SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com
www.securenvoy.com/partner/crm

Introducing SecurAccess

An easy to use, easy to implement, cost effective solution for multi-factor authentication (MFA)

Over 1000 Companies Trust SecurEnvoy Globally

Any user. Any device. Anywhere.

More Control. More Options. More Secur.

Version 2.0 – 19/04/18

Introducing Multi-Factor Authentication

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

Passwords alone are not strong enough to protect your business' critical data. Multi-factor authentication (MFA) 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 or need to create headaches for IT management

Deployment options to meet your business needs

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, as well as our own vendor cloud hosted alternative.

On Premise + **Hosted** + **Cloud** + **Hybrid**

DID YOU KNOW...

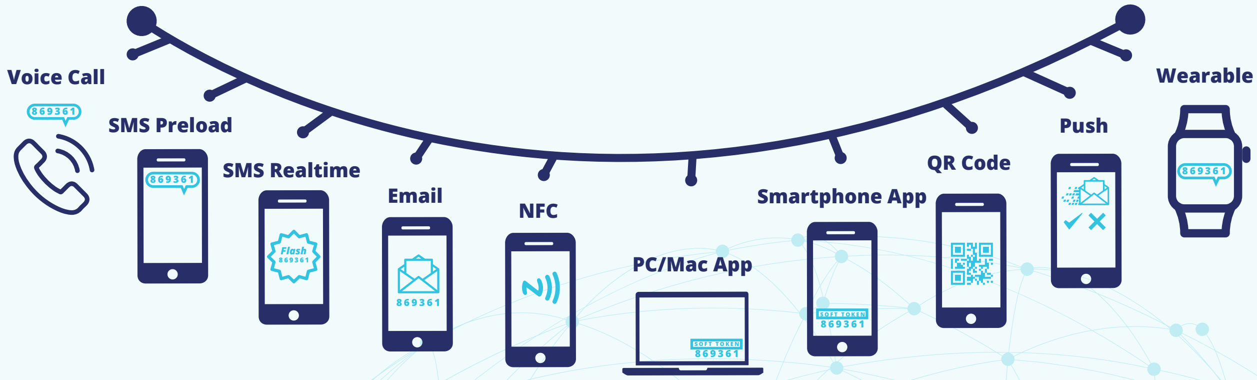
63% of confirmed data breaches
involved weak, default or stolen passwords

Source: DBIR (Data Breach Investigation Report) 2017.

Flexible authentication options with no Footprint

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 can seamlessly move their identity between devices without leaving their footprint behind.



SecurEnvoy's various out of band (OOB) authentication methods deliver user flexibility, including selection and control via a brandable self-enrollment portal.

SoftToken App for all smartphone and wearable platforms allows for online push notification or offline availability of One Time Passwords (OTP). QR codes are also supported as an alternative.

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 text conveniently allow secure and reliable login independent of smartphone availability or network coverage.*

Windows XP through to Windows 10 PC and Mac support, allows for second factor authentication via desktop.

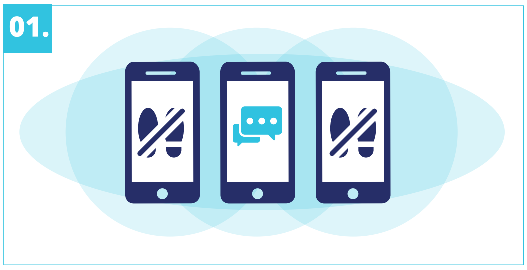
Wearable's are supported natively from the device, allowing authentication from any device carried or worn!

*

PreLoad SMS?

The key to success when utilising SMS passcode delivery is to resolve intermittent network coverage and SMS delivery dealys. SecurAccess is essentially designed to resolve these issues utilising preloaded

Solution Highlights



01. Zero footprint with SMS

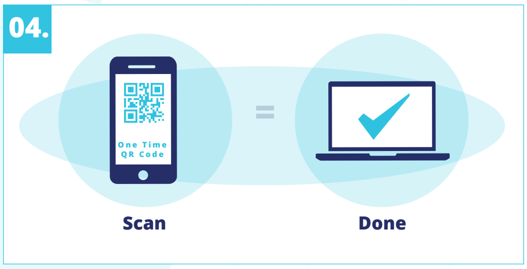
No software required on the device, provides easy end user deployment, 100,000 users provisioned in under 60 minutes. Managing SMS delay and loss of signal is absolutely key to a business grade service. SecurEnvoy patented Pre-Load provides true end user convenience.

