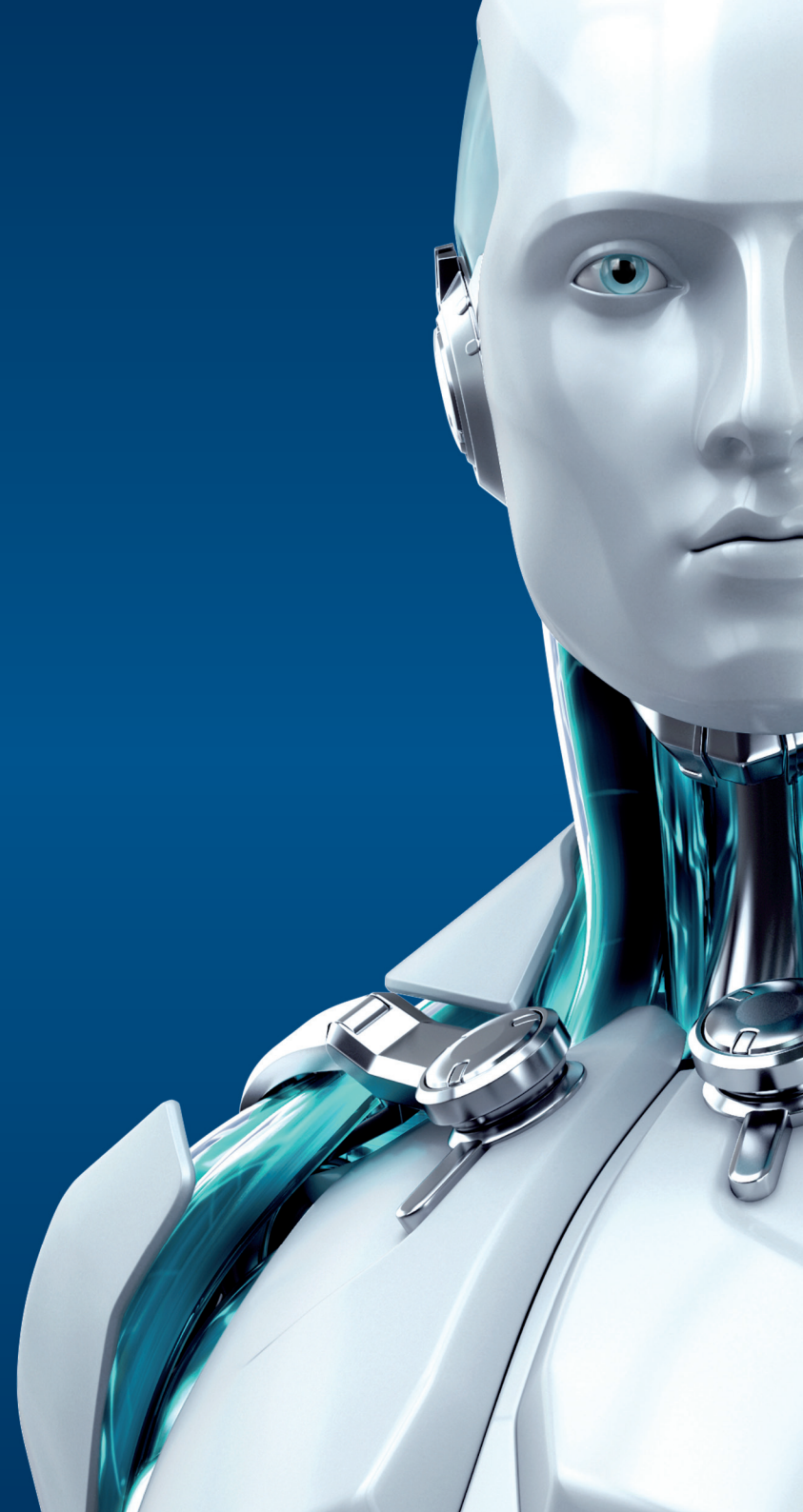




# SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™





## SECURE AUTHENTICATION

ESET Secure Authentication ist eine mobilbasierte Zwei-Faktor-Authentifizierungslösung, die Zugriffe auf Ihre Unternehmensnetzwerke und -daten zuverlässig absichert.

