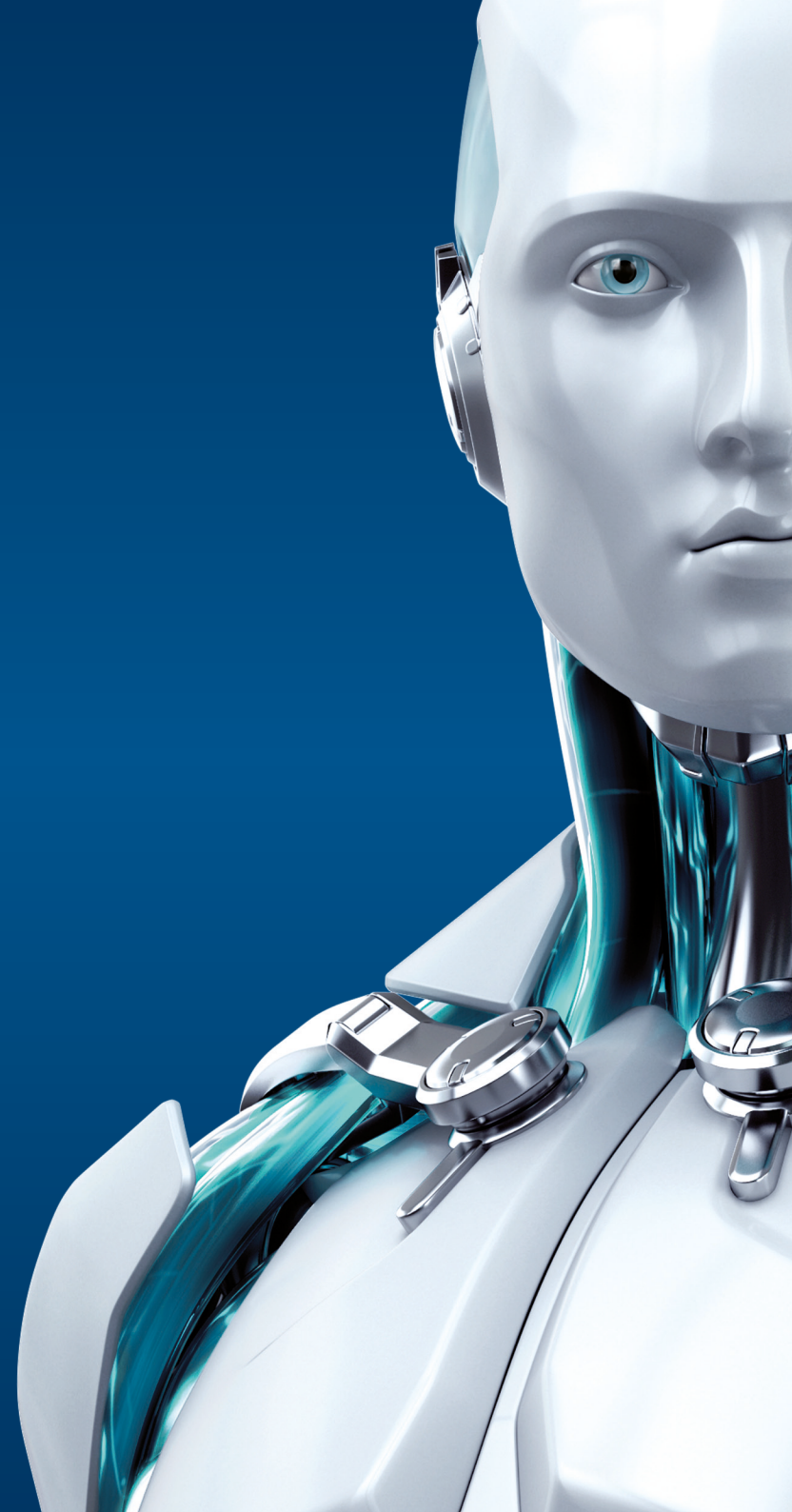




SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™





Autenticación ultrarresistente para proteger el acceso a la red y la información corporativa

ESET Secure Authentication proporciona una autenticación fuerte para proteger el acceso remoto a la red corporativa y los datos confidenciales, pero sin complicaciones.