02. Apps with lifecycle management

Users that can install apps have the added benefit of continuing to work whilst offline for indefinite periods. They can self-enroll with a simple onboarding process that is boot strapped via an SMS or Email one time code and they can seamlessly move their single identity between these devices without leaving their identity behind on obsolete technology.

03. Most secure with split keys

Our SMS codes are Fips140-2 random numbers with no keys or seeds required and our apps use split keys where the second part is the device's unique characteristics. Only part of a key is ever stored on the device thus malware cannot copy a key that isn't present and cannot call external API's as none are available. No customer sensitive data or keys are ever stored by SecurEnvoy.

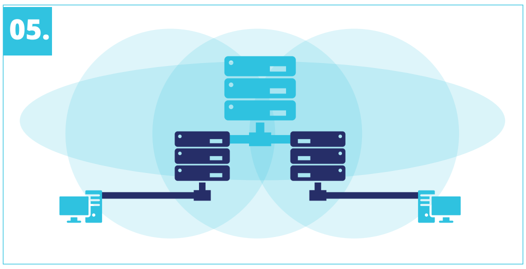


04. Easy to authenticate

You don't need a PIN, you can reuse your existing Microsoft or other application password. SMS users get their new passcode inserted in their existing messages, so they don't need to delete old ones. App users can take advantage of One Swipe, a simple scan of a onetime QR Code and you're in, no need to enter your userID, password or passcode.

Solution Highlights Contd.

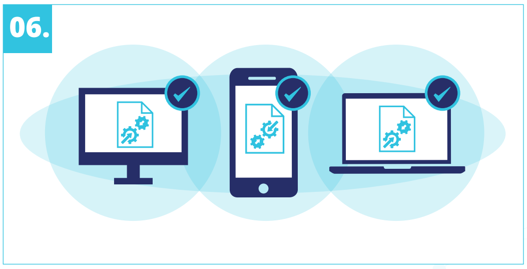
05.



05. Leverage existing user stores

Harness the power and scalability of Active Directory (AD) or other LDAP based servers as the core database. All replication is already performed by your existing infrastructure. Deployment is as simple as adding a user to an existing AD group. No Schema change is required as we use existing attributes such as Telex Numbers. Unlimited multiple domains can be configured.

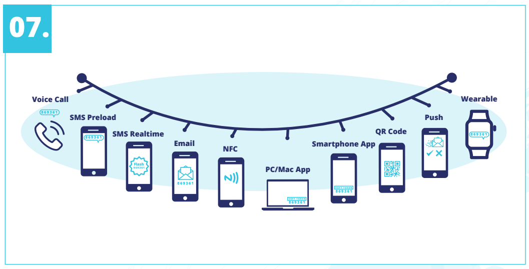
06.



06. Integrate with leading technology

We provide simple to follow integration guides for VPNs, cloud apps, on-premise apps and more to allow you to quickly and easily set up your security solutions.

07.



07. SecurEnvoy: Freedom of Choice – Freedom from Fear

SecurEnvoy's core product SecurAccess wrote the book on tokenless security for small, medium and enterprise organisations across every vertical. As is becoming increasingly clear, unauthorised access to desktops, web portals, admin consoles, remote users and internal assets are one of the most glaring holes in cybersecurity and the lowest hanging fruit for hackers. SecurAccess should be considered a must-have technology for any project or deployment that needs competitive multi-factor authentication.

08.

08. End User License Agreement (EULA) and EULA Updates

All EULA terms and conditions apply to every generated license. The EULAs are provided at the point of delivering the service and activated at the point of receiving such licenses. (SecurEnvoy may update EULA terms at any time).

