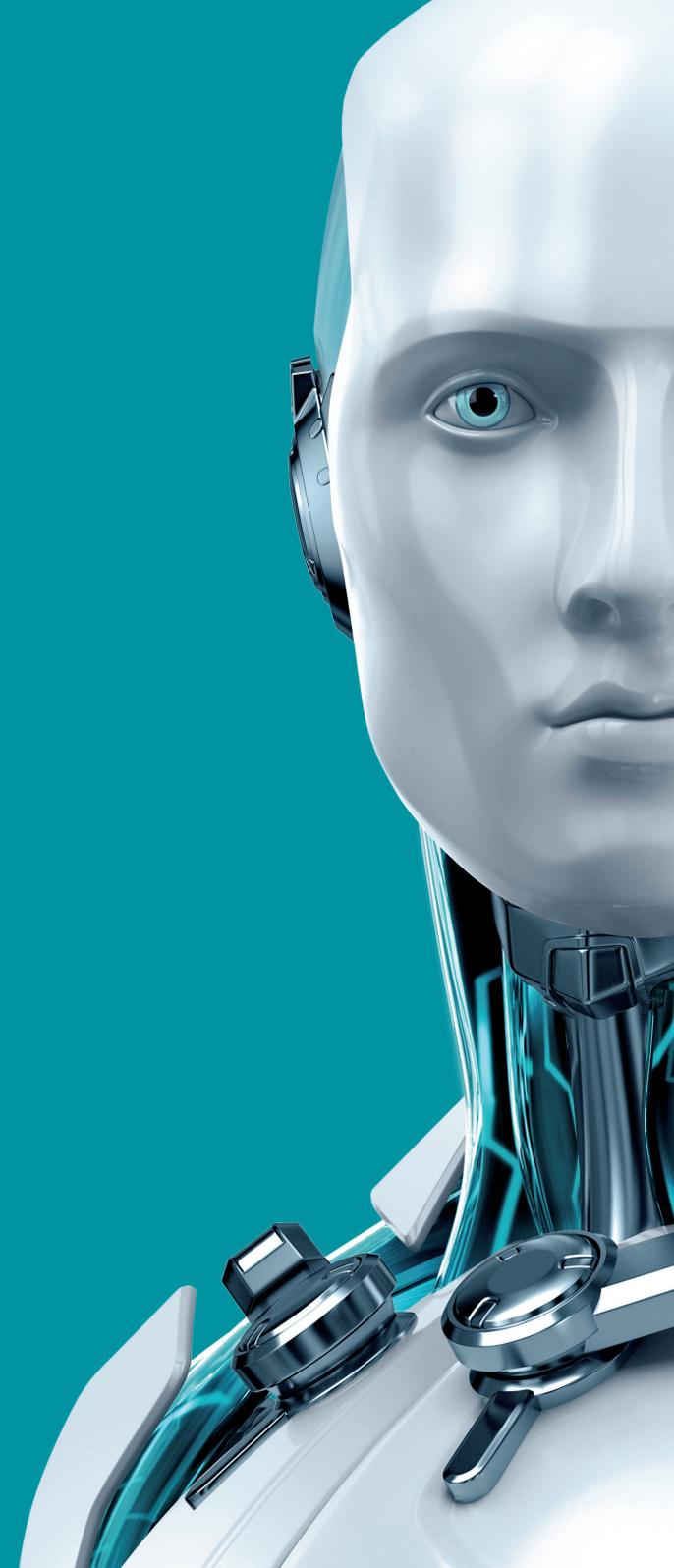




# SECURE AUTHENTICATION



ENJOY SAFER TECHNOLOGY™





# SECURE AUTHENTICATION

ESET Secure Authentication ayuda a las empresas a hacer que el acceso a su información sea más seguro. Cualquier empresa puede implementar la autenticación de doble factor de ESET en solo 10 minutos, para así reducir el riesgo de fugas de información, causadas por contraseñas robadas, débiles o puestas en riesgo.

Esta solución se compone de la parte del servidor y la del cliente, siendo ésta última una app para dispositivos móviles. Las opciones de autenticación incluyen la Autenticación por pulsación, así como la capacidad de generar y enviar contraseñas de un solo uso (OTPs) mediante la aplicación móvil, pero también mediante mensajes SMS o los tokens de hardware existentes en tu empresa.

## Autenticación de doble factor para una protección adicional de tu información.

Puedes utilizar ESET Secure Authentication para:

- Acceder a la VPN de la empresa
- Protocolo de Escritorio Remoto
- Autenticación adicional para el inicio de sesión en el escritorio (acceso a un sistema operativo)
- Servicios en la web o en la nube mediante Microsoft ADFS 3.0, tales como Office 365 y aplicaciones de Google
- Varias aplicaciones web de Microsoft, tales como Outlook Web Access (OWA)
- Panel de control de Exchange 2010 y el Centro de Administración de Exchange 2013
- VMware Horizon View
- Servicios basados en RADIUS



### Beneficios a nivel empresarial

- Ayuda a prevenir el riesgo de accesos no autorizados con contraseñas únicas para cada inicio de sesión
- Te protege del uso de contraseñas débiles
- Otorga flexibilidad para definir tu propio canal de entrega de la OTP (por ej., tu propia puerta de enlace SMS)
- Ahorra costes, sin necesidad de ningún hardware adicional
- Fácil migración y uso
- Es compatible con los tokens físicos existentes para cumplir las directivas de la empresa
- También añade autenticación de doble factor (2FA) a tus aplicaciones en la nube como Office 365 o aplicación de Google

### Beneficios a nivel técnico

- Cuenta con una API/SDK para una integración fácil en software propietario y herramientas de la empresa
- La aplicación funciona sin conexión a Internet (una vez descargada)
- Funciona con una amplia gama de aplicaciones VPN
- Es compatible con la mayoría de sistemas operativos móviles
- Cuenta con soporte técnico en español
- Solución lista para ser utilizada
- Aumenta la productividad y reduce las molestias innecesarias al acceder a sitios de confianza, gracias a la creación de listas blancas por IP
- Cuenta con herramientas para la instalación y configuración en entornos con un gran número de usuarios

## Características

<b>Autenticación de doble factor</b>	<p>Autenticación de doble factor (2FA) basado en dispositivos móviles, que proporciona un mayor nivel de seguridad.</p> <p>Es totalmente compatible con una amplia gama de plataformas (ver "Resumen de plataformas compatibles").</p> <p>Producto solo basado en software, sin necesidad de llevar ningún dispositivo o token físico adicional.</p> <p>Adecuado para los trabajadores móviles.</p> <p>Compatible con los tokens físicos.</p>
<b>Lado del cliente (aplicación móvil)</b>	<p>Instalación muy sencilla, con una interfaz de usuario simple y efectiva.</p> <p>Es compatible con una amplia gama de sistemas operativos móviles y con cualquier teléfono móvil que permita el envío de SMS.</p> <p>Cuenta con PIN de protección de acceso para evitar el fraude en caso de robo o pérdida del dispositivo.</p> <p>La aplicación está disponible en español y en otros idiomas.</p>
<b>Métodos de autenticación</b>	<p>Aplicación móvil en el cliente: genera contraseñas de un solo uso (OTPs). No requiere conexión a Internet.</p> <p>Autenticación por pulsación mediante teléfono móvil (requiere la aplicación móvil en el cliente; funciona con dispositivos Android).</p> <p>Envío de las contraseñas de un solo uso por SMS.</p> <p>Tokens físicos: aunque el programa no necesita hardware de tokens para funcionar, es compatible con todos los tokens HOTP basados en eventos que son compatibles con OATH.</p> <p>Métodos personalizados: por ejemplo, mediante correo electrónico.</p>
<b>Lado del servidor</b>	<p>Producto listo para ser utilizado.</p> <p>Fácil instalación y configuración con doble clic.</p> <p>El instalador reconoce automáticamente el sistema operativo y selecciona todos los componentes apropiados.</p> <p>Instalador interactivo. Instalación inmediata en el ADFS (sistema de archivos de Active Directory).</p>
<b>Opciones de integración personalizada</b>	<p>En el entorno de Active Directory, utiliza la API de ESET Secure Authentication o la API de Administración de Usuarios para una fácil integración en sistemas propios.</p> <p>El SDK permite una implementación para los no usuarios de Active Directory.</p>
<b>Administración remota</b>	<p>Es compatible con la Consola de Administración de Microsoft (MMC).</p> <p>Integración con Active Directory.</p> <p>ESET Secure Authentication añade a los usuarios y equipos de Active Directory características adicionales para poder administrar la configuración de la doble autenticación de los usuarios.</p>