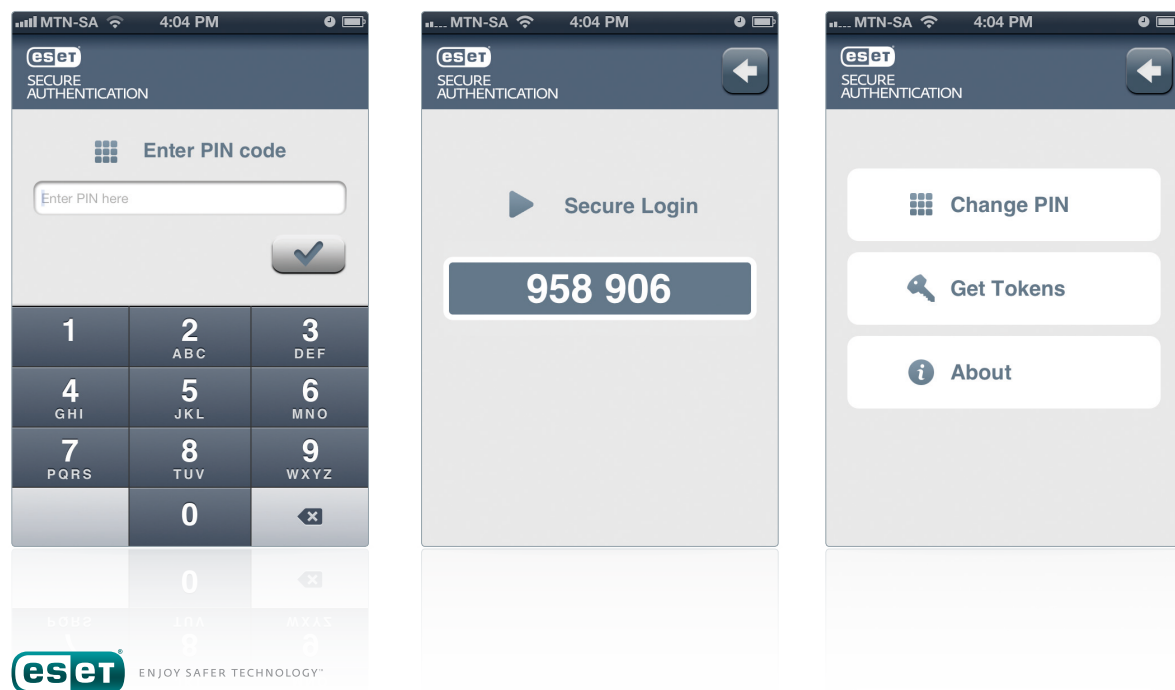
Es una solución para móviles que utiliza la autenticación de dos fases (2FA) y con contraseña de un solo uso (OTP) para acceder a la VPN y OWA (Outlook Web App). La ventaja de las contraseñas de un solo uso (OTP) es que se generan en forma aleatoria y no se pueden predecir ni volver a usar..

¿Cómo funciona ESET Secure Authentication?

Cuando los empleados acceden en forma remota a la red corporativa mediante VPN u OWA, se genera una contraseña de un solo uso en sus teléfonos móviles. Esta contraseña se usa para complementar y reforzar el proceso normal de autenticación. Como resultado, los datos y bienes de la empresa quedan protegidos ante intrusos, ataques por diccionario, adivinación de contraseñas y otras formas de crímenes cibernéticos. Utiliza la tecnología de autenticación de dos fases y con contraseña de un solo uso.

Explicación de la autenticación en dos fases (2FA)

A diferencia de la autenticación por contraseña estándar, la OTP con 2FA usa dos elementos. Estos elementos son "algo conocido por el usuario", como una contraseña o un código de identificación personal, y "algo que el usuario tiene en su poder", en general un teléfono móvil o un token de hardware. Al usarlos juntos, se incrementa considerablemente la seguridad del acceso a los datos.



