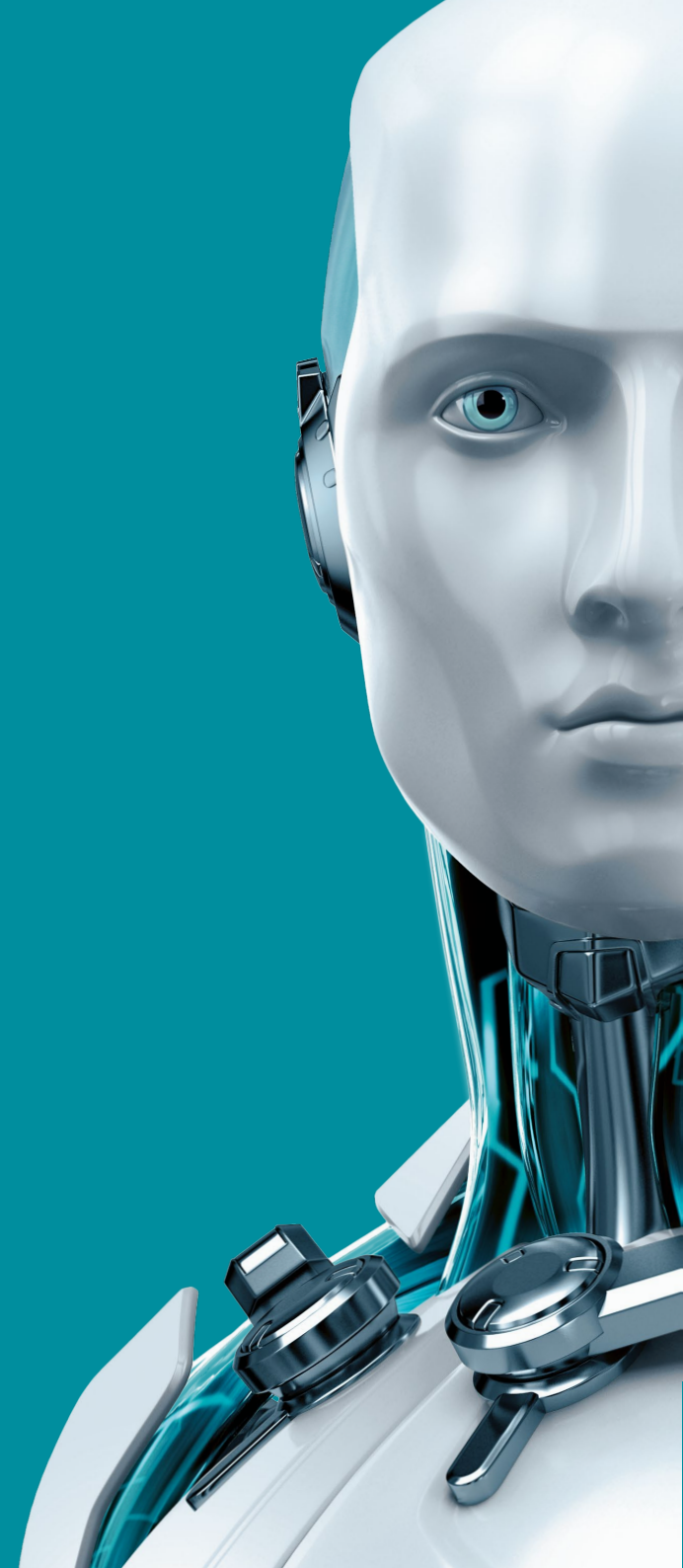




SECURE AUTHENTICATION



ENJOY SAFER TECHNOLOGY™





SECURE AUTHENTICATION

A ESET Secure Authentication ajuda as empresas a acessar seus dados com segurança. Qualquer organização pode configurar a autenticação de duplo fator da ESET em apenas 10 minutos, e então reduzir facilmente o risco de violação de dados causado por roubo e senhas fracas e comprometidas.

A solução é composta pelo lado do servidor e pelo lado do cliente - o último vem na forma de app de celular. As opções de autenticação incluem Push Authentication, bem como a geração e entrega de senhas de uso único (OTPs) através do app do celular, mas também através de mensagens SMS ou dos tokens já existentes no hardware da sua empresa.

Autenticação de duplo fator para proteção extra de dados

Você pode usar sua ESET Secure Authentication para:

- Acessar o VPN da sua empresa
- Protocolo de desktop remoto
- Autenticação adicional para login de desktop (logando em um sistema operacional)
- Serviços web/na nuvem através do Microsoft ADFS 3.0, como o Office 365 e o Google Apps
- Vários apps via web da Microsoft, como o Outlook Web Access (OWA)
- Exchange Control Panel 2010 e Exchange Administrator Centre 2013
- VMWare Horizon View
- Serviços com base em RADIUS

O ESET Secure Authentication também vem com um API para integrá-lo na já existente Autenticação do Active Directory, bem como com um kit de desenvolvimento de software que facilmente o implementa em qualquer sistema registrado.

Benefícios para a empresa

- Ajuda a prevenir o risco de violações com senhas únicas para cada acesso
- Protege contra práticas ruins de uso de senhas
- Dá à você flexibilidade para definir seu próprio canal de entrega da OTP (por exemplo, seu próprio gateway de SMS)
- Economiza nos custos (não é necessário hardware adicional)
- Fácil de migrar e usar
- Suporta os tokens existentes de hardware para alcançar os requisitos de conformidade
- Também adiciona autenticação de duplo fator aos seus aplicativos de nuvem, como o Office 365 e o Google Apps.

