication technology.

Security that puts you in control

Cryptographic keys, called seed records are inherent in the communication of an MFA solution, commonly generated and distributed by a server in the enterprise or cloud when issuing one-time passwords (OTP's) to clients.

SecurEnvoy's SecurAccess solution uniquely splits the keys with one part of the seed record created from a finger print of the user's device (mobile/desktop) and stored locally on the device and the other part of the seed record is created using FIPS 140-2¹ standards and stored AES 256-bit² securely within the enterprise directory services.

MFA security is most powerful when confident the split seed record is in your control, stored on your server and not known to any 3rd party.

Deployment methods

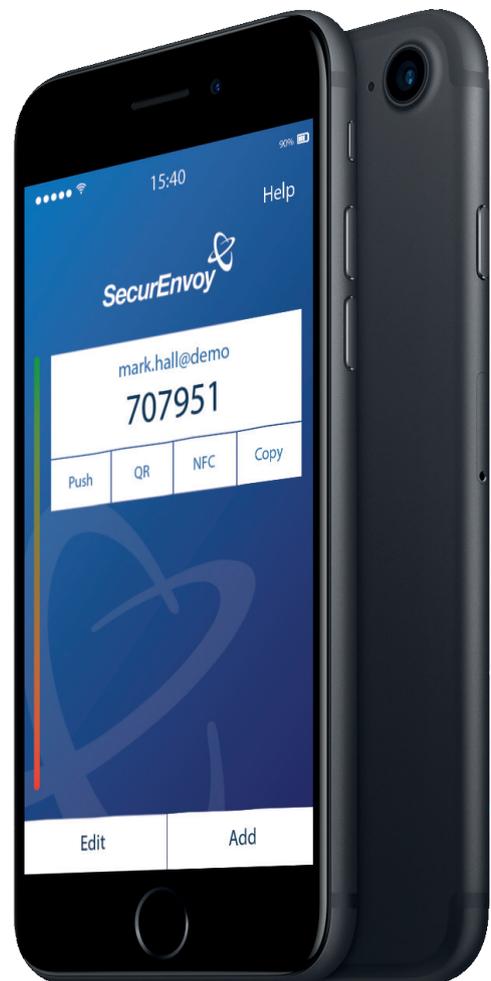
SecurAccess offers deployment options to suit any business, with an On-Premise or Private Cloud solution in either independent or industry recognised IaaS environments like Amazon AWS and Azure.

Scalability and High availability

SecurEnvoy's MFA solution integrates seamlessly with Microsoft's Active Directory, reutilising the enterprises existing authentication database infrastructure, avoiding the need to re-architect, deploy, backup and manage a secondary user database.

Managed via a single server, SecurAccess is able to make use of a mixed LDAP environment (includes AD LDS)³, consisting of multiple authentication domains across distributed sites that will have been designed with scalability and high availability in mind when first implemented.

With limited demands on the server, SecurAccess deployments are focused primarily at delivering a resilient and distributed server architecture with seamless replication of configuration data.



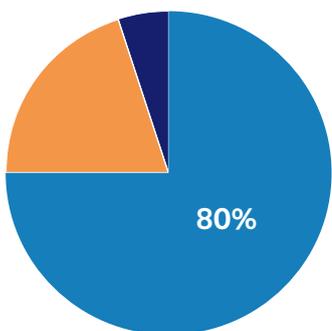
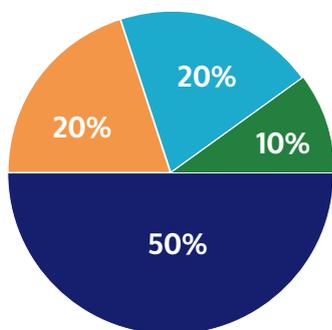
Management and Reporting

The challenge of deploying any MFA solution to a user base is the method in which users are notified and enrolled simply, timely and as painless to the user as possible.

Applying SecurEnvoy's seamless integration into the Enterprise LDAP environment, SecurAccess utilises "Automatic Group Deployment" to monitor selected LDAP groups for any new or removed users, issuing an enrolment invite via the chosen method i.e. SMS or Email or placing user into an unmanaged state when removed from LDAP environment.

Examples of Management Reports

Authentication Type



User Status



DID YOU KNOW...

63% of confirmed data breaches involved weak, default or stolen passwords.



Source: DBIR (Data Breach Investigation Report) 2017.

Integration

SecurAccess supports various interfaces to support countless SaaS or on-premise applications or network connectivity that require securing.

- RADIUS with individual configuration for each client allows integration for all major SSL/IPSEC based security appliances.
- Windows Server Agent offers the ability to secure any IIS hosted websites (e.g. OWA, SharePoint or customer web application).
- Support for ADFS in delivering MFA authentication to public SaaS or SAML authentication based applications.
- Windows Logon Agent extends MFA authentication to domain joined laptops in an online or offline state.
- Compatibility with over 30 Internet based SMS gateway providers or via Wavecom or Siemens SMS modems.