Soluciona los siguientes problemas:

- Contraseñas estáticas que se pueden interceptar
- Contraseñas creadas por los usuarios que no son una cadena aleatoria de caracteres y que se pueden adivinar fácilmente
- Reutilización de contraseñas destinadas a acceder a los bienes corporativos desde cuentas privadas
- Contraseñas que contengan datos específicos de los usuarios: por ej., nombre, fecha de nacimiento
- Patrones simples desde los que se crean nuevas contraseñas, como "juan1", "juan2", etc.

Beneficios corporativos

- Ayuda a prevenir el riesgo de infiltraciones gracias al uso de contraseñas únicas para cada acceso
- Protege ante el uso inapropiado de contraseñas
- Disminuye los costos: no requiere hardware adicional
- Fácil migración y uso
- Soporte técnico global en idiomas locales

Beneficios para TI

- Solución lista para usar
- API y SDK disponibles para la integración con aplicaciones personalizadas
- Envío de la OTP mediante la aplicación en el equipo cliente o a través de un SMS
- La aplicación funciona sin conexión a Internet (una vez descargada)
- Funciona con la mayoría de dispositivos VPN
- Es compatible con la mayoría de sistemas operativos para móviles
- Soporte técnico global en idiomas locales

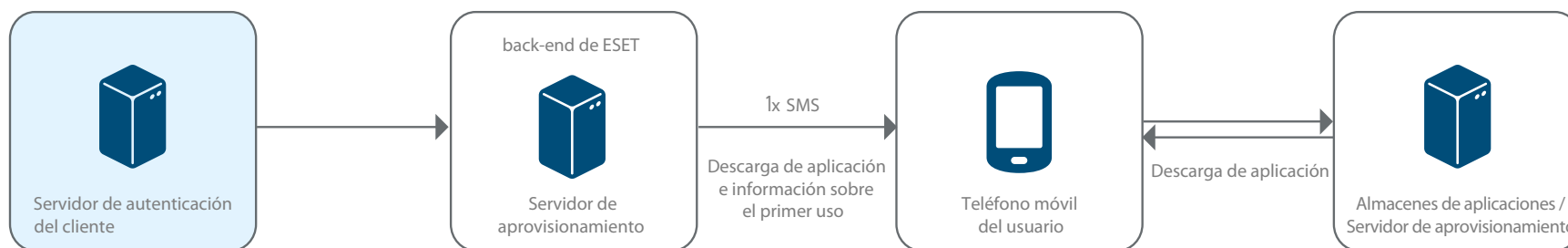
Con más detalle

La arquitectura de ESET Secure Authentication fue diseñada para usar solamente la infraestructura existente de la empresa. Además de la aplicación ESET Secure Authentication para los teléfonos móviles de los empleados (lado del cliente), contiene una aplicación para el servidor que se integra perfectamente con el familiar entorno de administración de red de la consola MMC (Microsoft Management Console) y con ADUC (Usuarios y equipos de Active Directory).