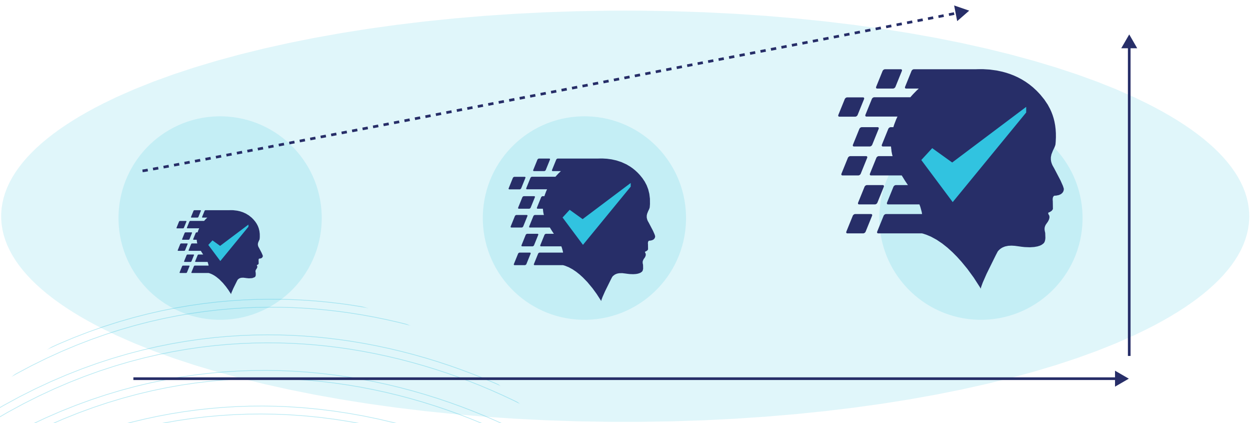
Technical Introduction

Scalability and High availability

SecurEnvoy MFA solution is designed to scale as your business grows integrating 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.

SecurAccess is able to make use of a mixed LDAP environment, consisting of multiple authentication domains across distributed sites.

SecurAccess deployments are focused primarily at delivering a resilient and distributed server architecture with seamless replication of configuration data.

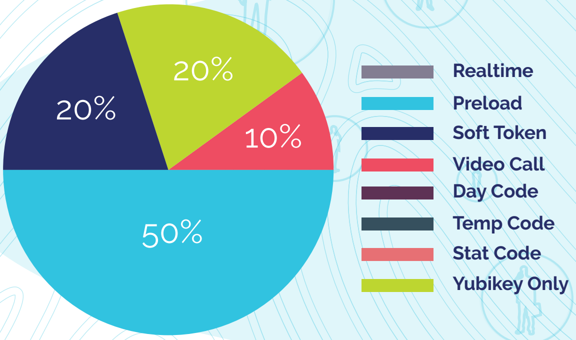


Management and Reporting

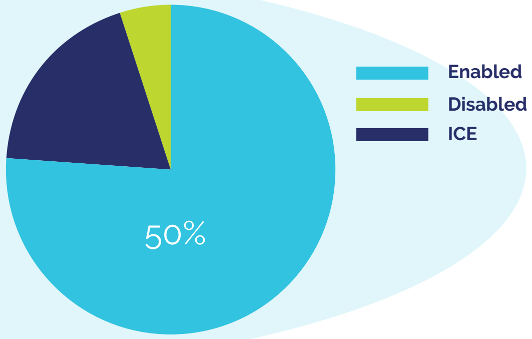
The challenge of deploying any MFA solution to a user base is primarily down to the method in which users are notified and enrolled simply, timely and as painless to the user as possible. Applying SecurEnvoy's seamless integration into the Enterprise LDAP environment, SecurAccess utilises *"Automatic Group Deployment"* to monitor selected LDAP groups for any new or removed users; issuing an automated enrolment invite.

Examples of Management Reports

Authentication Type



User Status



Technical Introduction

Integration

Direct integration without the complexity, and the flexibility to adapt to your changing business needs. SecurAccess supports various interfaces to support countless SaaS or on-premise applications or network connectivity that require securing. For legacy password or token based MFA environments, SecurEnvoy have a migration solution that offers parallel running, whilst users can be migrated across to our frictionless solution.

01
02
03
04
LOGIN
****
05

CONFIG

RADIUS with individual configuration for each client allows integration for all major SSL/IPSEC based security appliances.

SERVER

Windows Server Agent offers the ability to secure any IIS hosted websites (e.g. OWA, SharePoint or customer web application).

SUPPORT

Support for ADFS in delivering MFA authentication to public SaaS or SAML authentication based applications.

LOGON

Windows Logon Agent extends MFA authentication to domain joined laptops in an online or offline state.

