

In case of emergency: mobile phone-based, two-factor authentication.

Immediately authenticate all users and maintain productivity.



Key benefits:

- Enhanced security in high-risk situations
- Maintained business productivity
- Immediate, secure remote access for all users in an emergency
- Affordable, tokenless two-factor authentication
- Unaffected by text delays or signal loss
- No lengthy enrolment procedures
- No need to manage extra devices
- No software needed on the mobile phone

In the event of an emergency, many organisations allow remote users to authenticate with a standard username and password. But this is when the need for secure access is at its highest: during emergency situations corporate defenses are at their weakest and the threat from attack at its greatest.

SecurICE from SecurEnvoy is a revolutionary approach to the age-old problem of providing secure access to corporate systems in the event of an emergency – without the need for tokens or smartcards.

SecurICE provides clients with the ability to turn on strong, two-factor authentication for all users in the event of an emergency. The user's existing Microsoft password is the first factor, and a passcode sent to the user's mobile phone is the second. There is no need for the user to enrol and remember an additional PIN, and no need for extra tokens or smartcards - the perfect emergency two-factor authentication system.

Passcodes are sent via SMS to an entire organisation or a pre-identified group of users with one click from the SecurEnvoy Security Server Dashboard. The end user then connects to their protected company resource and is prompted for their UserID, PIN and Passcode. By pre-sending the first required passcode **SecurICE** eliminates problems caused by network delays and intermittent signal areas.

If an incorrect pin or passcode is entered, a new one is sent to the user's mobile phone ensuring that a passcode is always available. If more than a set number of bad PINs or passcodes are entered, the end user is disabled and no new passcodes will be sent. This security measure prevents hackers running brute force attacks.

Passcodes are sent to users' phones in a manner that enables the phone to overwrite the old message, so that the mobile phone will only ever have one SMS passcode message that is dynamically updated.

The **SecurICE** server integrates directly into Microsoft Active Directory and other common directories servers via LDAP, preventing the unnecessary burden of recreating users or trying to keep them in synchronisation.

SecurICE is licensed per user on an annual subscription.

Key Features:

- Any GSM phone can be transformed into an authentication token.
- No additional hardware required.
- No additional hardware deployment costs.
- No end user hardware failure problems.
- Supports any system that includes a radius client, such as VPN servers and WiFi access points.
- Direct real-time integration via LDAP to existing user directories.
- Protects applications that run on Microsoft IIS.
- Simple six-digit authentication code.
- Single-use passcodes prevent key-stroke logging and brute force attacks.



SecurEnvoy SecurICE

Two Factor Authentication For Disaster Recovery