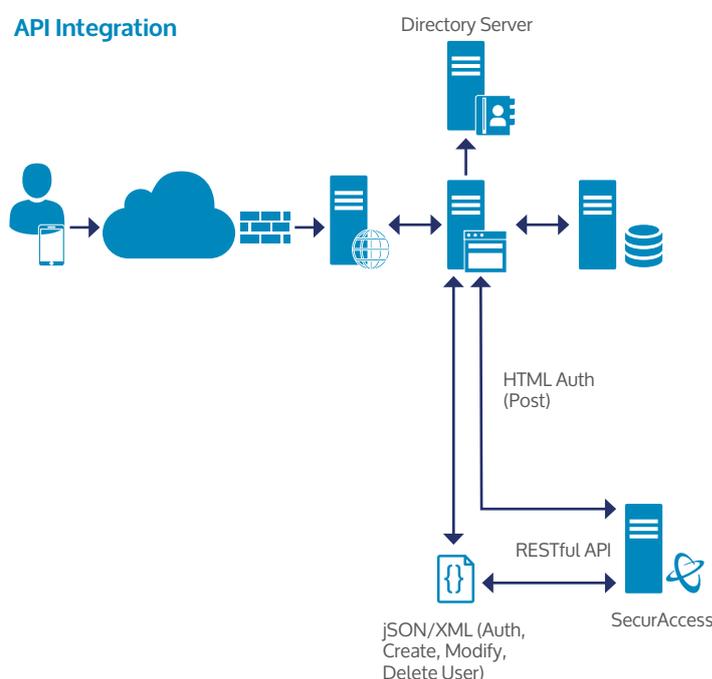
If a legacy password or token based MFA environment is in need of replacing, SecurEnvoy have a migration solution that offers parallel running, whilst users can be migrated across to a tokenless solution.

RESTful API

SecurEnvoy's Open APIs allow software developers direct access to information and configuration controls of the SecurAccess environment.

Built using the Representational State Transfer (REST) framework, SecurEnvoy's Open APIs enable you to automate the creation and modification of users, including the authentication via HTTP web call.

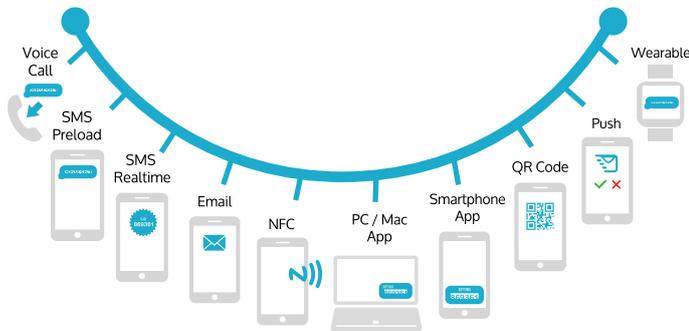
API Integration



Authentication Methods

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 on obsolete technology.



SecurEnvoy's various authentication methods allow for a comprehensive fulfillment of different user's requirements, including selection and control via brandable self-enrollment portal.

- **SoftToken App** for all smartphone or wearable platforms allows for online push notification or offline availability of One Time Passwords (OTP).
- **NFC** is the technology of choice for mobile payments. SecurEnvoy's innovation in published web applications and NFC push provides a new and simple way to authenticate.
- **SMS Preload and Realtime** schemes conveniently allow secure and reliable login independent of smartphone availability or network coverage.⁴
- **Windows XP through to Windows 10 PC and Mac support**, allows for second factor authentication via desktop.

⁴Why Preload SMS?

The key to success when utilising SMS passcode delivery is to resolve intermittent network coverage and SMS delivery delays. SecurAccess is essentially designed to resolve these issues utilising preloaded passcodes, sending the next passcode following successful authentication.

yubico

Yubico is an open online identity protection solution and offers the YubiKey®, a unique driverless USB and NFC one-time hardware authentication token that does not require pre-registration before sending out to the user, drastically reducing admin overhead from deployment, as is common with alternative OTP hardware tokens.

SecurAccess delivers support for the YubiKey, when it is not possible to use soft token authentication methods via PC/MAC or mobile devices.



Additional SecurEnvoy Solutions

- **SecurPassword** - With the growing reliance on IT, the number and complexity of passwords per user becomes a serious overhead. Typically, when the password has to be changed, your IT helpdesk is overwhelmed with confused users, who may have locked themselves out of the network. SecurPassword delivers a new approach to password security. [Click here for datasheet](#)
- **SecurMail** - Sending and receiving encrypted emails is not an easy or simple experience. Businesses rely on email with an increasing amount of sensitive data sent across their networks. SecurMail does not suffer from the traditional overheads of deployment and encryption management; providing confidence that your business communications are secure at all times. [Click here for datasheet](#)

For more information about SecurEnvoy's products and solutions, please visit; [SecurEnvoy.com](https://www.securenvoy.com). If you would like to trial SecurAccess, please [click here](#).

¹ FIPS 140-2 - Federal Information Processing Standard (FIPS) 140, is a generic term that refers to code, in software or firmware, that performs one or more security functions. The Standard sets requirements for cryptographic modules to be used in sensitive but non-classified government systems.

² AES - Advanced Encryption Standard (AES) - Encryption using a key length of 128, 192 or 256 bits.

³ AD LDS - Active Directory Lightweight Directory Services is a Lightweight Directory Access Protocol (LDAP) directory service designed for use where a user does not have a full Microsoft Domain Controller infrastructure.

E: sales@securenvoy.com

W: www.securenvoy.com

Securenvoy 
A Shearwater Group plc Company