

Less than half the price of tokens,
with twice the convenience.

Next generation, mobile phone-based
two-factor authentication.



Key benefits:

- Strong, affordable, convenient two-factor authentication
- Enhanced security
- Reduced helpdesk costs
- No password reset or PIN management issues
- No token/smartcard deployment, renewal or replacement costs
- No need to carry additional devices
- No software required on the mobile phone
- No delays waiting for a passcode
- Passcode always available even if temporarily out of communication

SecurAccess from SecurEnvoy enables trusted people to log on to corporate networks securely, removing password and token management problems, and social engineering attacks. It's an elegant solution to a serious business problem.

SecurAccess is simple to use. Its patented system sends a six-digit passcode to a user's mobile phone via SMS. Users then simply access the passcode from their mobile phone's SMS text store and enter it along with their UserID and Microsoft password, or PIN, to access protected corporate systems.

Once the passcode has been used, a new one is sent to the user's phone, automatically replacing the previous code. If an incorrect passcode is entered, a new one is sent, ensuring that a code is always available. The company can also decide how many 'bad' PINs or passcodes are acceptable, and disable the user once this number has been reached.

The **SecurAccess** security server integrates directly into Microsoft Active Directory and other common directories servers such as eDirectory, eliminating the need to recreate or synchronise users in a separate database. Administration is easy, via SecurEnvoy's dynamic web pages which can be accessed remotely and securely.

Key Features:

- Any GSM mobile phone can be transformed into an authentication token
- No additional hardware token required
- No end-user hardware deployment costs
- No end-user hardware failure problems
- Supports any system that includes a Radius client, such as all known VPN servers
- Direct integration to your existing user directory, no additional database is required.
- Protects applications that run on Microsoft IIS, no integration or code changes required
- Simple six-digit SMS authentication code
- Single-use passcodes prevent all known password attacks

Supported applications include:

- Any VPN Technology
- Microsoft IIS Based Applications
- Outlook Web Access
- Citrix
- Lotus Notes (via IIS)
- Any Application with a Radius Client (password authentication)

Additional requirements:

Windows 2000 or 2003 server with IIS Installed

Wavecom or Siemens modem with SIM chip or a third party web SMS Gateway provider.

Radius clients include:

- Citrix
- Juniper
- Aruba
- Aventail
- Cisco
- F5
- CheckPoint
- Nortel
- Apache Web Server
- FunK SteelBelt Radius
- Cisco ACS Radius
- Unix PAM logon

Any applications with a Radius client that only requires password authentication