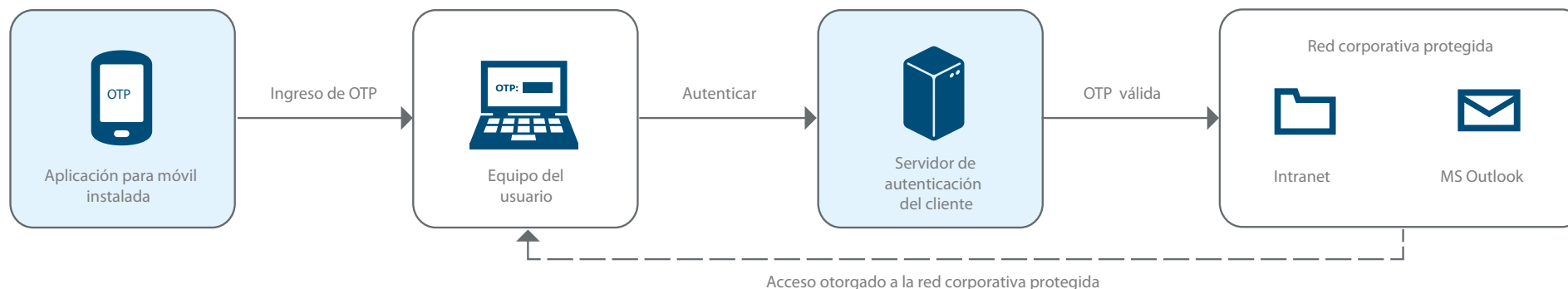
Para distribuir la aplicación ESET Secure Authentication a los teléfonos móviles, lo único que necesita saber es el número telefónico del empleado. ESET Secure Authentication le enviará al usuario un SMS con un vínculo para la activación. Al hacer un clic sobre el vínculo, automáticamente se descargará un programa de instalación para la plataforma correspondiente del móvil.

El acceso a la aplicación está protegido con un código de identificación personal para prevenir la manipulación no autorizada.

Instalación y primer uso



Comunicación del lado del cliente



Ficha informativa

Autenticación en dos fases	<p>Autenticación para móviles en dos fases (2FA) y con contraseña de un solo uso (OTP), que proporciona un mayor nivel de seguridad</p> <p>Protección nativa para Outlook Web App (OWA), redes VPN y todos los servicios basados en RADIUS</p> <p>Solución exclusivamente compuesta por software: no requiere un dispositivo o token adicional</p> <p>Conveniente para los trabajadores móviles</p>
Lado del cliente (aplicación para móviles)	<p>Instalación con un solo toque; interfaz del usuario simple y efectiva</p> <p>Distribución de las OTP mediante la aplicación en el equipo cliente o a través de un SMS</p> <p>La generación de las OTP funciona en forma independiente de la disponibilidad de conexión a Internet</p> <p>Compatible con todos los teléfonos móviles que permiten el uso de mensajería por SMS</p> <p>Incluye soporte para una amplia gama de sistemas operativos móviles</p> <p>Acceso protegido con un código de identificación personal para prevenir el fraude en caso de robo o pérdida del dispositivo</p> <p>Funciona con varias zonas de OTP, por ej., acceso a OWA, acceso a la VPN, y más</p>
Lado del servidor	<p>Solución lista para usar</p> <p>Instalación y configuración sencillas con un doble clic</p> <p>El programa de instalación reconoce automáticamente el sistema operativo y selecciona todos los componentes adecuados</p>
Administración remota	<p>Compatible con la consola Microsoft Management Console (MMC)</p> <p>Integración con Active Directory</p> <p>ESET Secure Authentication extiende la función de Usuarios y equipos de Active Directory (ADUC) con características adicionales que permiten administrar la configuración de la autenticación en dos fases de los usuarios.</p>



Requisitos del sistema:

Lado del servidor

Versiones de 32 y 64 bits de Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012

Lado del cliente

iOS 4.2.1 o posterior (iPhone)
 Android 2.1 o posterior
 Windows Phone 7 o posterior
 Windows Mobile 6
 BlackBerry 4.3 a 7.1
 Symbian: todos con soporte para J2ME
 Todos los teléfonos habilitados para J2ME

www.eset-la.com

Copyright © 1992 – 2013 ESET, spol. s r. o. ESET, el logotipo de ESET, la imagen del androide de ESET, NOD32, ESET Smart Security, Sysinspector, ThreatSense, ThreatSense.Net, LiveGrid, el logotipo de LiveGrid y/u otros productos mencionados de ESET, spol. s r. o., son marcas comerciales registradas de ESET, spol. s r. o. Windows® es una marca comercial del grupo de empresas Microsoft. Las demás empresas o productos aquí mencionados pueden ser marcas comerciales registradas de sus propietarios. Producido conforme a los estándares de calidad ISO 9001:2000.

Información de contacto: