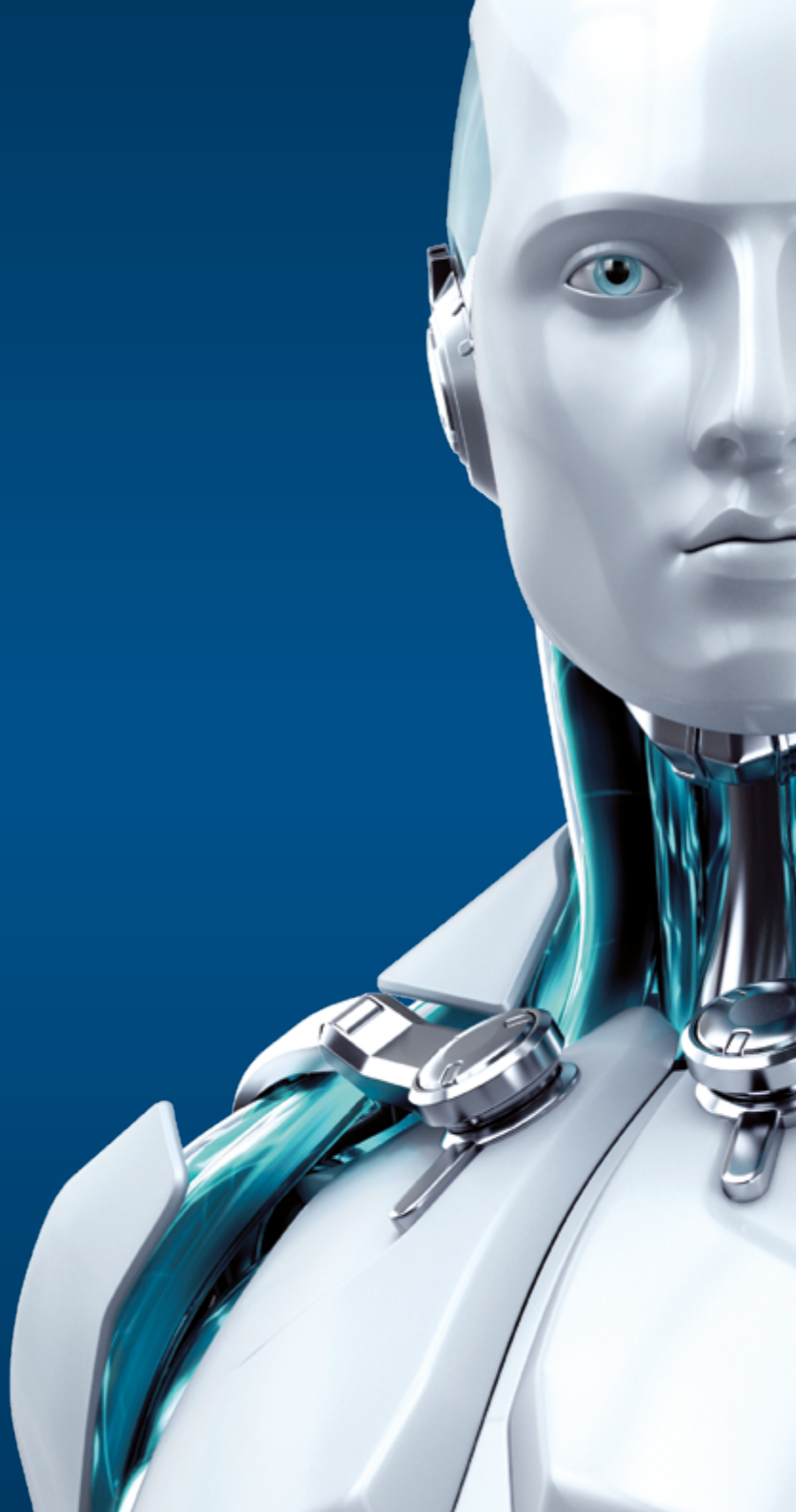
SECURE AUTHENTICATION



ENJOY SAFER TECHNOLOGY™

SECURE AUTHENTICATION

ESET Secure Authentication es un sistema de autenticación en dos fases para dispositivos móviles que proporciona seguridad adicional durante el acceso a la red corporativa y a sus datos confidenciales, sin complicaciones.

La solución está compuesta por dos partes: un lado servidor y un lado cliente; este último se suministra como una app móvil. La generación de contraseñas de un solo uso (OTP, del inglés) no es la única opción para la app móvil, dado que también se pueden usar mensajes de SMS o tokens existentes.

Autenticación extremadamente resistente para proteger el acceso a la red y a los activos corporativos

ESET Secure Authentication sirve para:

- Acceder a la VPN de la empresa
- Protocolo de escritorio remoto
- Autenticación adicional para el inicio de sesión en equipos de escritorio (iniciando sesión en un sistema operativo)
- Servicios basados en la Web o la nube mediante Microsoft ADFS 3.0, por ej., Office 365 y Google Apps
- Varias de las apps en la Web de Microsoft, como Outlook Web Access (OWA)
- Exchange Control Panel 2010 y Exchange Administrator Centre 2013
- VMware Horizon View
- Servicios basados en RADIUS

ESET Secure Authentication también incluye una API para su integración con la autenticación existente basada en Active Directory, y un SDK para su fácil implementación en cualquier sistema propio de la empresa.