Schwache und verlorene Passwörter gehören zu den größten Sicherheitsrisiken. ESET Secure Authentication ergänzt das normale Anmeldeverfahren aus Benutzernamen und Passwort um einen zusätzlichen Sicherheitsfaktor. Zu den Authentifizierungsmethoden gehören Push-Benachrichtigungen sowie die Bereitstellung eines Einmal-Passworts – per mobiler Client-App, SMS oder bestehenden Hardware-Token.

## Starke Authentifizierung zum Schutz Ihrer Daten und Netzwerke

Nutzen Sie ESET Secure Authentication für:

- Zugang zu Ihrem Unternehmens-VPN
- Remote Desktop Protocol
- Zusätzliche Authentifizierung für Desktop-Logins (Anmeldung beim Betriebssystem)
- Web-/Cloud-Dienste via Microsoft ADFS 3.0, wie Office 365 und Google Apps
- Verschiedene Microsoft Web Apps, wie Outlook Web Access (OWA)
- Exchange Control Panel 2010 & Exchange Administration Center 2013
- VMware Horizon View
- RADIUS-basierte Dienste

ESET Secure Authentication enthält eine API zur Integration in Ihr bestehendes Active Directory Authentifizierungssystem sowie ein SDK zur problemlosen Einbindung in proprietäre Systeme.

### Vorteile für Ihr Unternehmen

- Verhindert das Risiko unberechtigter Zugriffe dank einzigartiger Einmal-Passwörter
- Schützt vor schwachen Passwort-Praktiken
- Bietet die Möglichkeit, den Weg der OTP-Bereitstellung zu definieren (z.B. über eigenes SMS-Gateway)
- Ohne Zusatzkosten – keine extra Hardware nötig
- Einfache Migration und Handhabung
- Unterstützt bestehende Hardware-Token zur Einhaltung der Compliance-Richtlinien
- Sichert Zugriffe auch bei Ihren Cloud Anwendungen wie Office 365 oder Google App

### Vorteile für Ihre IT

- Bietet API und SDK für eine problemlose Integration in proprietäre Software und Business-Tools
- Nach Installation funktioniert die App auch ohne Internetverbindung
- Unterstützt die meisten VPN Appliances
- Unterstützt alle marktüblichen mobilen Betriebssysteme
- Weltweiter technischer Support in Ihrer Landessprache
- Innerhalb weniger Minuten einsatzbereit
- Erhöht die Produktivität und verringert dank IP-Whitelisting unnötige Probleme beim Aufruf vertrauenswürdiger Webseiten
- Bietet Tools zur Entwicklung und Konfiguration in großen Benutzerumgebungen