**SOPORTE  
TÉCNICO  
GRATUITO  
EN ESPAÑOL**

Cada licencia cuenta con el servicio de soporte técnico gratuito por parte de nuestros especialistas, proporcionado en español.

### Requisitos del sistema

Lado del servidor: versiones de 32 y 64 bits de Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2.

Lado del cliente: iOS 4.3 o superior (iPhone); Android 2.1 o superior; Windows Phone 7 o posterior; Windows Mobile 6; BlackBerry 4.3 a 7.1 y 10 y superior; Symbian - todos los compatibles con J2ME; todos los teléfonos con J2ME activado.

Compatible con hardware de token: aunque el programa no necesita hardware de tokens para funcionar, es compatible con todos los tokens HOTP basados en eventos que son compatibles con OATH.

## Resumen de plataformas compatibles

Para unos requisitos técnicos detallados, por favor, consulta el manual del producto de ESET Secure Authentication, disponible en esta dirección:

[http://download.eset.com/manuals/eset\\_esa\\_product\\_manual\\_enu.pdf](http://download.eset.com/manuals/eset_esa_product_manual_enu.pdf)

<b>Plataformas para el inicio de sesión remoto</b>	<b>Protocolo de escritorio remoto</b> <b>Protección VPN:</b> Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall	
<b>Protección para el inicio de sesión (Windows)</b>	Windows 7 y posterior	Windows Server 2008 R2 y posterior
<b>Servicios de la federación de Active Directory</b>	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
<b>Plataformas VDI compatibles</b>	VMware Horizon View	Citrix XenApp
<b>Aplicaciones web de Microsoft</b>	Microsoft Exchange 2007 Acceso web de Outlook Microsoft Exchange 2010 Aplicación web de Outlook Panel de control de Exchange Microsoft Exchange 2013 Aplicación web de Outlook Centro de administración de Exchange	Microsoft Dynamics CRM 2011, 2013, 2015 Microsoft SharePoint 2010, 2013 Acceso web al Escritorio Remoto de Microsoft Acceso web a los servicios de Terminal de Microsoft Acceso web remoto a Microsoft
<b>Integración personalizada</b>	ESET Secure Authentication se integra fácilmente con tus servicios basados en RADIUS, y mediante la API de ESET Secure Authentication o la API de Administración de usuarios en tu autenticación basada en Active Directory. Los clientes que no usan Active Directory y tienen sistemas personalizados pueden usar el SDK, que es fácil de instalar.	
<b>Sistemas operativos (parte del servidor)</b>	Windows Server 2003 (32 y 64 bits), 2003 R2 (32 y 64 bits), 2008 (32 y 64bit), 2008 R2, 2012, 2012 R2 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials Las herramientas de administración también son compatibles en los sistemas operativos cliente desde Windows XP SP3 en adelante, tanto en las versiones de 32 como de 64 bits.	
<b>Sistemas operativos para teléfonos móviles (aplicación del lado del cliente)</b>	iOS Android Windows Phone Windows Mobile	BlackBerry Symbian: todos los compatibles con J2ME Todos los teléfonos con J2ME activado

Copyright © 1992 – 2016 ESET, spol. s r. o. ESET, el logo de ESET, la figura del androide ESET, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, el logo de LiveGrid y/u otros productos de ESET, spol. s r. o., son marcas registradas de ESET, spol. s r. o. El resto de compañías o marcas registradas son propiedad de sus respectivos titulares. Producido según el estándar de calidad ISO 9001:2008.

Ficha v: 20170323