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
- Brinda flexibilidad para definir su propio canal de distribución de contraseñas de un solo uso (por ej., mediante su propia puerta de enlace para SMS)
- Disminuye los costos: no requiere hardware adicional
- Es fácil de migrar y de usar
- Es compatible con los tokens de hardware existentes para cumplir con las normativas corporativas
- Además permite incorporar la autenticación en dos fases a las aplicaciones corporativas en la nube, como Office 365 o Google Apps

Beneficios para TI

- La API y el SDK permiten una fácil integración con el software propio de la empresa y con herramientas corporativas
- La app funciona sin conexión a Internet (una vez descargada)
- Es compatible con una amplia gama de dispositivos VPN
- Es compatible con la mayoría de sistemas operativos para móviles
- Soporte técnico global en idiomas locales
- Solución lista para usar
- Mejora la productividad y reduce problemas innecesarios al acceder a sitios de confianza, gracias a la Lista Blanca de direcciones IP
- Herramientas para el despliegue y la configuración en entornos de mucha cantidad de usuarios

Ficha informativa

Autenticación en dos fases	Autenticación para móviles en dos fases (2FA) con contraseña de un solo uso (OTP) para lograr un mayor nivel de seguridad
	Soporte nativo para una amplia gama de plataformas (consulte la Información general sobre plataformas compatibles)
	Solución conformada exclusivamente por software: no requiere la presencia de un dispositivo o token adicional
	Conveniente para los trabajadores móviles
	Soporte para tokens de hardware
Lado cliente (app móvil)	Instalación con un solo toque; interfaz del usuario simple y efectiva
	Distribución de las OTP a través de la aplicación en el equipo cliente, un SMS o un token de hardware
	La generación de las OTP funciona independientemente de la conexión a Internet
	Compatible con todos los teléfonos móviles que admiten el uso de mensajería por SMS
	Incluye soporte para una amplia gama de sistemas operativos móviles
	Acceso protegido con un código de identificación personal para prevenir el fraude en caso de robo o pérdida del dispositivo
	Funciona con varias zonas de OTP, por ej., acceso a OWA, acceso a la VPN, y más
	Las apps móviles están disponibles en los siguientes idiomas: inglés, alemán, ruso, francés, español y eslovaco
Lado servidor	Solución lista para usar
	Instalación y configuración sencillas con un doble clic
	El programa de instalación reconoce automáticamente el sistema operativo y selecciona todos los componentes adecuados
	Programa de instalación interactivo, instalación integrada a los Servicios de Federación de Active Directory (AD FS, del inglés)
Opciones de integración personalizada	En un entorno con Active Directory, puede utilizar la API de ESET Secure Authentication o la API de la Administración de usuarios para una fácil integración con los sistemas propietarios
	El SDK permite la implementación en entornos que no utilizan Active Directory
Administración Remota	Compatible con la consola Microsoft Management Console (MMC)
	Integración con Active Directory
	ESET Secure Authentication extiende la función de Usuarios y Equipos de Active Directory (complemento ADUC) aportando características adicionales que permiten administrar la configuración de la autenticación en dos fases de los usuarios

Información general sobre plataformas compatibles

Plataformas para el inicio de sesión remoto	**Protocolo de escritorio remoto** **Protección de la VPN:** **Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall**	
Protección del inicio de sesión local (Windows)	Windows 7 y posterior	Windows Server 2008 R2 y posterior
Servicios de Federación de Active Directory	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
Plataformas de Infraestructura de escritorio virtual (VDI, del inglés) compatibles	VMware Horizon View	Citrix XenApp
Aplicaciones Web de Microsoft	Aplicaciones Web de Microsoft Outlook Web Access Microsoft Exchange 2010 Outlook Web App Panel de control de Exchange Microsoft Exchange 2013 Outlook Web App Exchange Admin Center	Microsoft Dynamics CRM 2011, 2013, 2015 Microsoft SharePoint 2010, 2013 Acceso Web de Escritorio Remoto de Microsoft Acceso Web de Terminal Services de Microsoft Acceso Web Remoto de Microsoft
Integración personalizada	ESET Secure Authentication se integra fácilmente a sus servicios basados en RADIUS. También se integra a la autenticación existente basada en Active Directory a través de la API de ESET Secure Authentication o la API de Administración de Usuarios. Los clientes que tengan sistemas propios hechos a medida pueden utilizar el SDK, que es muy fácil de desplegar.	
Sistemas operativos (lado servidor)	Windows Server 2003(32 y 64 bits), 2003 R2 (32 y 64 bits), 2008 (32 y 64 bits), 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 de equipos cliente con Windows XP SP3 en adelante, tanto en las versiones de 32 como de 64 bits.	
Sistemas operativos de teléfonos móviles (App del lado cliente)	iOS 4.3 o posterior (iPhone) Android 2.1 o posterior Windows Phone 7 o posterior Windows Mobile 6	BlackBerry 4.3 a 7.1 y 10 y posterior Symbian (todos con soporte para J2ME) Todos los teléfonos habilitados para J2ME