# Datenblatt

---

<b>Zwei-Faktor-Authentifizierung</b>	<p>Die auf Mobiltelefonen basierende Zwei-Faktor-Authentifizierung (2FA) mit Einmal-Passwörtern (OTP) bietet ein höheres Maß an Sicherheit</p> <p>Nativer Schutz für eine Vielzahl an Plattformen (einen Überblick der unterstützten Plattformen finden Sie auf der nächsten Seite)</p> <p>Reine Software-Lösung – keine zusätzlichen Geräte oder Hardware-Token nötig</p> <p>Sicherheit und Nutzerkomfort für Mitarbeiter im Außendienst</p> <p>Unterstützung für Hardware-Token</p>
<b>Client (mobile App)</b>	<p>Installation mit einem Klick, einfache und effektive Benutzeroberfläche</p> <p>Kompatibel mit jedem SMS-fähigen Mobiltelefon</p> <p>Unterstützt die marktüblichen mobilen Betriebssysteme</p> <p>PIN-geschützter Zugriff verhindert Fremdnutzung</p> <p>Die App ist in folgenden Sprachen erhältlich: Deutsch, Englisch, Französisch, Spanisch, Russisch und Slowakisch</p>
<b>Authentifizierungsmethoden</b>	<p>Generierung eines Einmal-Passworts (OTPs) über die mobile Client-App – Internetverbindung ist nicht erforderlich</p> <p>Authentifizierung über Push-Benachrichtigung auf das Mobiltelefon – funktioniert nur auf Android-Geräten; mobile Client-App erforderlich</p> <p>Bereitstellung eines OTPs per SMS</p> <p>Bereitstellung eines OTPs über bestehende Hardware-Token – unterstützt alle ereignisbasierten, OATH-konformen HOTP-Token</p> <p>Individuelle Methoden (z.B. per E-Mail)</p>
<b>Server im Unternehmen</b>	<p>Innerhalb weniger Minuten einsatzbereit</p> <p>Einfache Installation und Konfiguration per Doppelklick</p> <p>Der Installer erkennt automatisch das Betriebssystem und passt die Grundeinrichtung entsprechend an</p> <p>Interaktiver Installer, Drop-in-Installation in ADFS</p>
<b>Remote Management</b>	<p>Unterstützt die Microsoft Management Console (MMC)</p> <p>Active Directory Integration</p> <p>ESET Secure Authentication erweitert ADUC (Active Directory User &amp; Computers) mit einem Plugin, das zusätzliche Verwaltungsfunktionen von Einstellungen der Zwei-Faktor-Authentifizierung bereitstellt</p>

# Unterstützte Plattformen

<b>Remote-Login-Plattformen</b>	<b>Remote Desktop Protocol</b>	
	<b>VPN-Schutz:</b>	
	Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall	
<b>Schutz für lokale Anmeldung (Windows)</b>	Windows 7 und höher	Windows Server 2008 R2 und höher
<b>Active Directory-Verbunddienste</b>	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
<b>Unterstützte VDI Plattformen</b>	VMware Horizon View	Citrix XenApp
<b>Microsoft Web Applications</b>	Microsoft Web Applications Outlook Web Access	Microsoft Dynamics CRM 2011, 2013, 2015 Microsoft SharePoint 2010, 2013
	Microsoft Exchange 2010 Outlook Web App Exchange Control Panel	Microsoft Remote Desktop Web Access Microsoft Terminal Services Web Access Microsoft Remote Web Access
	Microsoft Exchange 2013 Outlook Web App Exchange Admin Center	
<b>Individuelle Integration</b>	ESET Secure Authentication lässt sich problemlos in Ihre RADIUS-basierten Dienste sowie mithilfe der ESET Secure Authentication API oder der User Management API in Ihr bestehendes Active Directory Authentifizierungssystem integrieren. Für Eigenentwicklungen oder Systeme ohne Active Directory Anbindungen kann die vollständige Funktionalität über das SDK eingebunden werden.	
<b>Betriebssysteme (Server)</b>	Windows Server 2003 (32- & 64-Bit), 2003 R2 (32- & 64-Bit), 2008 (32- & 64-Bit), 2008 R2, 2012, 2012 R2 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials Zudem werden Management-Tools auf Clients mit Betriebssystemen von Windows XP SP3 an, sowohl 32- als auch 64-Bit-Versionen, unterstützt.	
<b>Mobile Betriebssysteme (Client)</b>	iOS 4.3 oder höher Android 2.1 oder höher Windows Phone 7 oder neuer Windows Mobile 6	BlackBerry 4.3 bis 7.1 sowie 10 oder höher Symbian – alle, die J2ME unterstützen Alle J2ME-fähige Mobiltelefone

Copyright © 1992 – 2016 ESET, spol. s r. o., ESET, das ESET-Logo, ESET Android-Abbildung, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, das LiveGrid Logo und/oder andere aufgeführte Produkte von ESET, spol. s r. o., sind eingetragene Warenzeichen von ESET, spol. s r. o. Windows® ist ein eingetragenes Warenzeichen der Microsoft Group of Companies. Andere hier erwähnte Firmennamen oder Produkte können eingetragene Warenzeichen ihrer Eigentümer sein. Hergestellt nach den Qualitätsstandards von ISO 9001:2008.