Benefícios de TI

- API/Kit de Desenvolvimento de Software para fácil integração com software registrado e ferramentas de negócios
- O app funciona sem conexão com a internet (uma vez baixado)
- Trabalha com uma grande variedade de equipamentos VPN
- Suporta a maior parte dos tipos de sistemas operacionais de celular
- Suporte técnico global em seu idioma local
- Solução pronta para usar
- Aumenta a produtividade e reduz resistência desnecessária ao acessar sites de confiança, graças às listas brancas de IP
- Ferramentas para instalação e configuração em grandes ambientes de usuário

Datasheet

Autenticação de duplo fator	<p>Autenticação de duplo fator com base no celular (2FA) para um nível mais alto de segurança.</p> <p>Suporte nativo para uma grande variedade de plataformas (veja abaixo Informações Gerais sobre Plataformas Suportadas).</p> <p>Solução baseada em software – não é necessário carregar um aparelho adicional ou token.</p> <p>Conveniente para sua força de trabalho móvel.</p> <p>Suporte para os tokens de hardware.</p>
Lado do cliente (app de celular)	<p>Instalação com um toque, interface de usuário simples e efetiva.</p> <p>Compatível com qualquer telefone celular que suporte mensagens de SMS</p> <p>Suporta uma grande variedade de sistemas operacionais de celular.</p> <p>Acesso protegido por PIN para proteger contra fraudes em caso de roubo ou perda.</p> <p>Apps disponíveis nos seguintes idiomas: inglês, alemão, russo, francês, espanhol e eslovaco.</p>
Métodos de autenticação	<p>App do cliente de celular – gera senhas para uso único (OTPs), não há necessidade de conexão com a internet.</p> <p>Push Authentication – autenticação com um único toque através do telefone celular (requer app do cliente de celular, trabalha com aparelhos Android e iOS).</p> <p>Senha de uso único (OTP) entregue via SMS.</p> <p>Tokens de hardware (enquanto que a solução não requer tokens de hardware para funcionar, ela suporta todos os tokens HOTP baseado em eventos que sejam compatíveis com OATH).</p> <p>Métodos customizados (por exemplo, via e-mail).</p>
Lado do servidor	<p>Solução pronta para usar</p> <p>Fácil instalação e configuração com duplo clique.</p> <p>O instalador reconhece automaticamente o sistema operacional e seleciona todos os componentes compatíveis.</p> <p>Instalador interativo, instalação rápida e fácil no ADFS.</p>
Opções de customização integradas	<p>No ambiente do Active Directory, use tanto o API de Autenticação de Segurança ESET como o API de Gerenciamento de Usuário para fácil integração em um sistema registrado.</p> <p>O Kit de Desenvolvimento de Software permite a implementação para não-usuários do Active Directory.</p>
Gerenciamento Remoto	<p>Suporta o Console de Gerenciamento da Microsoft (MMC).</p> <p>Integração com o Active Directory.</p> <p>A Autenticação de Segurança ESET se estende aos Computadores e Usuários do Active Directory (plugin ADUC) com funcionalidades adicionais que permitem o gerenciamento das configurações da autenticação de duplo fator dos usuários.</p>

Informações gerais sobre as plataformas suportadas

Para requisitos técnicos detalhados, por favor, consulte o manual da Autenticação de Segurança ESET, disponível neste endereço:

http://download.eset.com/manuals/ezet_esa_product_manual_enu.pdf

Plataformas de login remoto	Protocolo de desktop remoto Proteção de VPN: Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Cjeck Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.	
Proteção de Login Local (Windows)	Windows 7 ou mais recente	Windows Server 2008 R2 e mais recente
Active Directory Federation Services	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
Plataformas VDI suportadas	VMware Horizon View	Citrix XenApp
Aplicativos de web Microsoft	Microsoft Exchange 2007 — Outlook Web Access Microsoft Exchange 2010 — Outlook Web App — Exchange Control Panel Microsoft Exchange 2013 — Outlook Web App — Exchange Admin Center	Microsoft Dynamics CRM 2011, 2013, 2015 Microsoft SharePoint 2010, 2013 Microsoft Remote Desktop Web Access Microsoft Terminal Services Web Access Microsoft Remote Web Access
Integração Customizada	ESET Secure Authentication se integra facilmente com serviços baseado em RADIUS, bem como através do API de Autenticação de Segurança ESET ou do API de Gerenciamento do Usuário para sua já existente autenticação baseada no Active Directory. Os clientes sem Active Directory com sistemas customizados podem usar o kit de desenvolvimento de software fácil de instalar.	
Sistemas Operacionais (Lado do servidor)	Windows Server 2003 (32&64bit), 2003 R2 (32&64bit), 2008 (32&64bit), 2008 R2, 2012, 2012 R2 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials As ferramentas de gerenciamento também são suportadas nos sistemas operacionais do cliente a partir do Windows XP SP3 em diante, em ambas versões de 32 e 64 bits.	
Plataformas de telefone celular suportadas (App do lado do cliente)	iOS Android Windows Phone Windows Mobile	BlackBerry Symbian – todas que suportam J2ME Qual aparelho que habilitado com J2ME

Copyright 1992-2017/ESET spol. s. r. o. ESET, o logo ESET, a figura Andréide da ESET, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, o logo do LiveGrid e/ou outros produtos mencionados da ESET spol. s. r. o. são marcas registradas da ESET, spol. s. r. o. Windows é uma marca registrada do grupo de empresas Microsoft. Outras empresas ou produtos mencionados aqui podem ser marcas registradas de outros proprietários. Produzido de acordo com os padrões de qualidade do ISO 9001/2008.