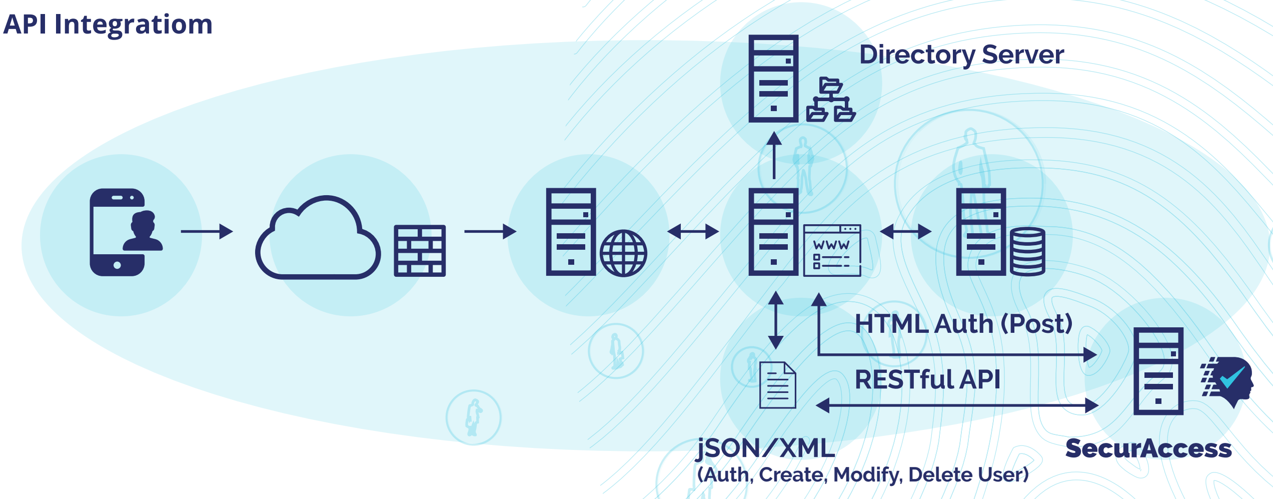
COMPATIBLE

Compatibility with over 30 Internet based SMS gateway providers or via Wavecom or Siemens SMS modems.

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 enables the creation and modification of users.

API Integratiom



Technical Introduction

Security

Security that puts you in control: SecurAccess provides security without compromise utilising Split Keys, FIPS 140-2 standards, AES 256-bit security – providing Secur user identity for your organisation.

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 140-2 standards and stored AES 256-bit securely within the enterprise directory services.

MFA delivers powerful security giving you the confidence that the split seed record is in your control, stored on your server and not known to any 3rd party

USB token

For users that haven't embraced mobile devices and prefer the hardware alternatives, we have the capability to support these users with a USB token. A driverless USB and NFC one-time hardware authentication token, that does not require pre-registration before use.

Technical Introduction

Costing

Security without compromise.

Embracing flexible billing concepts, either utilising annuity methods or by using consumption based billing. With no hidden extras you pay for what you use, ensuring cost predictability where there's no incremental hardware or deployment costs.

A variation of licensing:

SecurICE

In the event of an emergency, many organisations allow remote users to authenticate with a standard username and password. This is when the need for secure access is at its highest: as during emergency situations corporate defences are often at their weakest and the threat to attack is at its greatest. SecurEnvoy provides a licensing model that supports the ability to turn on robust, multi-factor authentication for users in the event of an emergency.

The users existing password is the first factor and a unique passcode sent to the mobile phone is the second, providing security when you need it most. SecurEnvoy reduces the reliance on helpdesks providing users a secure two factor self –service authentication to reset a forgotten password.

SecurEnvoy's solution enables the user to reset their password in real time, securely. Organisations find requests to reset passwords rapidly reduce when SecurPassword when implemented. Some organisations have seen a 100% reduction in requests and a rapid return on their investment.

SecurPassword

Password Reset with true Security

User passwords are a pain to users. They get forgotten, accounts get locked. They are time consuming to reset. SecurPassword provides the only end user experience that is simple to use and leverages true security.

- ✓ Reduced Helpdesk costs
- ✓ Ease of Use
- ✓ Intelligent alerting
- ✓ Zero Footprint
- ✓ Leverage existing user stores

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 8970 0745 22

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

General Information

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

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.

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

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.

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com
www.securenvoy.com/partner/crm

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010
Company No. **04866711** VAT Number **GB 862076128**