



SecurAccess™

La próxima generación
Autenticación de dos factores
Sin Hardware adicional
Ningún software en el móvil



Beneficios clave:

- **Mayor Seguridad**
 - Autenticación de dos factores de usuarios remotos
 - Algo que sabes: tu PIN, y algo que tienes: tu teléfono móvil
 - Las contraseñas de un solo uso (One-Time Password, OTP) previenen los ataques de hackeo como puede ser la captura del rastro de las impresiones de las teclas
- **Costes reducidos de soporte para usuarios**
 - Sin los problemas del reseteo de las contraseñas
 - Sin los problemas de sincronización
 - Sin costes de despliegue, renovación o cambio de Tokens y tarjetas inteligentes
 - Con integración directa en tiempo real a través del LDAP con el directorio actual de los usuarios
 - Sin gestión de PINes, porque la contraseña actual de Windows es el PIN
- **Comodidad para el usuario final**
 - No hace falta llevar un dispositivo adicional ya que el propio móvil es el Token
 - Un código de autenticación de SMS de seis dígitos, fácil de leer
 - No requiere ningún software en el móvil del usuario
 - Sin espera por la contraseña porque se ha sido enviado previamente
 - La contraseña siempre está disponible, incluso en caso de que no haya cobertura

Convierta cualquier teléfono móvil en un Token de autenticación enviando mensajes SMS con una contraseña de un solo uso

Sin Hardware adicional

Sin costes de despliegue

Sin problemas de fallo de Tokens Hardware

Soporta cualquier sistema que incluye un cliente de RADIUS, como servidores de VPN/SSL y puntos de acceso WiFi

Protege aplicaciones que corren en Microsoft IIS

SecurAccess es fácil de utilizar, leer los seis dígitos previamente recibidos en el buzón de los SMS y teclearlos en el campo de la contraseña de un solo uso (OTP) después de haber entrado el nombre de identificación del usuario y la contraseña de Windows o el PIN estático.

Cuando un administrador da de alta por primera vez a un usuario, el OTP se envía al móvil del usuario a través de SMS. El envío previo del OTP da tiempo con creces para que el usuario reciba el OTP de seis dígitos. Si el teléfono del usuario está temporalmente fuera de cobertura, apagado u ocupado, el mensaje de SMS se pone en cola para intentar entregarlo más tarde hasta que el usuario lo reciba.

El usuario se conecta entonces a la red corporativa y el sistema le pide su nombre de identificación, contraseña de Windows o un PIN de acceso y la contraseña de un solo uso.

Nombre de usuario: es el mismo que el de Windows u otro de LDAP

El PIN: 4 - 8 dígitos que memoriza el usuario

El OTP: el número de seis dígitos recibido en el móvil del usuario

Si el usuario se equivoca al teclear el PIN/contraseña de Windows o el OTP, un nuevo OTP será enviado a su móvil asegurando de que, en caso de borrado del SMS que contiene la contraseña, un nuevo OTP esté siempre disponible.

En caso de teclear 10 veces erróneamente los PINes o los OTPs, la cuenta del usuario se deshabilita y no se envían más OTPs. Esta medida previene que los hackers puedan utilizar ataques de fuerza bruta.

